CISOs INVESTIGATE:

USER BEHAVIOR ANALYTICS

Peer-authored Research

securitycurrent

Sponsors

Platinum

SECURONIX
Security Analytics. Delivered.

Gold

LogRhythm™
The Security Intelligence Company

sqrrl
Target. Hunt. Disrupt.

VARONIS

Silver

exabeam

Table of Contents

INTRODUCTION....4
A CISO LOOKS AT THE HISTORY OF UBA....5
TECHNOLOGY OVERVIEW....8
UBA Core Features....8
A Deeper Dive into UBA....9
Key Considerations....9
To Deploy or Not to Deploy....10
SELLING TO THE C-SUITE....11
Reducing Potential Losses from a Breach....12
UBA's Role in the Defense-in-Depth Approach....12
Maintaining Compliance through UBA....13
Staffing Implications....15
When UBA May Have Stopped Real World Breaches....16
Beyond Security: Other Business Cases for UBA....17
MARKET ASSESSMENT....19
KEY TAKEAWAYS....23
First Takeaway – A Win-Win for CISOs....23
Second Takeaway – Effective Across Industries....25
Third Takeaway – A Natural Fit for Risk-based Security....26
SUSTAINABILITY....27
WHEN UBA DOESN'T WORK....29
SUMMARY....30
CISO CONTRIBUTIONS....31
Actian Corporation....31
Aetna....33
Barclays....36
IBM....37
Levi Strauss & Company....39
MIAX Options....42
Oppenheimer & Co....44
RWJBarnabas Health....47
Surescripts....50
APPENDIX A – COMPLIANCE....53
APPENDIX B – SUPPLEMENTAL INFORMATION & RESOURCES....59
APPENDIX C – VENDOR RFIs....61
SPONSORED ADDENDUM....103

Introduction

About CISOs Investigate

The value of peer input cannot be overstated. Authored by leading Chief Information Security Officers, CISOs Investigate is an ongoing series that offers first-hand insights to security leaders as they make business-driven technology decisions.

CISO Contributors

CISOs Investigate: User Behavior Analytics (UBA) includes interviews with 11 security leaders who have deployed or are looking to deploy third-party solutions. This report replaces the ad hoc, often informal and time-consuming processes of personally gathering peer insight.

Spanning verticals, the CISO contributors share real-world use cases and provide guidance.

Participating UBA Solution Providers

The report includes responses to Requests for Information (RFIs) submitted by eight vendors. Developed by CISOs, the RFI criteria highlight the most important technology aspects of the potential solutions.

To qualify, a solution must transcend traditional log monitoring and reporting, and focus on user and entity activities beyond network elements, such as IP addresses.

Participating Companies:

Exabeam
Fortscale
LogRhythm, Inc.
NuData Security
Prelert, Inc.
Securonix
Sqrrl
Varonis

LEAD WRITER:
FirstBank
Greg Schaffer, CISO

HISTORY OF UBA:
GE Capital Americas
James Beeson, CISO

CONTRIBUTORS:
Actian Corporation
David W. Rooker, CISO

Aetna
Kurt Lieber, Global Security IAM Leader

Barclays
Troels Oerting, Group Chief Security Officer

Barclays
Elena Kvochko
CIO, Group Security Function

IBM Cloud & SaaS Operations
David Cass, Global CISO

Levi Strauss & Company
Colin Anderson, CISO

MIAX Options
John J. Masserini, CSO

Oppenheimer & Co. Inc.
Henry Jiang, CISO

RWJBarnabas Health
Hussein Syed, CISO

Surescripts
Paul Calatayud, Former CISO

Note: There was no cost for vendors to submit an RFI for inclusion in this report. A full list of vendors invited to participate can be found in Appendix B.

A CISO LOOKS AT THE HISTORY OF UBA

James Beeson, *Chief Information Security Officer and IT Risk Leader*, GE Capital Americas

A risk-based approach is highly recommended in order to gain some quick wins. Generally, this starts by looking at privileged access to various applications.

UBA AS A DERIVATIVE OF OTHER BEHAVIORAL-BASED TECHNOLOGIES

User Behavior Analytics (UBA) was born in part due to identity and access management's (IAM) inability to provide thorough data analysis. The earlier generation IAM solutions were unable to parse the data effectively across complex networks and provide normalization. As IAM matured, UBA evolved, increasing its ability to provide normalization, and more importantly to identify anomalies.

A great example of the evolution of user behavior analytics comes from the retail space. Initially used for marketing to identify users' interests and spending patterns, it became clear that the intelligence garnered could be utilized for other purposes within the business.

As losses mounted from fraud and abuse, the industry put a focus on and became smart about transaction analysis. A purchase in New York City and then, seconds later, one from Paris, France, is an abnormal spending pattern. The developers of UBA took note of this capability and the opportunity to pinpoint discrepancies, and applied it increasingly to other needs within the business, in particular security and compliance.

Online banking is another fantastic example of how UBA was able to learn from previous challenges. The mid-2000s saw the FFIEC (Federal Financial Institutions Examination Council) require adaptive authentication for online banking transactions.

For example: someone logging into their account may normally check their balances and then transfer funds. However, an attacker may login, edit account records, and wire money. UBA technology alerts generated based on the observation that these are two entirely different behavior patterns is a result of the technology being applied to new challenges.

In its application to the field of enterprise security, UBA uses a similar approach for detecting user access anomalies. For example, when there are multiple 2AM VPN sessions from a foreign land when the employees only arrive at their local office elsewhere and login at 8AM their time, there is a potential issue that needs to be addressed quickly.

UBA QUICK WINS

UBA is what security leaders make of it. There's a tremendous amount of value that can be gained from its implementation, but it also must be implemented methodically and simply or it has the potential to be overwhelming.

A risk-based approach is highly recommended in order to gain some quick wins. Generally, this starts by looking at privileged access to various applications.

There must be good inventory and account provisioning and deprovisioning for this to be effective. With an internal focus on business applications that have privileged access,

ensuring there is a good inventory and that access granting and revoking procedures are mature should be a top priority. An attacker is looking for weakness in this process in order to get in, maintain persistence, and exfiltrate data.

Therefore, one of the first steps should be to conduct a risk assessment and address the greatest risk to the business from an account and application standpoint.

Also, narrowing the scope and developing a solid foundation with a repeatable process is key. It is easy to allow scope creep to impact the success of the project. However, by narrowing the scope, teams will be able to define a process that is sustainable and scalable.

For example, global companies may want to start with North America and address the key privacy and regulatory laws that are most familiar. Then they move forward once there is a solid foundation that can be implemented globally. Too much at once is only going to exacerbate the problem, diminishing the return on security investment due to resource drain and the limits on the ability to execute.

RECOMMENDATIONS TO PEERS

Historically, security investments have been allocated mostly to preventative technologies. In theory, this makes sense, but in reality, these solutions no longer adequately withstand the attacker's ability to compromise companies. The proverbial perimeter has vanished and now the account is essentially the perimeter. This is not to say that perimeter defenses are not needed.

This means that security leaders have realized that they cannot stop it all and need to shift some investment dollars from prevention to detection. Ultimately there should be a formidable process to monitor, detect, and contain threats and that process should be centered on accounts, computers, and sensitive data.

The process should tie back to quick wins and in doing so should lend itself to improving security's agility in monitoring and containing anomalies. To be successful, it is a matter of narrowing the scope to focus on the accounts and applications at greatest risk and for security teams to quickly detect and contain real and potential attacks.

Strive for prevention, but do not get so immersed that the ability to detect and contain is an afterthought. UBA can then broaden beyond users and accounts to machine-to-machine detection for an even more robust and effective incident management program.

WHERE UBA COMPLIMENTS OTHER TECHNOLOGIES

UBA is a compliment to security information and event management (SIEMs) as it identifies anomalies that historically were incapable of being recognized by log or network-based solutions. The SIEM is a valuable and necessary technology in the industry but hasn't had the account-level visibility that allows security teams to detect, respond, and contain as quickly as needed.

It is important to look beyond traditional security technologies and capabilities. There is a lot to be said for the work being done in other fields. For example, the engineering field has invested billions of dollars into complex algorithms that are capable of learning what is normal versus abnormal behavior.

The ability of aeronautical engineers to develop technology that is proficient in determining when a part of a plane is deteriorating and proactively ordering and notifying engineers is a process methodology that UBA can (and should) take a cue from. There is no need to reinvent a practice if these algorithms are competently recognizing and aiding in the triage process. There is tremendous opportunity for security to learn from technologies used in other fields.

AUTOMATION AND UBA OUTLOOK

UBA has the ability to impact automation, especially where there are lower-level tasks that don't require the attention of highly skilled security professionals.

Automation is not likely to be the top priority when implementing UBA, but it is a useful byproduct to augment other areas of the security operation. UBA can help significantly in account provisioning, deprovisioning, and review if there is already a good process in place. Over time as teams become more confident, the ability to take preventive action dynamically is possible through automation.

Again looking outside of the security space, security leaders can learn from other technologies that are already taking advantage of automation.

One area in particular is the call center. There are countless complicated algorithms in place to have agents take calls faster and more efficiently. The same concept can translate to security, and UBA can help pinpoint where some of the more experienced staff are spending their time.

A word of caution: this kind of user behavior based analytics can be seen as invasive oversight (i.e., surveillance) and may raise privacy concerns in some parts of the world. These concerns need to be addressed prior to implementation.

GETTING UBA RIGHT

For starters, the inventory of the systems and accounts must be in good shape or it will not allow teams to benefit from what UBA has to offer. Like many things, without a solid foundation in place, security will not see the gains from the solution that they are expecting to obtain. The old cliché of garbage in, garbage out definitely applies to UBA.

Second, ensure there is the right level of buy-in across the organization. Obtain support from all necessary business units, such as human resources, privacy, legal and risk management. UBA will have deep insight into the company's personnel and their behavior, which means privacy and corresponding policies need to be top-of-mind when rolling out a solution. It is better to be transparent to the team than to appear as an infiltrator.

Third, ensure there is the right level of expertise internally or with trusted partners. This means someone who really understands the space and can take a risk-based approach. Start small and grow a repeatable process.

UBA STAFFING REQUIREMENTS

At the onset of a UBA rollout there is likely going to be a need for additional help in order to get it right. However, over time and through automation, there is certainly opportunity to allocate staff to other areas where they may more wisely spend time on higher value tasks.

UBA can potentially lend itself to a reduction in headcount through attrition where lower-level positions do not need to be replaced. Meanwhile, more senior staff will be able to do more complex duties as opposed to monotonous work.

Also, security leaders need to move away from multi-year projects and move towards an agile or iterative process. The attackers, business, and technology are moving too fast, and so dragging out the implementation over the course of several years is no longer feasible. Again, this is why it is necessary to break up the implementation into smaller projects as opposed to a start-to-finish full implementation.

The SIEM is a valuable and necessary technology in the industry but hasn't had the account-level visibility that allows security teams to detect, respond, and contain as quickly as needed.

SUMMARY

UBA will likely be one of the more valuable additions to the technology stack. Security leaders can learn a lot and potentially apply technologies and processes from other functional areas. UBA is a derivative of other useful behavioral-based technologies that have been in place for over a decade. It is now time for teams to look to UBA as a means to better predict, detect, and contain malicious threats. Start small, build a process, and iterate based on greatest risk to the business.

Technology Overview

Written from CISOs' perspectives, CISOs Investigate: UBA incorporates real-world experience with information gleaned from solution providers' RFI responses to give security decision makers access to unparalleled insight when considering UBA as a component of their overall information protection strategy.

UBA Core Features

While the market is still determining the exact definition of what comprises a UBA solution, two unique features define its core:

- Incorporating user behavior beyond simple login and destination information, expanding to external, non-technology resources.
- Analytics founded on base lining of past behavior to spotlight current and future threats. In other words, rather than looking at each transaction as frozen in time, UAB analyzes information in a way that connects the past (baseline), the present (event) and future (pre-direction).

This is a shift in approach for CISOs using static signature analysis of logs and traffic as the primary source of actionable information for defense.

Because UBA provides insight beyond simple transaction data, examining "what makes sense," unlike port-based and signature-based defenses, it gives security professionals a predictive view into potential future threats. UBA builds upon network intelligence but is not limited by it.

While UBA is an emerging technology in the information security space, analyzing users' behavior has been in use in business for some time.

A Deeper Dive into UBA

UBA provides information outside normal model parameters, which often is actionable. Its implementation options mirror other security controls: deployed on premises as a standalone server, appliance, or VM, in the cloud with a colo service, or subscribed to as part of a Managed Security Provider (MSP) agreement. Although UBA incorporates SIEM elements and integrates with deployed SIEM systems it is not a next generation SIEM.

UBA's most notable differentiator is its predictive nature through its focus on user behaviors. By incorporating human elements, role-based risk scoring, and data from non-technology sources such as performance reviews and business-specific rules, UBA provides information based on calculated risk rankings informed by a real-world knowledge of the environment.

For example, a privilege elevation action by a database administrator might be routine whereas a user in the Finance Department who never has performed such an action might cause an alert to trigger. By examining elements beyond network traffic and log entries, UBA can differentiate between a valid account escalation procedure and a potentially dangerous anomaly.

Key Considerations

UBA AS A PREDICTIVE CONTROL

The incorporation of external elements beyond log entries in risk analysis on a case-by-case basis provides visibility into possible future threats. UBA examines elements that have occurred in the past to make assumptions about the behavior of individuals. UBA compares user events with established baseline norms, incorporating input from a variety of sources. Behavior outside the baselines might be a predictor of an imminent attack.

UBA AS A PASSIVE CONTROL

UBA by itself provides information and does not act on it[1]. However, UBA systems can interface with firewalls and other technology access controls for automated blocking.

UBA AS A RISK ASSESSMENT TOOL

UBA, with its risk-scoring attributes, is part technology, part institutional security policy, part human resources management, and part business acumen. UBA brings a level of business integration and sophistication not seen in previous security controls, aiding in the organization's information security risk assessment process.

UBA REQUIRES A BASELINE

UBA analyzes current activity against a behavior history. Generating this baseline requires time (days to weeks and beyond) to collect data, but some UBA systems import historical data from other systems to begin providing intelligence almost immediately. Like all predicative, data-driven models, the more relevant data points the model has to work with, the more useful it is and accurate it will become.

[1] (ROUSE, 2016)

To Deploy or Not to Deploy

Deciding whether to deploy UBA begins as usual with a clear understanding of the business objectives, the threat environment, existing controls, and UBA's capabilities. For example, UBA can counter the risk and associated losses from internal data exfiltration by an authorized user. However, an organization with a Virtual Desktop Infrastructure (VDI) may see the biggest benefit from the monitoring and modeling of the privileged administrators, who, to do their job, have far greater access than most users.

UBA can provide security teams with an unprecedented view into what is happening within the infrastructure. Learning how it may have helped to eliminate actual breaches in specific market segments and looking at use cases can also aid in the decision process. With this knowledge, the CISO can determine if the business case for UBA makes sense in their organization.

Selling to the C-Suite

CISOs know that while their colleagues in the C-Suite and on the Board of Directors are not interested in the minutia of information security, they want to stay out of the headlines for suffering a breach.

Technology control initiatives like UBA solutions provide value through a focus on reducing the risk of capital loss – be it directly through financial account takeover or future losses from information exfiltration and reputational damage. The value then is in finding the most cost-effective methodology for reducing risks to minimize potential loss.

CISOs can determine how UBA can benefit their organization and the subsequent business case through this crucial, high-level cost/benefit analysis. Consider the following:

- What does the overall threat environment look like relative to the organization's vertical and peers?
- Do existing compensating controls meet the organization's risk tolerance at least as effectively and efficiently as UBA will?
- Does the cost to implement and support UBA exceed its projected benefits?

Addressing these questions requires a deep dive into the organization's current posture by examining potential loss from a security breach, risk management attributes, regulatory and compliance standards, staffing needs, and real-world applications. Many organizations already have a sense of their current risk posture and all that is required is translating that into how UBA can impact the organization. Others will need to undertake all or parts of this deep dive for the first time.

Reducing Potential Losses from a Breach

Predicting the potential loss from a cybersecurity breach is an inexact science at best. Each case is different; every organization places different values on its information based on such characteristics as capital, reputation, intellectual property, and regulatory constraints.

Historical data often provides the best starting point for estimating potential loss. The 2016 average cost per data breach, as reported by the Ponemon Institute, was $4 million[2] based on a survey of 383 companies across 12 countries, a 29% increase over 2013. Predictably, the number of records lost impacted the cost, from $2.1 million for less than 10,000 records to $6.7 million for more than 50,000.

More regulated industries, such as healthcare and finance, face stiffer penalties and fines and should expect higher costs in the event of a breach. If the organization protects intellectual property on behalf of their clients, then the compromise of that intellectual property can result in the loss of that business.

UBA can aid in mitigating potential losses regardless of industry. While UBA does not provide significant data discovery and inventory capabilities, as both a preventive and detective control, it potentially lowers the cost of a breach. Because of its predictive nature, UBA has the ability to discover quickly anomalous behavior, potentially staving off an attack. As well, by automating these investigative functions, traditionally carried out by security analysts, UBA potentially significantly shortens the time to breach discovery and subsequent mitigation. It also has been shown to reduce the number of false positives allowing organizations to focus on true threats.

UBA's Role in the Defense-in-Depth Approach

By tracking and alerting on user behavior, UBA directly mitigates the high risk associated with the number of individuals who have access to records. Both its predictive capabilities and its ability to import information such as performance evaluations and roles, enhances the CISO's understanding of the evolving internal threat environment.

UBA contributes to the defense-in-depth approach to information security. UBA complements, enhances, and / or replaces the function of some existing controls, both internal and external, such as SIEM and data loss prevention (DLP). UBA can mitigate cloud-based security risks by accepting cloud access data for analysis and reporting on it. In the case of a breach, UBA can provide actionable intelligence on a user's behavior as part of the necessary information gathering in incident response.

Because UBA provides detailed information on the risks associated with user behavior, it can help determine and measure adherence to the risk tolerance of the organization. In that sense, where an organization has developed a mature UBA system, that system is an integral part of the organization's risk management program.

[2] (IBM AND PONEMON INSTITUTE, 2016)

Maintaining Compliance through UBA

A successful layered security strategy meets the cybersecurity requirements of various regulations and standards. Measuring that success involves examining effectiveness of the compensating controls deployed in the environment and how they map to regulatory requirements.

While compliance does not equal security, a properly designed and implemented information security management system should achieve the compliance requirements of cybersecurity regulations and standards that are relevant to the organization. UBA fits well into that strategy.

REGULATION / STANDARD	CONTROL REQUIREMENT	USER BEHAVIOR ANALYTICS
GLBA	501 (b) - Protect against unauthorized access or use of such or records or information which could result in substantial harm or inconvenience to any customer	Monitoring of user behavior to ensure proper access and use of customer Nonpublic Information and other confidential financial information
HIPAA	Security Rule - Administrative Safeguards - Access to EPHI must be restricted to only those employees who have a need for it to complete their job function	Monitoring access rights and changes to files containing EPHI to ensure patient record confidentiality and integrity
SOX	Section 404 - Assess both the design and operating effectiveness of access controls	Ensure access is limited to authorized users for authorized business and that separation of duties is maintained by examining behavior of access against peers and role requirements
PCI	Regularly monitor and test networks - track and monitor all access to network resources and cardholder data	Construct baselines of user access behavior based on authorized actions and monitor for deviations to the baseline
NIST 800-53 REV 4	AC-3 - Access Enforcement - Determine if the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	Analyzes and reports on user access to information systems and alerts on significant changes in access activities

ISO 27001-2013	A.6.1.2 - Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets	Monitors and reports on violations of organizational-defined information system separation of duties
ISO 27001-2013	A.12.4.1 - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed	Provides a detailed log of user activities
FACTA	Red Flag Rule - Implement reasonable policies and procedures for detecting, preventing, and mitigating identity theft	Analyzes new and existing accounts at financial institutions to detect variations in usual customer behavior that may indicate identity theft
FERPA	Conditions under which student records may be released	Monitors employee access to and manipulation of student electronic records
NIST Cybersecurity Framework	PR.AC-4 - Access permissions are managed, incorporating the principles of least privilege and separation of duties	Ensures proper management of access permissions through analysis of access events
FFIEC Cybersecurity Assessment Tool	D3.PC.Am.B.1 - Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege	Ensures actual employee access behavior conforms to established policies and baselines

For a more comprehensive list of regulations, see Appendix A.

Staffing Implications

Since UBA can run in-house, in the cloud or as part of a managed security service, it is incredibly flexible in terms of staffing needs.

Because it analyzes user and entity activity, it stands to reason the larger the organization, the more staff needed to effectively manage UBA. This relationship does not scale linearly, however. Moreover, depending on what existing controls it may replace, UBA's automation features could result in a net-net impact on staffing or even reduce analyst-staffing requirements. Unlike human analysts who are looking for the proverbial needle in the haystack, UBA provides automated identification of anomalies enabling the analysts to focus on actual threats. Still, it follows that more information could reasonably incur more interaction from Human Resources and other departments.

Therefore, it is difficult to create a single staffing model that addresses all situations but taking into account the following variables can help provide an estimate of staffing requirements.

- Managed Security Provider - Third party installs, configures, administers, and manages UBA, providing only alerts to the organization.
- Managed In-House/Cloud Hosted - The organization manages the server and application within their environment or within a cloud environment.
- Replaces Existing Control(s) - Another control system (an in-house analytics process for example) is decommissioned when UBA is implemented.
- Number of Employees - Provides for a non-linear increase in staff needs (analyst and other) for investigating alerts.
- Corporate Risk Tolerance - On a scale of 1-5, where 1 is the most risk (high) tolerant, 5 is the lowest risk tolerant.

Actual staffing needs will be based on an organization's unique attributes. Keep in mind that the effectiveness and predictive nature of a UBA solution may free up staffing resources who traditionally may have been investigating false positives and/or involved in incident response.

When UBA May Have Stopped Real World Breaches

Analyzing user behavior may have prevented the following recent breaches across several industries.

HEALTHCARE

Large Public Health Authority – An employee emailed PHI without authorization, exposing 91,000 records. The employee exchanged emails with her brother for nearly two years, seeking technical assistance with spreadsheets containing the information. UBA incorporating email traffic analysis could have triggered an alert on the anomalous email actions of the employee. http://www.seattletimes.com/seattle-news/health/91000-state-medicaid-clients-warned-of-data-breach/

HUMAN RESOURCES

Payroll Provider – Criminals stole payroll and other confidential information from corporate clients by creating false accounts in the employees' names. UBA may have triggered an alert regarding the activation and use of such accounts. http://krebsonsecurity.com/2016/05/fraudsters-steal-tax-salary-data-from-adp/

RETAIL

Retail Pharmacy – A pharmacy technician stole data on approximately 100 customers for purpose of fraudulently obtaining credit and credit cards over a period of two years. The employee periodically and without authorization printed customer personal information when processing incoming prescriptions. UBA may have identified this activity by comparing the employee's printing activities to a baseline of activity for that employee and others with the same responsibilities. http://www.sandiegouniontribune.com/news/2015/jul/17/pharmacy-patient-data/

FINANCE

Regional Credit Union – An employee used their authorized access to view accounts beyond the scope of their duties. Through analysis of baseline and current account activity, UBA may have alerted security analysts to the snooping. http://www.databreaches.net/golden-1-credit-union-notifying-customers-after-insider-wrongdoing/

GOVERNMENT

A terminated employee accidentally downloaded to their personal USB drive confidential information of 44,000 FDIC customers. The agency did detect the transfer of information to the USB drive after the fact, but UBA may have alerted at the time of drive attachment and before the download occurred, if connecting a drive fell outside this user's normal activity. https://www.washingtonpost.com/news/powerpost/wp/2016/04/11/inadvertent-cyber-breach-hits-44000-fdic-customers/

Could other controls have possibly prevented these breaches? Yes. But these attacks occurred because authorized accounts were either intentionally or unintentionally abused for their access to information.

Beyond Security: Other Business Cases for UBA

Use cases across multiple industries highlight additional business benefits of examining user behavior:

HEALTHCARE

Pharmaceutical facilities use UBA to identify discrepancies in a drug inventories, preventing unauthorized dispersal or use of medication and potentially saving lives.

ENTERTAINMENT

Sports management companies use UBA to provide confidence in allowing vendors and system administrators to work remotely while ensuring security and audit capabilities, allowing the businesses to focus on staging competitive events.

FINANCE

Financial services companies use UBA to identify suspected violations of Anti-Money Laundering rules and comply with other Bank Secrecy Act (BSA) provisions by monitoring BSA-related IT control effectiveness and providing related reporting.

TECHNOLOGY

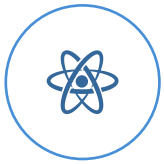
Technology services companies leverage UBA's visibility into application usage resulting in improved worker productivity, increased awareness of suspicious user actions, and easier audits and investigations of incidents.

RETAIL

Merchants use UBA to ensure the protection of their customers' information by monitoring and alerting on access to Point of Sale (POS) systems.

MANUFACTURING

Food and beverage manufacturers leverage UBA to meet requirements to monitor and audit vendor access, and enhance incident response capabilities.



CRITICAL INFRASTRUCTURE

Energy companies use UBA to secure their critical infrastructure by providing forensic-level visibility into the network and profiling users' access to servers and other network resources.

LEGAL

Law firms use UBA to protect intellectual property of top-tier companies and maintain attorney-client privilege.

Market Assessment

As CISOs continue to adopt UBA, the capabilities of third-party solutions become more standardized. However, not all solutions are equal. Implementing a solution that falls short of its intended use at the very least impedes the CISO's mission to secure the enterprise. The vendor RFI was designed to inform CISO expectations. Eight vendors completed the RFI, providing valuable insight into the solution provider space. The RFI covered many aspects beyond the technology solution itself, to include:

- Company Information
- Customer Background
- Product Overview
- Product Roadmap and Development
- Product System Attributes
- Set Up, Administration, and Reporting
- Additional Information

The complete RFI responses with detailed answers to each section are available in Appendix C.

A high-level review of the aggregate responses provide a snapshot of the vendors and their UBA products:

- **No Acquisition**: All of the vendors developed solutions in house as opposed to obtained through a merger or acquisition.
- **Company Age**: Approximately half of the vendors came into existence within the last five years.
- **Varying Sizes**: The vendor employee base is either below 100 or above 500 associates.
- **All on Site**: All of the vendor platforms provide on premises solutions.
- **Less in the Cloud**: Slightly more than half support a cloud-based implementation, and slightly fewer than half provide or support Software as a Service (SaaS) deployments.
- **At Rest**: Most (87.5%) incorporate a RESTful API to allow for the incorporation of custom data feeds and logs.

In addition, all of the vendors support input from a multitude of sources, including CSV and other formats, to calculate inherent risk baselines, suggesting that at least on a limited scale no data source is off-limits.

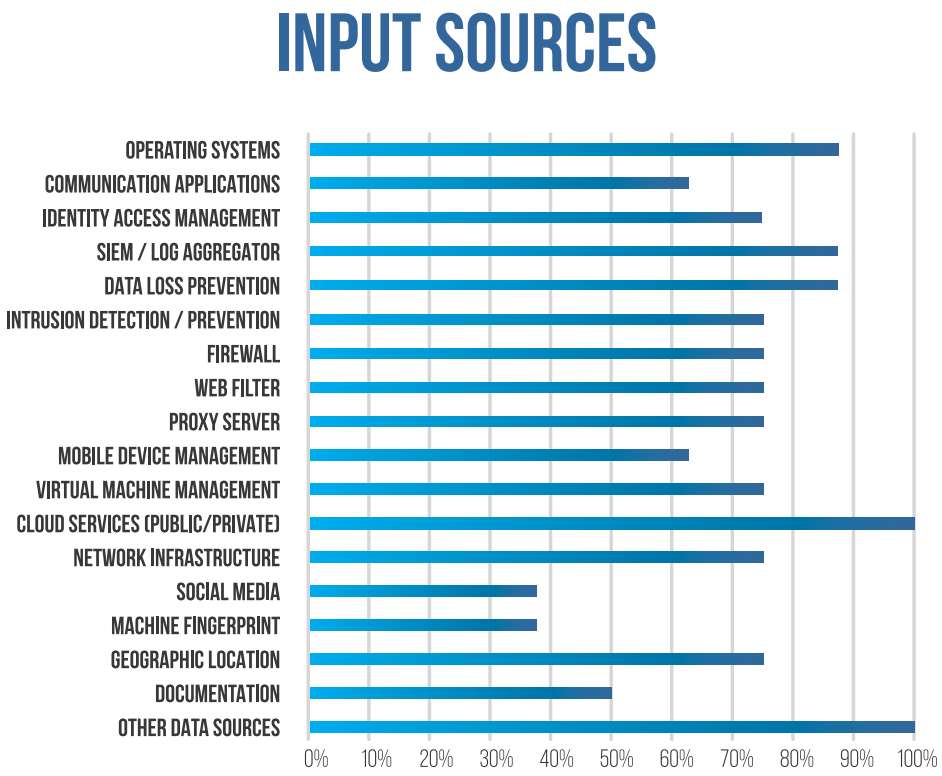


Figure 1: *Sources of inputs for UBA systems from RFI responses.*

Most offerings incorporate feeds from SIEM systems, an expected feature given the close relationship UBA has with SIEM solutions. They also accept input from other sources, such as operating systems, data loss prevention systems, and firewalls, as shown in figure 1.

Not as many solutions allow for higher-level behavioral data sources such as social media. This is somewhat surprising as 84% of companies who responded to a 2015 survey on the use of social media for talent acquisition leveraged social media for recruiting[3]. It logically follows that since social media presence has found such prominence in pre-employment screening, the importance of social media monitoring does not diminish after filling the position. Expect these data points to be pulled increasingly into the analysis.

[3] (SOCIETY FOR HUMAN RESOURCE MANAGEMENT, 2016)

DASHBOARD FEATURES

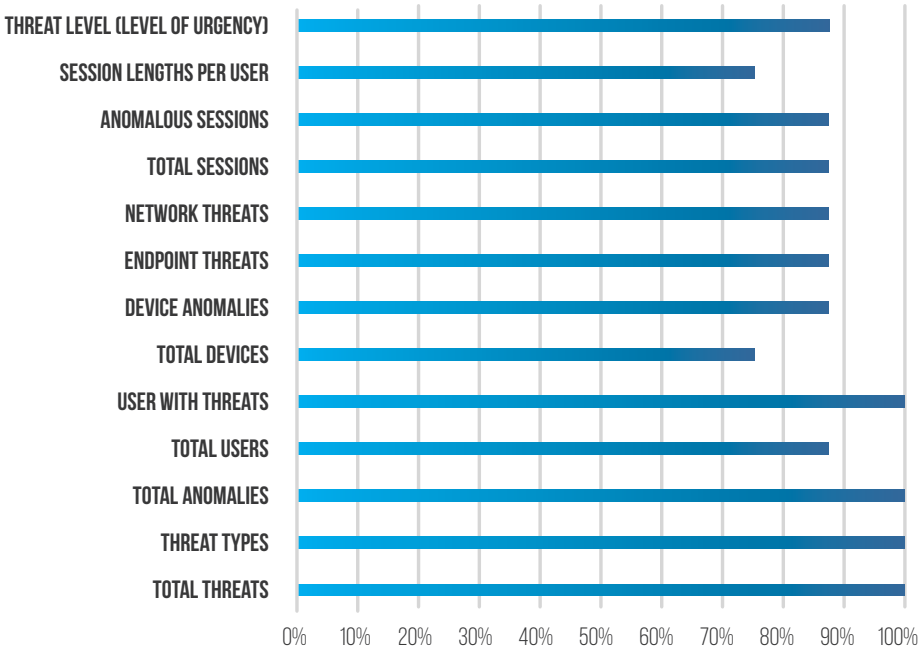


Figure 2: *Information available on UBA system dashboards from RFI responses.*

Most solution providers offer a wide variety of visibility into threats via dashboards. All also integrate with other dashboards to provide single pane of glass representation. Many solution providers offer customized reports geared toward administrators, CISOs, the C-Suite, and the Board of Directors. Some metrics and examples of their relevancy when compared to baselines include:

ADMINISTRATORS:

- **Top suspicious users by access protocol (VPN, SSH, etc.)** – to determine access behavior inconsistent with role, business need, or previous history.
- **Remote connection data transfer volume** – can identify users or user accounts exfiltrating corporate information.
- **Login location** – to identify patterns or impossibility of geographic access points.

CISOs:

- **Most accessed systems** – changes in the access frequency of systems may identify a high-risk user or event.
- **Risky users** – specific metrics on those users that may pose a significant risk to the organization based on confidential parameters.

C-SUITE AND BOARD OF DIRECTORS:

- **Aggregated user information security risk** – a snapshot of the riskiest users by department, location, and role is an input to strategic decisions.
- **Risk to the company's high-value assets** – measure whether actual risks to the company's "crown jewels" agree with stated corporate risk tolerances.

These customized reports are available in a wide variety of formats, from printed output to real-time dashboards. They may be customized for content and date ranges to provide the targeted information required. Delivering the correct metrics in an easily digestible format, regardless of role, permits proper and timely action on information security risks.

Key Takeaways

One may draw many conclusions and observations from analyzing the various aspects and applications of UBA, its features, uses, and case studies. Three stand out regardless of the organization's attributes:

First Takeaway – A Win-Win for CISOs

UBA use can result in more efficient allocation of scarce information security resources

The U.S. Bureau of Labor Statistics projects the demand for information security analysts to remain high through at least 2024[4] despite the stress of demands placed on them.

The volume of false positives alone generated by SIEM systems today frustrates information security analysts[5] as each alert must be examined. Chasing red herrings is an inefficient use of scarce analyst resources. The inability to find sufficient qualified information security staff impacts innovation as businesses struggle to achieve and maintain a competitive advantage. Without sufficient competent staff to help them keep those activities secure, they have a choice of slowing down or taking on unnecessary increased risk[6].

There also is the natural human tendency to introduce errors. Whether missing an important data point while parsing alerts or not "connecting the dots" between related events, manual analysis can overlook critical opportunities for threat identification while providing a false sense of security.

Automation of the analysis of user behavior information via UBA:

- Maximizes security operations through more efficient use of resources, thereby narrowing the gap between supply and demand of information security analysts.
- Enhances secure use of the Internet and other technologies to maintain a competitive advantage.
- Reduces human-introduced errors in the behavior analysis.

UBA can also provide a complete view of an incident. The efficiency of a well-designed interface focusing on threat information and workflow gives the organization more of the most valuable resource in incident response – time.

[4] (U.S. BUREAU OF LABOR STATISTICS, 2016)
[5] (LEMOS, 2016)
[6] (INFORMATION SECURITY FORUM LIMITED, 2015)

While decreasing over the past few years, in 2015 the median number of days from breach to detection was still quite high at 146[7]. By quickly providing actionable intelligence, CISOs and their staff can reduce loss to the organization by identifying and thwarting an attack earlier.

The Bottom Line - Deployed and managed properly, UBA offers focused, actionable information while maximizing staff resources due to the automation of analytical functions, providing a potential win-win for CISOs.

By quickly providing actionable intelligence, CISOs and their staff can reduce loss to the organization by identifying and thwarting an attack earlier.

[7] (MANDIANT CONSULTING, 2016)

Second Takeaway – Effective Across Industries

UBA use is not limited to certain industries

UBA is industry agnostic. Whereas UBA technology first evolved, in areas such as credit scoring, to determine credit worthiness and consumer marketing to track and predict consumer-buying habits, its benefits have now translated across industries to further business objectives. It is natural that information security has adopted UBA technology, given the enormous data available for user analysis.

The UBA solutions providers report customers from a wide array of verticals. While banking, finance, and healthcare were early adopters of UBA, other industries such as transportation, education, and government appear to be increasingly leveraging UBA. The sampling of customers suggests no single industry is dominating UBA adoption.

The Bottom Line - CISOs, regardless of what market they serve, may consider UBA implementation, as its deployment is not limited to specific sectors.

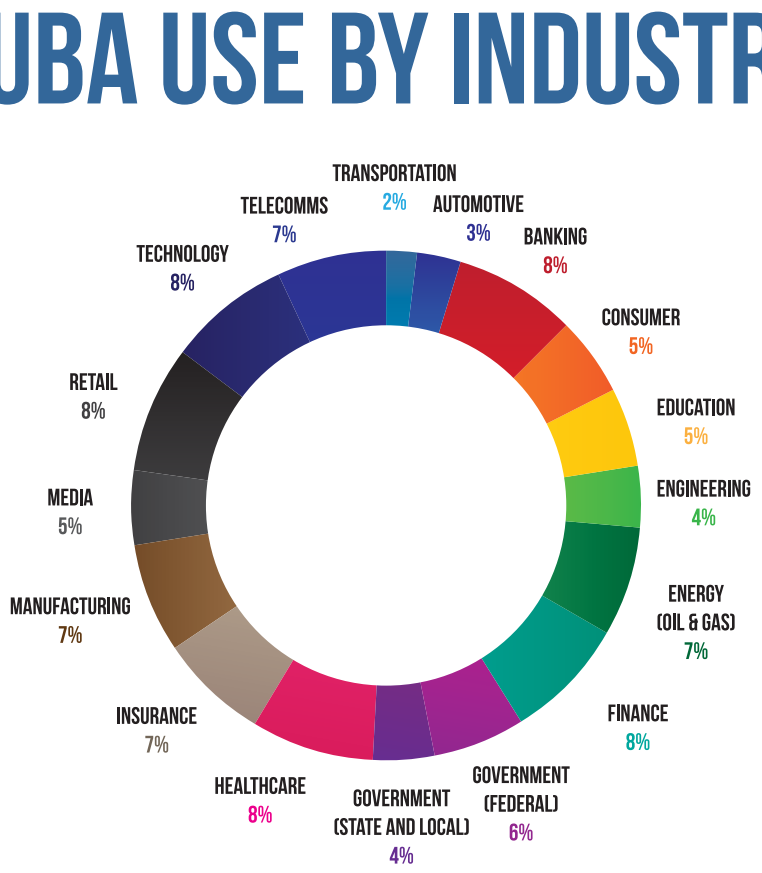


Figure 3: *Industry distribution of UBA customers of vendors who responded to the RFI*

Third Takeaway – A Natural Fit for Risk-based Security

UBA builds on the risk management approach to information security, aiding in compliance as well

An often-quoted truth is meeting regulatory and standards compliance alone does not equal security. Achieving compliance represents ensuring certain controls are effective at a specific snapshot in time, whereas a risk management based information security program identifies and prioritizes mitigation of the most serious risks to corporate data.

Compliance should follow naturally in such a program.

Figure 4: *Percentage of respondents who incorporate risk analysis attributes into their UBA application*

Many enterprises have adopted an information security risk management framework, be it industry-agnostic such as ISO 27005 and NIST 800-39 or frameworks specific to particular verticals such as the Health Information Trust Alliance (HITRUST) in healthcare and FFIEC in banking.

UBA, with its risk-based analysis and scoring, fits naturally into a holistic risk-based information security strategy. The majority of the vendors' UBA products emphasize risk elements, as shown in figure 4. By recognizing that not all users have equal inherent risk, for example, the products prioritize the analysis from the beginning, thus eliminating the reliance on human interpretation of one-size-fits-all output.

Most of the solution providers reported that they offer customization by incorporating business rules into their UBA systems to address organization-specific use cases. Furthermore, the capability to input other risk-influencing data, such as performance evaluation scores, maximizes high-risk action identification.

The Bottom Line - Applying a risk management approach to information security not only helps the CISO meet compliance objectives, it enhances the overall security posture of the organization. UBA supports that strategy.

Sustainability

The question needs asking – how sustainable is this technology? While information security is an ever-changing discipline, a few risks have existed for some time and show no signs of fading:

- The threat environment will evolve rapidly.
- Users will lose control of credentials be it through phishing, poor password construction, or hacked sites exposing passwords, leading to account takeovers.
- Passwords, despite their tendency to introduce weakness, are not going away any time soon (although multifactor authentication use will continue to increase[8]).
- Insiders will fall to temptation and steal company intellectual property for personal gain.

All suggest the need for analyzing user behavior will not only continue but likely will increase. Thus, UBA vendors will probably continue, to develop and expand their product's capabilities, and more organizations will investigate and deploy UBA as part of a layered protection scheme.

Expansion of input sources will likely, continue as well, particularly those indirectly associated with system access logging and other traditional information technology controls. Expect further analysis of social media and other Internet posting use in particular to expand. In addition, with an increase of private cloud adoption from 63% (2014) to 77% (2015) and with 96% of enterprises using cloud resources in some form in 2015[9], the capability to analyze employee cloud use should increase as well.

CISOs who contributed to this report agree the UBA market will continue to mature. Technology adoption maps to the innovation adoption lifecycle, a normal distribution known as a Rogers' bell curve[10].

Today, UBA technology appears to fall between the Early Adopters and Early Majority at approximately 16% into the lifecycle. That suggests UBA will remain a viable and useful technology for quite some time.

[8] (REINER, 2016)
[9] (RIGHTSCALE, 2016)
[10] (ROGERS & SHOEMAKER, 1971)

INNOVATION ADOPTION LIFECYCLE

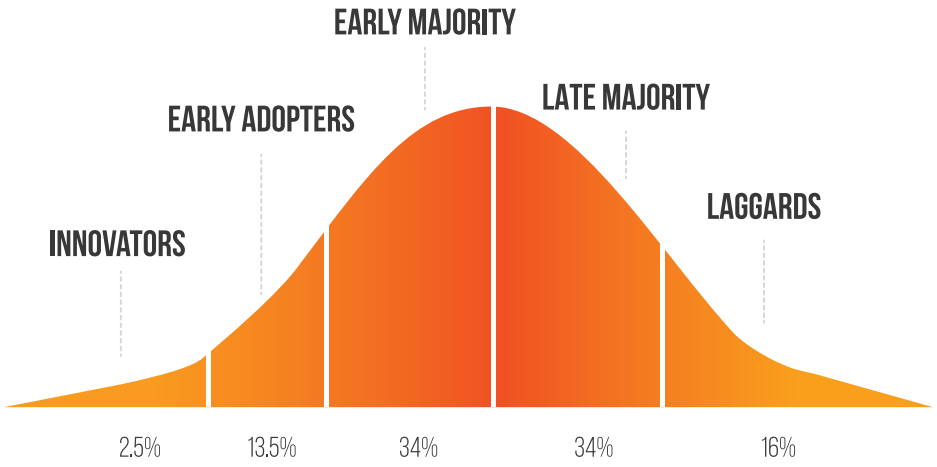


Figure 6: *Innovation Adoption Lifecycle (Rogers & Shoemaker, 1971)*

Perceived need supports that conclusion as prediction technologies supplant detection methods[11]. What results is greater security staff efficiency and greater visibility into threats. That need will continue to exist, driving sophisticated analytic technology solution development.

Other risk management-based information security tools will emerge and gain traction as companies continue to adopt a more risk-based approach to program management. For example, an Infrastructure Behavior Analysis (IBA) system combining the inherent risk of the use of a fiber optic circuit with the behavior change of a local utility company (digging nearby as alerted by the local "Call Before You Dig" system) could alert a network administrator to the increased possibility of a service interruption by a backhoe cut. The network administrator could then proactively reroute traffic away from that fiber optic cable until the IBA system reports a return to a reduced risk state following work completion.

Another example is a network administrator mistakenly performing an incorrect router configuration change. An IBA system could detect and alert on the anomaly of the request before implementing the update, averting an interruption in service. There may be numerous applications of analytics in disaster recovery to enhance business continuity.

[11] (ARMERDING, 2016)

When UBA Doesn't Work

Implementing a UBA solution successfully is highly dependent on the hygiene of the data fed into the models. Unlike the historical deployment of signature-based Intrusion Prevention Systems (IPS), UBA leverages machine-learning capabilities driven by complex modeling algorithms to identify the initial user baselines.

Most leading UBA solutions rely heavily on a fairly clean user directory that has some degree of role definition associated with it. If the directory, which defines the user population and roles throughout the organization, is polluted, the models will build invalid baselines to be used in future decision making processes. Because of this, there is often a degree of false positives during the initial deployment in organizations that have not invested in ensuring the internal user identity system is clean and structured.

Additionally, most UBA solutions leverage system logs from critical infrastructure devices as the method of monitoring activity. While the suggested deployment for most solutions is to leverage the log collection of the organization's SIEM, there are times when such logs are not available to the security teams. An inventory of critical logs is often necessary to ensure adequate modeling occurs of the users activities.

Finally, UBA solutions could potentially run against various international privacy laws. Ensuring legal council is actively engaged in the decision process to validate any discovery and privacy requirements is critical from the beginning. Organizations should consult their legal department prior to UBA implementation as to the potential impact, if any, of an increase in discovery scope and records retention requirements.

Summary

Visibility into user behavior elements is a potential game changer in how CISOs manage one of the greatest risks to information security – the user credential. UBA, as a predictive tool, focuses attention on the highest risk areas, allowing for proactive management of information security.

While on the surface UBA appears as a technology control, its behavioral analysis positions it as much more. It's reactive, detective, predictive, and passive control features provide enhanced opportunities and touch points for protecting information.

By examining potential loss, risk management considerations, compliance needs and staffing requirements in a highly competitive arena, the CISO can construct an accurate business case for UBA as it pertains to their organization. That business case can be measured against actual use cases, such as those breaches that may have been prevented through UBA implementation as well as actual case studies of UBA use from CISOs who have considered and deployed UBA.

Investigating and analyzing the market fuels a CISO's understanding of what is available in the market today and what may be coming in the future. Even if the CISO determines a fit for UBA in their holistic layered security plan, understanding the market is the second-to-last step in selecting a UBA vendor. The last step is cost, and that may be measured against the potential loss and the company's risk tolerance to make the final decision whether to implement the chosen UBA product.

In the end, the CISO has the information necessary to construct and validate the case for or against UBA. A well-informed decision is the best decision.

CISO CONTRIBUTIONS

ACTIAN CORPORATION

David W. Rooker
Chief Information Security Officer

COMPANY OVERVIEW

Actian Corporation enables organizations to transform big data into business value with data management and integration solutions to transact, analyze, and take automated action across their business operations. Corporate headquarters for Actian are in Palo Alto, CA, with additional offices in the United Kingdom, France, Amsterdam, Brazil, Australia, and Germany. Founded in 2005, Actian's specialization is in data integration, data management, and integration, and has over 10,000 customers worldwide.

WHY SECURITY LEADERS SHOULD CONSIDER UBA

Our investigation into UBA has shown that UBA provides the level of employee insight that is often not as granularly available with other network-based or SIEM solutions. Security leaders have, and will continue to cover endpoints as thoroughly as possible and also deploy network-based controls, even as the perimeter continues to erode.

However, advanced threats seek to find their way into the business through employees and UBA has shown that it helps to uncover anomalous behavior patterns that go unseen by other solutions. Or if they are seen, may be buried in hard-to-extract reports. UBA's ability to baseline and profile employees and alert on possible account compromise is a big addition to the arsenal of security solutions.

Another consideration, which is important for Actian, is the ability to provide employees a level of access that is within risk tolerance and that does not take a binary, block all or allow all approach. What this does is enable the business to still conduct a portion of their responsibilities within an acceptable tolerance level. Of course if the behavior is egregious, then the solution can and should invoke more drastic measures while the incident response team follows up on the questionable activity.

Third, UBA can provide security teams with the ability to automate tasks that are typically mundane, but necessary. Provisioning, deprovisioning, and access review must be done, but they consume resources and take time away from other value-add responsibilities. This is crucial in a day and age where information security professionals are hard to find and retain. Allowing the team more freedom to focus on what is more important is desperately needed and is what employees would prefer to do.

UBA TECHNOLOGY AREAS OF CAUTION

As with any technology solution, especially those that are newer on the market, false positives are a concern. False positives for UBA could lead to some business impact if there is a hard stance taken on certain activity. Certainly this will not go over well with business leaders if employees are negatively impacted. Likewise, there is an element of true negatives, which also must acquire a keen eye.

What is advantageous about UBA is the apparent unprecedented level of insight into employee account profiles. However, privacy is worthy of caution with UBA and should be dealt with from the outset. This is especially true for European countries where privacy regulations often differ from those in the United States and other countries. Security leaders should expect to work with their privacy and legal teams to include language in the acceptable use policy to ensure it is applicable when the system is in production.

COMPENSATING CONTROLS WITH UBA

SIEMs have their necessary place in the technology stack and they have been heavily invested in and will continue to be used. Depending on the maturity of an organization and ability to parse the data extrapolated a SIEM may suffice.

However, UBA reaches some areas where SIEMs do not have granular visibility, which is important to Actian. Not surprisingly, some leading SIEM vendors are either acquiring or enhancing their solutions with pure or UBA-like technology to incorporate this granularity.

Other compensating controls that complement UBA's ability to profile employees are in the deceptive technology space. The greatest risk to an attacker is what they don't know. This is what can expose them sooner than later if they trigger an alert, especially on a decoy.

With phishing a significant risk to every business, adding TTP (Targeted Threat Protection) technology is essential in safeguarding against an account compromise. Factor this in with regular phishing scenarios and it elevates the employees level of sophistication in defending against email attacks at the user level and further protecting the infrastructure.

UBA POTENTIAL USE CASES

Given UBA's profiling capabilities, baselining employee behavior that leads up to a leak is critical. The leak can be intentional or unintentional, but

regardless is tied to a potential loss of intellectual property. For some CISOs, this is their customer's data (SSN, credit card numbers), while for others this may be their company's software, which is their business value and what allows it to be profitable in the first place.

For Actian, the ability to monitor employee behavior, especially those who work directly with the intellectual property, will be a crucial baseline to help predict when an employee is on the verge, whether intentional or not, of causing harm to the business.

It can be two-fold; employees trying to do the right thing, but fall prey to an attacker, and employees who are intentionally seeking to harm the company. Both are key requirements to profile in the business use case. Again, privacy mandates are a top concern that must be addressed to support the former.

KEY CRITERIA TO REQUIRE WHEN CHOOSING UBA

For starters, for Actian it is important that there will be a low signal to noise ratio. The solution cannot be so overly cautious about missing an event that it reports all anomalous behavior as risky. Instead the solution would need to evaluate the behavior's potential impact.

If the behavior involves less sensitive resources, then it should receive a low impact score. Contrary, if it involves sensitive information like Personally Identifiable Information (PII) or HIPAA-based data, it should receive a higher impact score.

All of this sounds simple, but it is important that this is taken into account while conducting a proof of concept. If it is not a CISO may later find out that these abilities are not where they'd like them to be.

Ease of use is also a must-have. Historically many solutions have been great at collecting data, but terrible at reporting. Security teams must be able to come up to speed quickly and extract valuable data in reports that is comprehensive and easy to interpret.

Out-of-the-box quick wins must be achievable or the solution runs risk of minimal value. For example, an employee out of office on vacation that all of the sudden has activity from a VPN connection from a foreign land will be escalated to the security operations center.

Likewise, an employee who has never accessed payroll information is trying to connect to restricted shares, should now be easily identified. If these behaviors are not easily identifiable, then this is the wrong vendor and it is time to look to another.

The UBA space has a lot of vendors all trying to make a name for themselves in a somewhat crowded area. It is important to look at the vendor's reputation and their underlying technology. Is their solution built on a solid scalable foundation, or was it cobbled together and not scalable for today's and tomorrow's big data analytic needs? Scale, ease of use, and automation should be on the criteria shortlist.

UBA STAFFING REQUIREMENTS

When investigating UBA we assessed that it could potentially assist with positions that have been hard to fill due to challenges in hiring and retention. It could do this by automating some analyst functions where possible to allow some employees to move to positions where they can better use their time.

For example, senior security professionals strive to become more efficient. Typically, security winds up taking on more due to business needs and does not shed responsibilities. However, UBA can assume many of the mundane tasks and subsequently reduce the need for experienced security staff to work on lesser value requirements, allowing them to do higher value work.

In the CISO community conversations are often had about the dire need to automate more in order to keep pace with business needs and attacker threats. There simply just are not enough qualified security professionals to go around and that is not going to change anytime soon. Thus, automation is crucial and will be a top priority. UBA helps with this.

In our assessment, the headcount for UBA should not require additional employees. At the onset, a few people may realign to help implement UBA effectively, but once the solution is in place and operating, as it should, the staff could then focus on other higher value-add duties.

In fact, a successful UBA implementation should be able to allocate more advanced responsibilities to senior employees for work that has not been able to get done because the team is too distracted with tasks that can be automated but have not yet been.

TIMELINE TO EVALUATE UBA

UBA technology is on Actian's roadmap for 2017. There has been enough progress in the industry and enough value produced that the time is right to act on procurement. For security leaders who are in their 2017 budgetary planning and who have UBA as a consideration, it would be a technology worthwhile to budget, and subsequently PoC. The expectation should be that that within no more than 90-days, the solution would be fully implemented.

SUMMARY

Insider threats show no signs of slowing down, and the ability to profile and ultimately predict based on behavior is becoming more and more valuable and viable for security leaders. UBA is augmenting areas where historically security solutions have not provided, easily, granular insight.

It is one of the technologies that can be a real differentiator in the technology stack. UBA changes the landscape and provides automation and relief to some of the strain felt by security teams trying to keep up with the pace in the industry and the demand for qualified security talent.

AETNA

Kurt Lieber
Global Security IAM Leader

COMPANY OVERVIEW

Aetna was founded in 1853 in Hartford, CT, has more than 49,500 employees. The company focus is on providing individuals, employers, health care professionals, producers and others with innovative benefits, products, and services. Aetna services about 46 million people who look to the company for support in healthcare and spending needs. Plans cover medical (22.99 million members), pharmacy (15.24 million members), and dental (14.3 million members) as well as life and disability. Additionally, Aetna provides Medicaid services, medical management, and behavioral health programs. Aetna has an extensive network of about 1.1 million health care professionals, and more than 689,700 primary care doctors and specialists throughout 5,697 hospitals. Aetna's 2015 annual revenue was about $60.3 billion.

BUSINESS USE CASES

The healthcare industry is heavily targeted by cybercriminals. Attackers know that healthcare information systems are comprised of medical records and patient information, medical devices, and even payment information, all of which need protecting. There's a significant amount that is attractive to attackers and Aetna quickly evaluated UBA when it came onto the market.

The main use case for Aetna continues to be the early detection of inappropriate use of enterprise credentials, which is one of the key things attackers seek. An attacker will eventually find their way in, that's almost certain. However, security teams need to disrupt the attacker's mission once they have compromised an account.

A second use case for Aetna, which is closely aligned to the detection of credential misuse, is preventing a breach. Both of these go hand-in-hand. Once the attacker gets in and is logged on with a privileged account, they'll move "east-west" and attempt to exfiltrate data. UBA aids in identifying accounts with suspicious activity that have accessed resources in ways that are not in line with the user's normal behavior.

Third, Aetna's UBA deployment is a very nice compliment to the privileged identity management (PIM) solution deployed. The controls for PIM are robust, but UBA's ability to look at behavior is the addition to the security suite that gives Aetna added detection of anomalous activity.

THE TECHNOLOGY ENVIRONMENT WITH UBA

Many in the industry look to UBA as simply a detective control. However, Aetna has taken a different approach and uses UBA as a preventative control as well (through early detection misuse). Aetna's UBA deployment is in front of the applications. What this means is that when an employee accesses an application, the solution will evaluate the employee's risk score, which is an assessment of events that have occurred up to the point where the user attempted to access the application. If the profile and request is within the acceptable risk parameters, access is granted.

This analysis is still performed even if the credentials used are correct. The risk score takes into consideration the user's profile, their level of access, and recent behavior, to make a real-time decision as to whether the user can have access to the application. It is possible the user will be presented with two-factor or knowledge-based authentication in order to continue to have access to resources. But assuming the credentials and the employee's access is acceptable, the user will gain the requested access.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

Aetna has been able to get through the churn of data analysis much better due to how UBA has been deployed from a preventative standpoint. The detection approach created significantly more data to go through based on the events, which were created. However, preventative-wise, this allows Aetna to control access through escalation.

By escalating authentication, it permits business to continue and if there are additional failures along the way then the account is not granted access; thus the prevention. This is preventative approach works well for Aetna. Without this there would be many detection-based events that analysts would have to review. One word of caution to the prevention approach is to ensure UBA does not become a bottleneck to the business. Because the access still follows the user's approved authorization, and that approval follows a "least necessary" access model, this control supports Aetna's "least necessary" access model.

Another technical achievement that Aetna now has is through correlation of physical and logical access. Prior to UBA, these system log events were not correlated. For example, badge reader logs are sent to UBA as well as all VPN logs. If logs show that an employee badged in at headquarters at 8AM and then 5-minutes later there is an attempted VPN connection from an IP address in a foreign country, there is an obvious, alarming anomaly. The decision can be made to prevent this access and the case quickly can be escalated for additional investigation.

Lastly, UBA provides capability that can assess access from users outside the workforce. For Aetna, this would be customers and their activity to verify that it is truly them. There are obvious concerns about scalability, but it is certainly capable of providing insight into anomalous behavior occurring from external accounts.

BUSINESS GOAL IMPLEMENTING UBA

In the year that UBA has been in production, it has helped Aetna accomplish a couple of key business goals. With security often thought of as an inhibitor, it was important for the Aetna security team to not impede the business, but at the same time, provide a high degree of security.

One example is that Aetna has tiered all of the users and applications based on risk. If an employee is attempting to access a very low risk application that they don't have access to, the system can dynamically grant the employee access within seconds. If the user risk is low and the application risk is low, even if they did not have access to begin with, the system can provide it to them.

Prior to UBA, the employee would be denied access, required to fill out a ticket to get access, and then go through the approval process, and finally provisioned by an administrator. The entire process could take days or weeks, but now this is done in seconds. UBA acts as a business enabler.

Second, with compliance a big topic, UBA has helped Aetna's SOX compliance. SOX requires security access reviews be conducted and to ensure that users who have access need it. Likewise, the user may have access but may have not accessed the application in months, which may warrant revoking their access since it appears to no longer be needed. What's great is that UBA has reduced the number of clicks to review users and their application access by upwards of 90%! This is a huge timesaver for Aetna's security team and compliance is met in the process.

KEY FACTORS TO CONSIDER

UBA is very versatile and it is what a company makes of it. Aetna knew going into this that this solution would only be as good as the number of applications and entitlements for the primary business use. What this means is that the more the applications produce valuable log data required to profile the employee and their access, the more the solution can enhance the operation.

A lot of the data absorbed into UBA was already sent to Aetna's SIEM, which made it easier to poll the SIEM and make decisions within UBA. However, there were also other applications at Aetna, which needed to be adjusted to send high fidelity log data to UBA to align with the application tiers.
Also, with so many solutions on the market, it's very important to look for technology that aligns with business needs. Evaluating business use cases are beneficial in achieving an implementation that can be done at a pace that is acceptable for both the security team and the business. Otherwise, it may be tough to justify future projects if there is not a decent implementation timeframe that delivers some quick wins.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

With so many UBA solutions on the market, security teams need to do a fair amount of due diligence. Aetna brought UBA solutions into the lab and stress tested them to ensure they could perform as advertised.

For Aetna, scalability was crucial, especially because it would be used for preventative and dynamic provisioning of access. The solution could not be a barrier to the business while at the same time it needs to secure it.

How a UBA solution is designed varied from those who brought in the big data approach from the start, and those who were building on traditional databases. Vendors whose solutions were built on traditional databases tended not to perform as well as those who had a big data architecture.

Also, with Aetna creating tiers for applications and employees, a broad range of support for applications was imperative. This is very important because it may require some internal effort to get some applications sending necessary log data if they weren't doing it natively.

Lastly, it really is advantageous to be able to connect into a SIEM to capture log data that has already been formatted. This helps with the UBA analysis and at the same time ensures the SIEM data is preserved for historical use and requirements.

THE OUTCOME AFTER IMPLEMENTING UBA

Undoubtedly for Aetna, dynamic provisioning was a significant positive outcome of implementing UBA. There are now considerably lower costs when provisioning employee access to low risk applications. Again, prior to UBA, Aetna employees, IT, and security teams had to go through a manual approval process that required various resources. Now, when lower risk applications are called upon, the UBA solution can grant the access assuming the user's profile is in line with the parameters. On top of this, it is easy for the business, which is not always typical with a security solution. Security is able to say "yes," when a low-risk employee attempts to gain access to a low-risk application.

To determine the ROI for account provisioning, Aetna was able to employ a practical methodology. To do so, simply determine the average cost to grant access using the traditional workflow and compare that to how quickly and efficiently UBA is capable of performing the same task. This proved to be a fairly substantial cost savings through dynamic provisioning of low-risk applications.

ROI and ease-of-use for the business are a win for Aetna's security team. The team was able to take mundane, and must-do processes and automate them based on a sensible risk management model. This is noticed by company leadership who are now more apt to support additional UBA projects since there are metrics in place that demonstrate value back to the business, and bolster security at the same time.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

UBA's impact on Aetna's staffing levels is also a success story. For starters, there was no need to add to headcount. Where productivity gains continue to be noticed most is in the account access review. Typically, the reviews were done by well-compensated management positions. It was not a favorite task among the reviewers, but management understood it was necessary.

The old process was definitely not a favorite task of management and now they are more in favor and supportive of the current process. With UBA's record of accounts and access, the review is no longer a resource drain on employees, which frees them up for other tasks with higher value-add. These are the type of security and productivity gains teams seek when choosing solutions, and for Aetna, a great win for the security team and the business.

PEER RECOMMENDATIONS AND ADVICE

Security leaders will quickly realize with UBA that there is a lot that can be done. But this can distract the team from making an impact quickly. Simply put - don't try to do too much right away. Identify a high risk and/or high value use case, ensure the technology and business is understood, and get it right before moving on. What this does is provide the security team with a solid understanding of how the technology works and allows for a success story. It is also useful in setting up a repeatable process.

Also, determine the best way to communicate the success of this implementation with executive and board reports. Undoubtedly there will be very useful data that can be presented to company leadership. These reports show the preventative controls as well as giveback to the business through dynamic provisioning.

In the end, UBA is very versatile, therefore don't let it get so complex that there are no quick wins. Early wins go a long way building knowledge and trust.

SUMMARY

Aetna's approach to UBA is somewhat different than others, but it's been a big success. The pragmatic approach and preventive design is really an ideal implementation. Early detection of misuse and prevention is a top priority, but not in the way that it hampers business from getting things done. Dynamic provisioning is so valuable and does not create unreasonable risk. Security leaders should define their business use cases, ensure scalability and technology integration, and focus on a high-risk objective that returns a win to the security team and business.

BARCLAYS

Troels Oerting
Group Chief Security Officer

Elena Kvochko
CIO, Group Security Function

BUSINESS USE CASES

Financial services have long been a sought after industry for attackers and naturally they go where the money is. In the cyber security functions, comprehensive understanding of data, including behavioral data, has become part of the defense-in-depth strategy to identify anomalous activity. It goes without saying the core-underlying principal is respect for privacy.

For us at Barclays, comprehensive data analysis aids in overall security, resilience, intelligence and investigations of anomalous activities coupled with the principles of privacy and convenience. For global companies, technologies, like user-behavior analytics can help manage appropriate access and risk scoring of events. Risk scoring isn't a new phenomenon, as online banking, for example, have implemented this for a long time based on transactional patterns. But now profiling has moved into the back office to pinpoint patterns of anomalous behavior. Use cases, such appropriate reach to systems, policy implementation, integrity of operations and supply chains, are some of the areas where the technology can be applied. Another example, which companies across industries are inundated with, is malicious account takeovers. Whether it starts with a credential phishing theft or some other form of compromise, behavior and data analysis helps to pinpoint areas of concern and attempts to exfiltrate data. Anomalous behavior should be alerted before it becomes a bigger issue for companies, while seeking privacy and employee awareness.

THE TECHNOLOGY ENVIRONMENT WITH UBA

Ideally, analysis of behavior is integrated with the entire infrastructure of the business. Users, applications, permissions, system logs, and physical locations, all come into the equation. Historically, especially with a SIEM, the view was specifically focused on data collection, and primarily from the perimeter. But where the SIEM leaves off is when the user, their level of access, and their activity are not correlated.

With tight integration and a granular view, accompanies should make it a point to ensure employee privacy is paramount. Companies strive hard to earn and maintain the trust of their employees.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

UBA can be a robust layer of behavior profiling, baselining, correlating and insightful reporting. Any deviation from the norm is an opportunity to investigate the activity. User and application profiling, and distinguishing between what is and is not allowed, is some of the quick-win value behind UBA.

KEY FACTORS TO CONSIDER

It is important when choosing such technologies to realize that this is a market that is still maturing. Companies are getting better at turning out solutions in a very face-paced industry.

The size of the company and the assets one is seeking to protect matters greatly. For larger organizations, it is essential the solution could scale across diverse networks and geographic boundaries. The solution needs to be highly configurable to meet the different business unit requirements along with regulatory obligations where such data analysis provides with the evidence examiners are looking for.

A good starting point for organizations would be to outline their short, medium, and long-term goals and to verify that the solution is scalable for the future, but also not so complicated that quick wins are unachievable.

The solutions should be capable of working with structured and unstructured data. Global companies have a large global robust infrastructure that can stress the load limits. Integration with existing solutions and without a complicated configuration is a key requirement. As threats become more sophisticated, it is important to integrate various aspects of security together. As events occur, the granular level of detail and the reporting, and automated learning help manage each case effectively.

In terms of organization and functions, some companies, such as Barclays included, are building insider threat teams. These teams can be an addition to headcount or else, they can be an internal change in responsibility.

What's important is for companies to be flexible enough to adapt to changes in order to address the changing threat landscape.

SUMMARY

Companies should take a pragmatic approach to user behavior analysis and focus on the business use cases with a security-first design respect towards privacy and trust. This approach provides a higher-degree of confidence with detection, prevention, and prediction capabilities. Security, privacy, convenience should go hand in hand in implementing next generation security solutions.

IBM CLOUD AND SAAS OPERATIONAL SERVICES

David Cass
Global Chief Information Security Officer

COMPANY OVERVIEW

IBM is globally known with over a century of technology innovation. Located in Armonk, NY, and founded in 1911, IBM is operating in more than 175 countries. The company's nearly 400,000 employees continue their strong ability to innovate and in 2015 had over 7,000 patents. Revenue for 2015 was $81.7 billion and also have operating earnings per share of $14.92 and delivered operating net income of $14.7 billion. Cybersecurity solutions from IBM include security intelligence, analytics and forensic tools, just to name a few, deliver sought after value to customers. IBMers value dedication to every client's success, innovation that matters across the globe and a high degree of trust and personal responsibility in all relationships.

BUSINESS USE CASES

The use cases can vary depending on the line of business, and for IBM it is multifaceted. For example, there is a lot of intellectual property that is required to be protected. It is the company's competitive advantage. As leaders in technology securing thousands of patents annually, protecting intellectual property is essential to the company's long-term strategy to execute leading technology and innovation.

Additionally, included in the collection of intellectual property are the source code, which is unparalleled in its value to the company and the customers who rely on it to run their businesses. Unauthorized access to code has the potential to lead to negative consequences and the unfortunate mistake of allowing that to happen could lead to undesirable results.

IBM also is heavily invested in the cloud. Trust is imperative because it is what customers expect when they place their business into an IBM solution. Meeting this trust of our most important assets, our customers, is paramount. This requires, among other technological safeguards, maintaining proper segregation between customers so that one company's instance cannot impact another's.

Likewise, IBM has sophisticated technical teams that are entrusted to do the right thing. UBA can help provide the oversight to minimize the chances of insider misuse and decrease detection time, whether it is intentional or unintentional as a result of a compromise. IBM views this both for the internal operation as well as for solutions that are provisioned for customers that elect to make use of UBA.

THE TECHNOLOGY ENVIRONMENT WITH UBA

SIEMs have typically been focused on event monitoring and they have been a mainstay in nearly every security operation across various industries for a while, in recent years being augmented by UBA. UBA focuses less on system events and more on the employees' use of credentials and the access that they are entitled to. As most breaches continue to result from compromised credentials, profiling the use of the employee credentials on a regular basis – which is different than profiling the employee – allows the company to determine normal versus behavior. Once the baseline is achieved, it is unlikely an attacker will behave in the same or even similar manner with those compromised credentials.

UBA's place in the technology stack allows focus on patterns that are not inherently achievable through most SIEM system events. This way when attackers go slow-and-low and linger, once they become more active, the odds are they will get detected quickly.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

Defense in depth continues to be important and by implementing UBA a potential breach may be detected faster. Rather than being a headline where the attackers dwelled for 100-200+ days, the use of this technology is another way to close the gap on the attacker often much more quickly than other methods. UBA can offer significant value in quicker detection leading to faster incident response reducing the likelihood of an attacker completing their mission.

Although some organizations use UBA as a predictive control, our use cases have shown that it has greater success in detection. Whether there is credential compromise and an attempt at escalation of privilege or access to data, which data loss prevention (DLP) may or may not necessarily alert on, UBA picks apart some anomalies that otherwise may go unnoticed.

BUSINESS GOAL IMPLEMENTING UBA

One use case for implementing UBA is the reduction of insider threat capabilities whether the exploit is international or inadvertent. Also, UBA offers an additional level of protection for high value intellectual property and sensitive data in general. Regardless of industry, it is the sensitive data – from customers, clients, partners and the like, that executives often worry about.

If you have employees, you have insiders. While insider activity can be accidental or intentional, in either case, it can lead to a significant incident. When looking at the hiring process, all that goes into vetting employees comes to mind. Even with the best process in place, oftentimes it is not until later that employees either go astray or run into unintentional circumstances from simply trying to do the right thing on the job. As employees come and go, the potential for source code, strategic plans, and sensitive data to leave with them is a concern for all companies. UBA can alert on these situations even if an incident was unintentional.

KEY FACTORS TO CONSIDER

Security executives should review the maturity of their program on a regular basis. There is a natural tendency to try and procure new technology to address operational pain points. However, if the team is still struggling with the basics of identity and access management, i.e., provisioning and deprovisioning, then UBA may only lead to more alerts than the team is capable of handling. Always build from a solid base as you add capabilities such as UBA.

What this means is that there needs to be a good solid baseline within the company and fundamental security building blocks in place. UBA is the added-on layer to increase defense-in-depth and enhance the baseline process around credentials. However, security leaders should invest in their teams as well as technology tools. Investing in your teams will drive more efficient use of tools, such as UBA, and allow them to focus on actionable intelligence.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

When selecting a UBA vendor, automation and integration are essential. There is a limit to how many tools can be effectively monitored even by the most skilled of analysts.

If security teams have to spend a lot of time on configuration that time investment is contrary to the cloud model and today's business environment as a whole. Solutions need to have security capabilities that deploy with minimal intervention and offer automation of key capabilities to achieve baselines quickly and start demonstrating value.

Manual intervention and configuration slows the process down and goes back to the fundamental question as to whether the team and employee security skillset exists in general. It is great that solutions can be customized, but there must be opportunity to make progress quickly and without a need for highly specialized skills that may lock you into a product.

IBM is an expert in this and our solutions build ease-of-use into the technology. For solutions that are procured, there are high expectations for cloud and SaaS capabilities.

UBA also brings privacy into the equation. It is imperative to know what countries business operates in and if there are requirements around privacy that need to be factored into the solution. It is not a matter of user profiling; it is about how the credentials are used. The credentials are associated with the user, but it is really knowing how the credentials are being used that can lead to early detection of potential misuse.

THE OUTCOME AFTER IMPLEMENTING UBA

SIEMs are the central log point for security teams, which is great, but the issue of alert fatigue plagues most security teams and impacts their ability to extract all of the events that are top priority. Historically, this is evident in the industry with the average time of a breach discovery finding that the attacker was resident for an extended period of time. The addition of UBA highlights credential usage that is suspect and warrants investigation.

UBA provides intelligence, not just more log information, and that is a positive result that provides a return on security investment. Most UBA users have noticed quicker time to identify anomalous behavior and in turn faster incident response and containment. The industry is well aware an attacker can and will succeed given enough time and resources, and UBA is helping security teams reduce the dwell time.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

In terms of staffing, UBA may not have a direct impact. Though UBA's automation and efficacy of its altering is greatly improving it is not to the point of a net reduction of staff. On the flipside, UBA does not require more people in order to get the job done. However, it offers more actionable intelligence, which can increase efficiency. A lot of the intelligence gleaned without UBA may typically take an analyst much longer to go through the data and identify anomalous incidents. Solutions such as UBA that offer more actionable intelligence allow analysts to make better use of their time, such as following up on incidents and shutting them down much faster.

PEER RECOMMENDATIONS AND ADVICE

Keeping pace with technology is daunting for CISOs. UBA will certainly help mitigate risk through quicker detection of incidents with credential misuse. Likewise, in the cloud and go-to-market quickly regiment businesses are in, the solution cannot take a long time to obtain value and it certainly cannot create a bottleneck.

Those looking at UBA in the near future need to assess their team's ability to put process around the activity generated from the solution. It is not so much the challenge of managing the solution, but rather the practices around UBA that are important. If the team cannot sustain the process and activity that is generated by UBA then it is likely that UBA will not make the environment more secure. However, if it adds direct actionable intelligence and increases the ability of the security team to respond faster it will add value.

SUMMARY

Strategic deployment of UBA offers the potential to provide the business with greater insights into protecting intellectual property, and other assets. The technology sector is a very competitive space and the business expects patents, source code, strategic plans, and data to be protected. With the use of compromised credentials on the rise, the use of UBA offers better insights into behavior that does not align with historic user activity.

LEVI STRAUSS & COMPANY

Colin Anderson
Chief Information Security Officer

COMPANY OVERVIEW

Levi Strauss & Co. is a global retailer, founded 163-years ago. With approximately 2,800 retail stores, of which there are nearly 50,000 retail locations, the company had annual revenue in 2015 of $4.5 billion from sales in 110 countries. An iconic brand, Levi Strauss & Co. sells Levi's®, Dockers®, Denizen®, and Signature by Levi Strauss & Co™, recognized worldwide. Levi Strauss & Co. has corporate offices in San Francisco, Brussels, and Singapore. The 2015 annual report lists 12,500 employees worldwide (5,700 Americas, 3,700 Europe, 3,100 Asia).

BUSINESS USE CASES

The retail industry faces a number of challenges from bad actors which range from cyber attackers attempting to gain access to payment systems to counterfeiters selling fake, non-authentic merchandise to unsuspecting buyers, causing brand and reputational harm. As a globally-recognized brand, Levi Strauss & Co. values information security and is increasing its investment in cybersecurity to protect this iconic brand and its consumers. These investments continually work towards reducing risk to payment systems, personal information, and third-party dependencies. UBA is an important capability and has become part of the defense-in-depth strategy at Levi Strauss & Co. to aid in mitigating risk across the global enterprise.

A primary use case for Levi Strauss & Co. is monitoring access to critical data such as consumer and payment information. In the retail industry, this data is a favorite sought after by attackers and is a key operational dependency of the business.

As one might expect, access controls are a primary mechanism to protect against any wrongdoing. However, the individuals may be misusing their legitimate access or potentially accounts may have been provisioned that had more access than the "least necessary." The implementation of UBA aids in identifying any aberrations in the accessing of data and highlights the need to investigate, in many cases, before any wrongdoing.

Secondly, as a retailer, we have a fluid and seasonal workforce with turnover. Accounts are provisioned and deprovisioned in large numbers to meet the needs of staffing in the business. Due to this rapid change in accounts, there is potential for misuse. UBA provides oversight in the account management process by allowing Levi Strauss & Co. to get a good baseline to determine normal usage patterns and to identify anomalies between appropriate and inappropriate usage.

Thirdly, UBA is used with contractors and third parties. Levi Strauss & Co. has a large third-party user base. The services these third parties provide range from support, development, and even the provisioning of accounts in order to run the operation. In some cases, the ability to create additional accounts is turned over to the contract organizations. For example, UBA ensures that accounts are not being shared and the privileges granted aren't misused. This also provides the audit trail that is essential in controlling this workflow.

THE TECHNOLOGY ENVIRONMENT WITH UBA

Organizations are compromised all the time, but it does not have to result in a business-impacting event such as a data breach. UBA is a compliment to the SIEM and each control system provides its own unique detection value.

SIEMs have been heavily invested in through the years and they are central to the security operations center (SOC). UBA has insight into activity that SIEMs don't have visibility into and vice versa. As such, they both have their use, and probably for most, one technology would not replace the other. There are some activities that UBA can add to what SIEMs perform, but there is also a tremendous amount of data collected by SIEMs that is vital to the security operation. SIEM vendors have been slowly moving to more UBA-like capability within their solutions, but for the time being, they are complimentary and one does not necessarily eliminate the need for the other.

Levi Strauss & Co. leverages both UBA and SIEM technology for better detection of anomalous behavior.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

Through the use of UBA Levi Strauss & Co. has been able to enhance its detection and response capabilities accomplishing one of its core objectives of continuous improvement. UBA provides the capability to achieve much greater insight into accounts, their level of access, and use or misuse of that access. The detection capabilities, which are a core competency of a more mature security team, have been heightened as a result of UBA's granularity. When comparing to the Kill Chain®, the ability to disrupt the attacker much earlier through the determination of a compromised account is crucial to protecting against the attacker's goal of data compromise. The audit trail and reporting places emphasis on where security teams should prioritize their efforts. This prioritization allows teams to protect against much bigger problems than, for example, one compromised account.

BUSINESS GOAL IMPLEMENTING UBA

For Levis Strauss & Co. the business goal for implementing UBA is for consumer and brand protection. Being in business more than 160-years and having worldwide name recognition, the value of the brand is immeasurable. Protecting the brand and our consumers is paramount to what the security organization is all about.

Levi Strauss & Co. consumers can trust that the company takes protection of their information seriously. Whether in a retail store or shopping online, consumers must have confidence in the company's total dedication to protecting their personal information as if it were our own.

A second goal is to help ensure third-party compliance. Many of Levi Strauss & Co. contracts with third parties have very strict language about what they are, and are not allowed to do. A great deal of trust is granted to our partners. UBA helps to ensure the contractual commitments are upheld when partners are performing services for the company. Just as the controls we place on employee accounts, UBA assists us in protecting sensitive information and the brand when engaging third parties.

KEY FACTORS TO CONSIDER

Historically, some technology implementations are not only costly to acquire, but worse, are costly to maintain. They can be a resource drain on the technology employees who are tasked with implementing and maintaining them.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

Looking back at the UBA investment, a critical consideration was the total cost of ownership (TCO). Security employees are extremely valuable and get pulled in many directions. It was key for Levi Strauss & Co. to select a UBA solution that was easy to implement and did not take up significant technology resources in order to gain value.

A UBA solution should not be overly complex to implement or maintain. If it is resource intensive then it has the potential to slow down other parts of the operation. Levi Strauss & Co. needed to bring in a solution that did not drain time from employees who already had a fair amount of obligations.

Another key consideration for the successful implementation of UBA was native data support and the context to do analysis. With user data very dispersed, it was important to bring in other data sources. For example, the combination of logical and physical security is important. Physical proximity devices provide a lot of useful information that, when coupled with the employees' logical access, provides a holistic view of employee access.

Finally, Levi Strauss & Co. looked at the overall health of the UBA vendor. For example, their financial strength and ability to innovate. There are a growing number of vendors in the UBA space and some may be unable to sustain the requirements succeed and may no longer exist within a couple years. CISOs will definitely not want to acquire technology only to learn later that the company is no longer viable.

Levi Strauss & Co. sought a UBA vendor that could provide depth in technology along with their ability to be a sustainable company overall. It is somewhat expected that the vendor will be able to provide out-of-the-box technology as a standalone solution. However, the real value-add is when the vendor is able to enrich the solution by incorporating other sources of data.

UBA vendors that integrate data from Active Directory, VPN logs, CMDB, HR systems, physical security solutions, and more were desirable; this deepens the overall solution and as indicated earlier, provides a much more complete view of the employee, their access and their activity.

The technology requirements coincide with the overall key components in selecting a vendor. The solution must not be complex to manage, yet it must be nimble enough to derive immediate value from traditional as well as legacy or physical security systems, too.

THE OUTCOME AFTER IMPLEMENTING UBA

The goal of implementing UBA was to get more context behind each activity. Levi Strauss & Co. has a lot of systems that bring in events, but the events often lack context. Context is crucial in security.

When an incident is triggered, the security staff should not have to log into multiple sources and spend hours searching for more context around the event that just occurred. A good UBA deployment should bring this level of information to the dashboard. C-level reports also should be thorough and meaningful. Far too often other technology systems provide the source for incident and report data, but drain the analysts' time in order to extract value.

Once this value is brought to the forefront, case management is more efficient and employees' time is better utilized. Detection and anticipation of suspicious activity is sequestered when chosen and implemented wisely.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

The impact on staffing levels is still progressing at Levi Strauss & Co. as the UBA deployment is still in its measurement stage as the solution was only recently implemented. However, at a previous employer where UBA was deployed, the team was able to increase their incident investigation workload by 25% a day. Prior to UBA implementation there, the team's ability to analyze cases was lagging and there was a potential need to hire two more full-time employees, just to handle the incident load. However, when UBA was introduced, the team was able to take on more incidents per day and do it with a significant increase in efficiency. The ability to replace the potential hires with a UBA solution there provided a clear return on investment (ROI) to the enterprise.

RECOMMENDATIONS AND ADVICE

CISOs seeking a UBA implementation should first and foremost ensure their team is mature enough to get the full value out of the solution. Security teams should be able to sustain a UBA solution and not have it become an added solution with little-to-no value because it is not being used to its fullest.

What this means is that the foundation of the security program must be solid. Access controls are very important and if they are ineffective, teams will be chasing one problem after another. UBA may help identify where there are problems, but UBA is not going to fix these problems. Likewise, if the environment is full of unpatched vulnerabilities, UBA is not going to resolve fundamental core problems that should have been addressed long ago.

UBA is a great solution with a lot of value, but in order to be successful, like most areas of information security, there must be a solid foundation or UBA will only exacerbate problems.

SUMMARY

Levis Strauss & Co. has found a lot value in UBA that would otherwise not have been realized with only a SIEM correlating data. Likewise, UBA enhances and improves upon access controls to help protect the business brand and ensure consumer trust does not erode. While there is still room for improvement to gain more efficiencies, the fact is the team has gained valuable insight in detecting suspicious activity more quickly and protecting against a business-impacting event such as a data breach.

MIAX OPTIONS

John J. Masserini
Chief Security Officer

COMPANY OVERVIEW

MIAX Options is a fully electronic options trading exchange. MIAX Options has assembled a team with deep-rooted experience in developing, operating and trading on options exchanges. Its trading platform has been developed in-house and designed from the ground up for the unique functional and performance demands of derivatives trading. MIAX Options now lists and trades options on over 2,400 multi-listed classes. MIAX Options' unparalleled system throughput is approximately 38 million quotes per second. The average latency for a single quote on MIAX Options is approximately 16.21 microseconds for a full round trip. The executive offices and technology development center as well as the National Operations Center for the MIAX Options are located in Princeton, New Jersey.

BUSINESS USE CASES

In order to effectively manage risks throughout the environment, a program must continually mature to keep pace with the ever-changing world of our adversaries. When the company looks to manage risk, it's done so with an understanding not only of how an attack occurs, but how access was achieved and maintained for extended periods of time. In essence, we look at how we can mitigate risk around specific areas of the kill-chain, our maturity level and how we can enhance the control structure given the existing solution landscape.

In concert with the overall business drivers of ensuring a safe and sound environment, the regulatory landscape within the exchange space is, rightfully so, some of the most stringent imaginable. While in many industries, risk management and controls rarely positively impact the bottom line, in the financial industry, a secure environment is the expectation.

These two key factors, fueled by the continual maturation and re-assessment of the overall risk program, in concert with the lessons-learned from recent headline-making breaches, drove our desire to enhance our strategic approach to insider threats and account subversion. User Behavior Analytics (UBA) played a key part in the evolution of that approach, augmenting the existing aggregation and correlation solutions with one based on known baselines, real-time activity awareness, and integration into a single dashboard.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

While SIEM excels at the collection, aggregation, and alerting of potential security threats, they typically lack context to understand how behaviors change over time. A SIEM is very cut and dry - very black and white. We wanted to find the grey area between activity that a normal account sees and one that demonstrates behavior of a compromised account or a potential rogue employee. While a SIEM can correlate the "north/south" traffic adequately, most of their capability is lost on "east/west" traffic - subverted accounts used for illegitimate access by taking advantage of over-permissioning or privilege escalation.

CHALLENGES

By exposing a risk that was otherwise only detectable with significant in-house development efforts, UBA addresses a risk that was well known, but always challenging to monitor. Now, user analytics can be integrated into the commonplace SEIM to provide dynamic insight into account behavior. By enriching the data already collected, we are able to provide auditors and regulators far better views into user behavior and suspicious activities.

The integration of UBA with our existing solution set provides a level of user analytics that was unavailable before now. The ability to recognize a user's typical 'path' throughout the enterprise and to alert on the deviation from that main model is truly something that moves the needle.

KEY COMPONENTS

Currently, we monitor all aspects of user activity from remote logins, file/share access, web browsing, and application usage. The UBA solution has been integrated into our primary collection and aggregation solution, allowing it to easily monitor all critical logs and feeds from across the organization. Additionally, due to integration with our SEIM solution, our analysts are able to maintain their 'single pane of glass' model, simply moving between events, research, and resolution screens.

Another key benefit is the integration of the UBA solution with the Privileged Access Management (PAM) solution that is used to control privileged accounts. We now not only have control over the accounts from an access perspective, but now we can layer on behavior modeling to ensure the account is used appropriately.

Finally, access to the source code library and various development tools is being modeled for future inclusion into the effort. This functionality will enable us to closely monitor who accesses which source code libraries, who does builds, and who pushes deployments - all without adding new agents or tools to the developer's workstation.

UBA is still considered an emerging technology, and as such, any actions must be supported by another internal solution before any significant action is taken. That said, the forensic capture capabilities and the ability to quickly provide investigators with hard, accurate evidence is providing a substantial benefit to the organization in resource productivity.

As the solution, and the UBA space in general, matures, we anticipate significant benefits to our SOC operations and overall security program. This includes leveraging the UBA 'weightings' to deterministically drive adaptive authentication throughout the enterprise.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

As mentioned, the deployment of UBA has been a tremendous asset to our SOC analysts, providing vital intel during an investigation quickly and in the same pane of glass they are accustomed to using. By culling out the 'noise' and providing the analyst with a clear, step-by-step list of activities that occurred enables the researcher to investigate, and potentially remediate, the issues quickly.

SUMMARY

While more often than not, new tools require additional resources to manage the solution, the UBA solution was virtually 'plug-and-play,' ingesting logs from centralized SIEM collection point and integrating into already existing solution sets. Not only has the overall impact to staff been minimal, the solution has provided a high level of value add in a very short time.

OPPENHEIMER & CO. INC.

Henry Jiang
Chief Information Security Officer

COMPANY OVERVIEW

Oppenheimer & Co. Inc. ("Oppenheimer") is a leading investment bank and full-service investment firm that provides financial services and advice to high net worth investors, individuals, businesses, and institutions. For over 130 years, Oppenheimer has provided investors with the necessary expertise and insight to meet the challenge of achieving their financial goals. Oppenheimer's commitment is to clients' investment needs, with experienced and dedicated professionals, and a proud tradition to deliver effective and innovative solutions to clients. Reported results for 2015 include client assets under administration totaling approximately $78.7 billion, while client assets under management that were fee-based totaled approximately $24.1 billion. Oppenheimer employs roughly 3,200 employees.

BUSINESS USE CASES

The financial industry is a favorite target of attackers and they show no sign of slowing down. One of the challenges the industry faces and why UBA is an attractive technology to look into is the excessive alerts generated by traditional technologies and a finite number of analysts to investigate them.

For starters, UBA is an opportunity to get high fidelity alerts with less distraction from events that are innocuous. There are so many systems and each is capable of generating alerts for various events. But which events does a modestly-staffed team concentrate on when they can manage, for example, less than 20 alerts per day?

The abundance of alerts from systems and user activity, depending on staffing, may simply not be sustainable given a company's resources, changes in technology, and the evolving tactics of attackers. One solution is to add to headcount, but for many companies that is not a sustainable model. UBA can take some of the burden off analysts by using machine learning to promote high fidelity alerts.

Second, it is paramount for security teams to ensure the business is not disrupted. It is too easy for an analyst to take the wrong action in the midst of responding to an incident, and that response can interrupt part of the business. UBA gathers a solid user baseline and when there's a deviation the analyst has much more information and context in order to respond accurately.

Third, UBA is about alerting and triaging. Security teams need a better place to start when responding to incidents than simply relying on traditional technology. Prior to UBA, analysts often spend too much time in and out of systems trying to correlate activities. UBA consolidates data on the incident and provides meaningful insight to take the correct action.

THE TECHNOLOGY ENVIRONMENT WITH UBA

The lines have blurred between UBA and SIEMs. At Oppenheimer, they are two different technologies and each serves a very unique and useful purpose. Despite some experts' contentions, it would be premature to state that UBA is a SIEM replacement.

Businesses of any scale often collect and process millions of events per day in their SIEM. Regarding the challenge of adequate staffing, having enough analysts to work incidents, it does not make sense to keep hiring when UBA can dramatically lower the number of events to review each day.

UBA's machine learning does what SIEMs are not traditionally designed to do. SIEMs are great for data collection and correlation and to be investigative post a breach, but unlike UBA they are not built to identify behavioral deviations. At many organizations, UBA works in tandem with the SIEM and subsequently efficiency is increased.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

UBA improves the ability to get user-based data to the SIEM with context. The SIEM is still central to most security operations, but UBA obtains and sends syslog events to the SIEM for analysts to review.

Whether it is an insider threat as a result of account abuse, malware propagation, or DLP events, the analyst requires data flow to the SIEM. UBA sends its high-fidelity events to the SIEM and reduces the amount of analyst time spent gathering artifacts for the investigation.

The data provided by UBA can be so useful that analysts can now spend under 10% of their time viewing the UBA dashboard. This is because the SIEM is and has been the single-pane of glass for many security operations centers (SOC). But the UBA data is extremely valuable and it simply just outputs to a SIEM as opposed to an analyst in and out of too many dashboards. UBA's ability to integrate with the SIEM is a must have. In fact, for companies considering UBA, any UBA solution without the ability to output meaningful information to a SIEM would be very tough to contemplate.

Those security executives who think that the workflow with UBA will be so automated that the solution can respond automatically without human oversight will want to be careful. Deciding that automation can totally replace analysts' reviews is risky.

BUSINESS GOAL IMPLEMENTING UBA

The business goal for security teams varies. For many organizations it isn't to improve the business process workflow; that's not what the team is there to do. The team exists to protect the data. Like many enterprises this can be done through predictions and prevention of loss. UBA's business goal value is primarily around two basic, but hard principles – data protection and access control.

Security teams in many finance-related organizations are tasked with protecting the financial data of the account holders, and often need to do this without an excessive number of employee hours. People can always be allocated to the problem, but that does not make the team more efficient in combating it.

The purchase of UBA allows financial organizations among others to keep personnel costs under control as well. By taking some of the money that would have been allocated to staffing and giving a portion of that to the procurement of UBA, a company can save in personnel costs while achieving gains in productivity. In addition to the goal of protecting the data, keeping expenses to a realistic and manageable number is a necessity.

KEY FACTORS TO CONSIDER

Perhaps surprising to some, financial institutions are very cost conscious. Financial considerations are always an issue taken into consideration. On a scale of 10, cost would rank for many financial institutions as high as an 8 or a 9; it's that important. And typically this is part of the first conversation with decision makers, because if an investment is unaffordable then the conversation needs to end. Because of this it is important to evaluate UBA products license structures. Some solution providers base their license by host versus user. User licensing typically weighs in favor of the customer because there are way more hosts than users.

Depending on the company, the time to implement may or not be a factor, but it should at least be a talking point with the vendor. This is especially true if the business has selected a UBA vendor that is in growth mode as a business because they may be unable to meet a company's aggressive implementation demands.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

Suffice it say, UBA POCs require a lot of due diligence. Many UBA vendors will claim competency, but it's not until the POC is underway where the proposed ability to support a particular purpose is found lacking. It is insightful to hear a vendor's thought process for collecting data to understand their ability to innovate ahead of their competitors.

One area is the data collection mechanism. Many UBA vendors will support raw data captures and this is somewhat of a given. However, the structured and unstructured data is a very big consideration for many organizations in finance and across other industries. Additionally, UBA data collection considerations should include web proxy logs, netflow data, and syslog.

Second, additional expectations of UBA vendors include machine-learning capabilities. User group data collection and correlation is also something that an organization may want to ensure is available within the solution.

One area to watch out for is encryption. In today's climate, many organizations, in particular in the finance sector, demand encryption is enabled whenever possible. Therefore, network traffic, LDAP, web traffic, and data in storage, are typically encrypted. If this is important, an executive may view a vendor's lack of support of encryption of any of the above as a red flag. Simply put; they should have thought about this because their competitors have.

THE OUTCOME AFTER IMPLEMENTING UBA

After implementing UBA, as a rule security teams should able to perform incident response much faster. This is because the analytic capabilities of UBA and its machine learning help with the diagnosis of the incident so that analysts focus on the right events at the right time. As a result, malware outbreaks are sequestered rapidly.

In addition to automating analysis through more rapid detection, exfiltration of data by and large can be prevented due to the ability for a security team to resolve the incident fed from UBA to the SIEM console. Overall, this can lead to an improved defensive posture and better allocation of a security team's time through case management and workflow optimization.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

Acquiring UBA technology does not have to increase headcount for an organization. The events identified by the UBA system, while meaningful, can often be very manageable and do not require additional employees. In fact, because events from UBA are more streamlined than from other sources, staff may spend less time on those tasks than they did previously and more time on other value-add projects.

However, staffing levels may be impacted by how much data an organization chooses to input into their UBA from other machine learning systems. More data could potentially drive the need for more event review, and as a result additional staff may be needed

PEER RECOMMENDATIONS AND ADVICE

There can be a lot of confusion in this space and even for experienced teams. There hasn't been a lot formality developed towards common UBA features.

UBA is a very fluid technology and there is a lot of hype around each vendor. If a vendor is not listed by an industry analyst firm, they may decide to try and embellish descriptions of their solution and tell customers that they are forward thinking, that there is no category to define them yet as they are ahead of the market.

UBA is not a panacea! UBA does not substitute for the work of analysts; rather it can provide better analytics to do the work faster, better and more efficiently. If a security team does not have a way to use analytics in their operation, UBA is not going to help. The security team must have the maturity to bring on this technology in order to be successful.

SUMMARY

UBA is often a wise investment because of the machine learning and analytic enhancement it can bring to the operation. Still, it does not replace a SIEM, which is logical because it was not intended to do so, at least in most implementations. UBA enhances the team's ability to have strong access control oversight and protection against data loss, which are both business goals. Lastly, as an added benefit, compliance can also be boosted alongside the solution's ability to meet requirements in a mature and robust fashion.

RWJBARNABAS HEALTH

Hussein Syed
Chief Information Security Officer

COMPANY OVERVIEW

RWJBarnabas (RWJBH) Health is the most comprehensive health care delivery system in New Jersey, treating over 3 million patients a year. It is New Jersey's second largest employer – with more than 32,000 employees, 9,000 physicians and 1,000 residents and interns. The system includes eleven acute care hospitals, three acute care children's hospitals, a leading pediatric rehabilitation hospital (Children's Specialized Hospital), a freestanding 100-bed behavioral health center, ambulatory care centers, geriatric centers, the state's largest behavioral health network, comprehensive home care and hospice programs, fitness and wellness centers, retail pharmacy services, a medical group, multi-site imaging centers and four accountable care organizations.

BUSINESS USE CASES

Healthcare has become a prime target for attackers and user behavior analytics (UBA) is a key part of RWJBarnabas Health's defense in depth strategy. There are several use cases that were found to be valuable across the company, both in terms of governance risk and compliance, and security. Of the many identified use cases, there are a few that stand out.

As a highly regulated industry, healthcare puts a great emphasis on compliance. For many organizations, using UBA to help comply with regulations is an effective strategy. As a newer technology, UBA can provide great controls when protecting employee, patient and client information by ensuring that those who have access to information are authorized.

In addition to helping to meet HIPAA mandates, UBA aids in PCI compliance as well, by helping to detect and prevent any potential misuse of payment information. For RWJBH, it is critical that we adhere to regulations and prevent data exfiltration, which is an increasing risk in the healthcare sector. Some industry analysts put the value of a medical identity (i.e., information on the individual and their medical insurance) as far greater than credit card information by itself.

In addition to employees viewing data, RWJBH Health is able to investigate how employees access and use data. Appropriate use is critical to ensure compliance and privacy, which regardless of regulations, is paramount to RWJBH.

Potential violations include but are not limited to employees attempting to access other employees' information as well as trying to glean information on VIPs.

THE TECHNOLOGY ENVIRONMENT WITH UBA

RWJBH treats millions of patients annually and employs tens of thousands of people. We process and store a significant amount of data. User login and data access information is required to feed UBA. The data is capable of being captured through the use of internal resources and UBA was purpose-built to take in and analyze these feeds.

For example, patient, employee, address, scheduling, and location information can be captured, sent to UBA and then correlated. Once the appropriate mapping and rules are in place, a great deal of valuable analysis is created.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

The ability of UBA to identify anomalous behavior has been very effective for RWJBarnabas Health. While SIEMs are in place for log collection and data correlation, there are areas where the SIEM has been unable to provide the user behavior anomalies, which are needed to uncover suspicious behavior.

An example is someone who does not usually connect to the VPN at a particular time but all of a sudden connects during that period. This would trigger an anomalous behavior alert. It could be a legitimate connection, but regardless it warrants follow through for investigation. Essentially UBA helps to detect and alert on atypical personnel activity from, for example, attempting to access resources to which they have no reason to, to peering into information not required to perform their job.

Detecting anomalous behavior is particularly important in Healthcare because even though employees are given "least privilege" access to patient information, that access still tends to be fairly broad so that it never interferes with patient care.

Additionally, UBA has been used to baseline data loss prevention reports, which are then escalated to human resources or internal audit for further investigation. Since data is supposed to be accessed and handled within a set of predefined rules, UBA can assist other technologies in ensuring inappropriate access is identified.

Lastly, UBA's ability to alert on the misuse of credentials or any attempt at data exfiltration drives quick escalation at RWJBarnabas Health. These alerts may be the first indication of an attacker attempting to increase privilege, move laterally, and exfiltrate data.

BUSINESS GOAL IMPLEMENTING UBA

The initial business goal at RWJBarnabas Health was to help meet governance risk and compliance mandates. The results have been positive and from a technology and business perspective we are looking to extend our usage to more traditional security use cases.

We will continue to implement UBA to improve security and to detect (example Internet Proxy, VPN and Active Directory log correlation) and respond to behavior, which was different than expected.

The industry as a whole spends a significant amount on prevention, but detection also is critical. Executives see and read the impact attackers are having on the Healthcare industry. It is a multipronged approach, prevention, and detection. This approach also will aid the security team, providing significant benefits by identifying potential incidents early on. This allows RWJBarnabas Health to respond better and faster.

KEY FACTORS TO CONSIDER

When deciding to implement UBA it is important to ensure key stakeholders are involved from the outset. For Healthcare, this includes the executives responsible for legal, risk management, and privacy. UBA can provide significant insight into what is important to the business, but at the same time there is the potential for what could be perceived as privacy overreach.

With this in mind, RWJBH is careful to ensure separation of duties to ensure that administration and oversight are preserved. Since Healthcare has a tradition of monitoring for quality assurance, outcomes management and privacy, this separation comes naturally to the industry.

For example, security may be the group that builds and deploys the solution, but an access management team may be the team monitoring policy violations and escalating to incident response teams. With great power comes great responsibility and separation between front-end access and back-end administration is a core principle that applies to UBA.

Lastly, UBA is what you make of it, which means good asset inventory and classification are important to success. It is also essential not to attempt to do too much at once. Getting some small wins and repeatable process will help provide a sustainable operation.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

Integration and support for structured versus unstructured data are characteristics that should be taken into consideration. These directly impact a vendor's ability to scale. Definitely bring the solution in-house for a proof-of-concept and verify that the system can scale to meet future needs.

Also, a lot of vendors tend to promote their ability to be customizable. While this is good, there also needs to be some quick wins. The system must not be too complex, which would make short-term wins unachievable. If the system cannot be up and running within weeks to provide some immediate value, then perhaps the wrong vendor is being assessed. Too many security technologies have historically been complex, which for all intents and purposes is an enemy of security. Suffice it to say, ease of use and quick wins that link to business goals are important.

Lastly, there is also a need to integrate with current solutions to maximize ROI. This objective correlates with the ability to produce value quickly. The ability to easily integrate with existing solutions, including the SIEM, helps to round out the infrastructure.

THE OUTCOME AFTER IMPLEMENTING UBA

RWJBarnabas Health now has visibility into internal user behavior that we haven't had historically and we will continue to extend our UBA usage. The data and systems are there but oftentimes our current understanding is still too one dimensional. What may currently be perceived as normal or benign may in fact be an anomaly. Even if a connection is not malicious it does not mean that it isn't an invalid escalation of privilege.

Importantly, UBA has provided significant GRC gains. It also has provided the team greater visibility when there are privacy violations in order to produce evidence to meet the needs of a highly regulated industry.

RWJBarnabas Health also has seen a reduction in the number of false positives that have been generated by other systems. When UBA provides alerts, our analysts quickly gain insight whereas in the past they may have been searching for that proverbial needle in the haystack, taking time and resources. Because of this, UBA also helps catch and close incidents much faster. With UBA, RWJBH is able to preemptively investigate, stopping incidents before they turn into a breach of confidential data.

Lastly, the workflow for other areas has also benefited from UBA. For example, the access management group is a primary benefactor of UBA, which now assists them in fulfilling their compliance obligations. The security team is also seeking to extend the use of the solution.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

At RWJBH we have greatly advanced our detection and response capabilities with UBA. The various teams, in particular those overseeing GRC, have much more useful information to work with that would have otherwise taken more analyst time to uncover. With this automated identification of anomalous behaviors, there have been productivity gains as a result, letting staff members work on more value-add services. UBA allows our team members the ability to take mundane, but required tasks, and lessen the burden with the detection of anomalous behavior.

The initial implementation can require additional resources, but this should not be a continued need. In fact, we have found that once UBA is in place, staff can better utilize their time. In the end, for us, it has been net-net, without the need to add or remove employees.

PEER RECOMMENDATIONS AND ADVICE

Transparency with employees across the enterprise to gain their trust, and ensure they understand what is being checked, helps to build a better relationship when UBA is deployed. Also, the best, industry-leading solution, may not be the best for you. It's more important to choose the right solution for your environment than be overwhelmed by "best of breed."

It is also very important to evaluate the organizational structure to determine where and who will oversee the results produced by UBA. Ultimately this may be more than one group, depending on the structure of your organization. Is there a GRC team? Is the security team more of an advisor to the business and IT manages infrastructure, or does security also have infrastructure responsibilities, too? It is very important to define the team structure and determine where various aspects of UBA reside.

Lastly, don't overspend. Look for a solution that helps gain insight and can grow as the team and program matures. As the various programs mature the solution must be scalable enough to provide out-of-box quick value-add services across teams.

SUMMARY

UBA has become a very sought after solution that integrates and provides visibility to anomalous user behavior. Security and privacy leaders both can benefit from UBA deployments. RWJBarnabas Health has seen some great advancement in the GRC process and other technical areas have also enhanced their workflow as a result of the advances in data analysis. We are now seeking to further implement UBA as a pure security tool. UBA has the ability to augment many other technologies, both within security and beyond.

SURESCRIPTS

Paul Calatayud
Former Chief Information Security Officer

COMPANY OVERVIEW

Surescripts connects the broadest community of healthcare partners. Located in Arlington, VA, and founded in 2001 by pharmacies and pharmacy benefit managers (PBMs), Surescripts set out to replace paper prescriptions with electronic prescriptions. Today, Surescripts has a directory of more than 800,000 providers nationwide, which includes a patient benefit and eligibility data on more than 270 million insured lives in the U.S. Included in the Surescripts network are 900,00 healthcare professionals, 3300 hospitals, and 95% of pharmacies. A vast amount of data transmits seamlessly across the networks where annually there are around 10 billion transactions, 764 million mediation histories, 7.4 million clinical messages, and 1.2 billion e-prescriptions. Surescripts supports over 700 electronic healthcare record (EHR) applications across 32 state and regional networks. Without question, cybersecurity is a priority for Surescripts and has achieved ISO 27001 certification.

BUSINESS USE CASES

The use cases for Surescripts were distilled down to a couple key areas of risk that could be addressed with UBA. Simply put, the focus has been predominately on data loss prevention and credential theft.

With data loss prevention, UBA focuses on privileged accounts, employees, and their ability to access information on the network. For example, an employee is operating in the role of an administrator and they therefore have the rights to access large sensitive data sets. Security must ensure that what they are doing is within the normal grant of authority for their position, i.e., the lowest risk for that level of access. UBA aids the security team in identifying what normal versus abnormal access looks like.

Second, our credential theft use case expands beyond what many think of in the traditional sense of inside threats. Notice inside threat as opposed to insider threat. We have broadened the definition of insider threat, which traditionally concentrates on the employees inside who may be disgruntled or a bad actor abusing privilege. We add to this the case where the employee is not intentionally abusing privilege, but their credentials are. This is the employee's digital identity, which was somehow compromised. The attacker started from the outside, but worked their way to the inside. Inside threat combines the employees (insiders), and malicious actors who were outside- both are now considered an inside threat. When looking at what some malware attempts to do, it is to gain access to credentials and move laterally inside the network.

The ability for UBA to baseline and identify employees, or their compromised credentials, that may be acting out of character, links directly into the goal of data loss prevention for the business use case. This is an element of the Kill Chain™ to protect against data exfiltration through the use of UBA.

THE TECHNOLOGY ENVIRONMENT WITH UBA

UBA for Surescripts serves multiple roles in the technology stack. It enables our Data Loss Prevention (DLP) to do more than DLP could do as a standalone solution. The traditional deployment of DLP mainly serves compliance requirements. However, companies can really mature their DLP program through strategic use of UBA.

In order to achieve this, Surescripts began by deploying UBA in the form of an agent. The standalone agent is able to detect patterns of file use that extends beyond user authentication, something that is obtainable from the SIEM. The agent generates analytics by incorporating file metadata. The solution is able to determine data loss risk through its visibility into the file metadata. The agent is independent technology with big data on the backend. This was Surescripts initial strategy, where data is generated by the agent doing its own analysis in its own stack, and then generates alerts to the SIEM.

The next iteration of the UBA platform became an "ingest strategy" by pulling in data from the SIEM. The SIEM produces data that can be ingested into UBA's stack and alert on possible use cases with privilege or credential abuse. Combined, Surescripts leverages the intersection of self-sufficient, agent-based UBA and SIEM data.

The next focus will be on other unstructured data sets to monitor fraud, for example. This will require customization and partnership with solution providers, but the future looks promising for this use case at Surescripts.

TECHNOLOGY ACHIEVEMENTS BY IMPLEMENTING UBA

UBA determines the outliers based on the user's profile. So even if the employee has the right to access sensitive data UBA is able to bring in other attributes beyond a yes or no whitelist of access privileges. It compares the user agent data and SIEM events to make a more intelligent decision about the appropriateness of a user's behavior. This architecture brings in existing investments with sophisticated analysis and thus significantly enhances DLP. It is not so much that there was access to the data, but it is the manner in which the data was accessed.

A lot of companies have DLP solutions that are deployed to protect across email and web channels, but they lack the behavioral traits that UBA picks up on. UBA brings so many points of access and analysis to the forefront that it enriches the security operation. Again, it is not that a user accessed data, but rather how they went about accessing the data that may or may not have been within the acceptable profile of the individual or account.

BUSINESS GOAL IMPLEMENTING UBA

When one looks at the healthcare field and network access across providers and pharmacies, there is a lot of concern for data loss. The company processes billions of transactions annually. In order to do this, the network must be robust and also trusted at all the points of access including the entities that participate. Data loss is a top concern when it comes to security. A loss of data erodes trust and inflames legal, not to mention how data loss calls into question the compliance versus security debate.

Data loss events distract companies from their core business. They can be expensive, time consuming, and an opportunity for competitors to capitalize on misfortune about the company (i.e., the impact of reputation risk). When the team set out to evaluate UBA it was with the goal in mind of ensuring security was doing its part to support the business' execution and growth, and to ensure that a breach would not set the company off its path to success.

KEY FACTORS TO CONSIDER

Security leaders should consider their blind spots. UBA helps to provide visibility into other technologies and what they cannot detect or prevent. For example, in most of the recent, highly publicized breaches, an Intrusion Protection System (IPS) would likely have done little to protect the business from the exfiltration. The attackers appeared to be well aware an IPS was a layer of defense and they avoided setting off alerts. The attacker is going to try and blend into the environment but they are not likely to impersonate the users' behavior well, which is where UBA will pick up an anomaly that other technologies would miss.

CISOs should look around their network and that of their peers who have been breached and ask if their own network may be the next statistic. Where are the weaknesses and how would an attacker defeat the controls in place?

In doing so, don't get overly focused on compliance. Yes, compliance has its place and it is necessary, but it cannot be the driving force to stop a breach. UBA is not a compliance strategy. It is a risk and threat management solution to address inside threat.

Even the best endpoint security designed to withstand any malware that comes at it does not protect against an employee selling their credentials on the open market. If an adversary, for example, offers employees $100,000 for their credentials, eventually one of them may sell their credentials. Does the current security posture defend against this type of attack? There's no malware involved, nothing to set off the IPS, no traffic denied by the firewall. How does one address this threat? UBA for Surescripts is a key part of the strategy for dealing with a blind spot and the defense in-depth that needs to evolve.

KEY TECHNOLOGY COMPONENTS WHEN SELECTING A VENDOR

The number one attribute when considering a vendor is to assess the use cases from day one. There are so many traditional and non-traditional UBA vendors on the market and UBA is becoming another way of saying "algorithm." But discerning one algorithm versus another in the proof-of-concept process isn't feasible or a good use of time. The UBA vendors are essentially selling algorithms.

The goal should be to determine how quickly a use case could be executed with the vendor. In the case of Surescripts, the selection of a vendor was one that had turnkey ability to use an agent to generate activity, and technology integration to augment DLP concerns. Once the alerting begins, there are risk models and dashboards on which to focus.

What a CISO does not want is an algorithm looking for a problem, because what this leads to is an algorithm requiring internal resources to maintain.

Likewise, beware of the hidden purchase costs. For example, the solution may only sell for $50,000, but the implementation between professional services and the internal security team could eclipse $500,000. UBA could become the next Governance, Risk and Compliance (GRC) or ERP solution that seems to continually drain human and financial resources because it requires customization to meet use cases versus use cases being met from day one.

Surescripts sought UBA vendors who could execute quickly with customization as needed, but more importantly out-of-the-box use cases were provided. It also was important that the vendor who generate more revenue in product sales than professional services.

THE OUTCOME AFTER IMPLEMENTING UBA

Outcomes vary, but for Surescripts the team has made great strides to elevate the defenses. UBA, helped address the blind spots that needed to be addressed. Malware protection, privileged identities, SIEMs, and DLP were of course in place, but even so, there always is room for improvement to advance as the adversary continually advances.

On top of this, just like any security tool, the right solutions must be placed in the teams' hands in order to do the job they were brought on-board to do. This is why Surescripts sought a solution where the team's work was supplemented in ways where other technologies were not helping. Now when the team gets alerts they have the high fidelity events. This detail means the team is not required to spend hours to decipher the incident, the solution does it for them. Mind you, there is still response work needed, but the upfront analytics is provided to the team in a manner they can work with.

UBA'S DEPLOYMENT IMPACT ON STAFFING LEVELS

UBA for Surescripts has become net-net in terms of staffing because of the information that it brings in that needs to be analyzed, but at the same time the UBA brings in algorithms that self-analyze. For Surescripts, there is no longer this need to look for a needle in a haystack because UBA brings the needles to the forefront. Essentially, the team is looking at very meaningful, enriched data. The solution will provide awareness that an employee accessed and downloaded terabytes of data whereas in the past with the noise of the SIEM this event may have gone unnoticed or taken a lot more resource to get to the core of the event.

When comparing this level of detail to data that would have been looked at through a SIEM, we find that the SIEM would have required more analysts to get the same result. UBA produces higher fidelity information that means there is less of a need to do analytics because the solution does that. On the other hand, the data is so useful that it can justify additional headcount in other areas such as incident responders or forensics staff.

In the end, additional staff are not needed to manage UBA, but rather one could argue there is a greater need to expand the team to take action on the increased number of events that have been detected. In other words, the need for UBA administration does not create a need to grow the team, but there must be a team of sufficient size to handle the response.

PEER RECOMMENDATIONS AND ADVICE

Security leaders, your mileage may vary and will depend on which product is selected. It requires that leaders look at their current staff and determine if they have the talent to sustain the investment. Yes, there is a lot that UBA does for the analyst, but at the same time it does bring new responsibilities for investigation and response.

The solution out-of-box will produce valuable data, but will also require different skillsets of the team. Do these skillsets exist today, or will this require addition to headcount? One can liken this to SIEMs. They are great collectors and aggregators, but they are also what one makes of them. CISOs would quickly notice there are a lot of events, but if there is no one capable of responding to them, the team is no further ahead. UBA could result in more work, not less.

Also, if the solution being looked at is very customizable and could do wonderful things with a data science team, then unless you have a data science team at your disposal, these might be solutions to avoid because they are going to potentially put additional strain on the team to get value.

This is why out-of-the-box use case scenarios met are generally a better decision. The bar is a much lower point of entry into UBA if you pick the right product.

SUMMARY

Surescripts strategic deployment of UBA has provided the business use case benefits of augmented DLP and credential misuse detection. This implementation provided the insight into the users' conduct within the network that supports billions of transactions annually. The security team now has better visibility into the behavior of users as opposed to traditional whitelisting and awareness-type data that lacked context. The company's view of inside risk is now more holistic because it includes both the employees who may go rogue as well as attackers who may gain access to an account and thus become an inside threat.

This contribution was prepared while Paul Calatayud was employed at Surescripts as Chief Information Security Officer. The information and opinions expressed in this contribution are the author's own and do not necessarily reflect the current view of Surescripts.

Appendix A – Compliance

REGULATION / STANDARD	CONTROL REQUIREMENT	USER BEHAVIOR ANALYTICS
GLBA	501 (b) - Protect against any anticipated threats or hazards to the security or integrity of such records	Identify access risks to Nonpublic Personal Information to determine mitigating actions
GLBA	501 (b) - Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer	Monitoring of user behavior to ensure proper access and use of customer Nonpublic Information and other confidential financial information
BSA	12 CFR 21.21 - Procedures for monitoring Bank Secrecy Act (BSA) Compliance	Monitoring BSA-related IT control effectiveness and providing related reporting.
HIPAA	Security Rule - Administrative Safeguards - Access to EPHI must be restricted to only those employees who have a need for it to complete their job function	Monitoring access rights and changes to files containing EPHI to ensure patient record confidentiality and integrity
HIPAA	Security Rule - Administrative Safeguards - Review operations to identify potential security violations	Detection of behavior deviation to identify a possible security violation
HIPAA	Access to hardware and software must be limited to properly authorized individuals	Analysis of physical space access data to uncover unauthorized activity in the physical space
HIPAA	Security Rule - Technical Safeguards - Ensure data within systems has not been changed or altered in an unauthorized manner	Monitoring of file attributes for access and changes
SOX	Section 404 - Assess both the design and operating effectiveness of access controls	Ensure access is limited to authorized users for authorized business and that separation of duties is maintained by examining behavior of access against peers and role requirements
SOX	Section 404 - Perform a fraud risk assessment	Assess access rights and trends to maintain principle of least privilege

SOX	Section 404 - Evaluate controls used to detect or prevent fraud	Incorporate external information such as credit scores and debt records to predict a potential fraud risk
SOX	Section 404 - Monitor the information security program, infrastructure, and controls to ensure proper effectiveness in securing the company financial information	Monitor for unauthorized attempts to access and manipulate corporate confidential financial information
PCI	Implement strong access control measures - Restrict access to cardholder data by business need-to-know	Analyze access of cardholder data to uncover unusual trends
PCI	Implement strong access control measures - Assign a unique ID to each person with computer access	Uncover sharing of credentials through analysis if user account actions
PCI	Regularly monitor and test networks - Track and monitor all access to network resources and cardholder data	Construct baselines of user access behavior based on authorized actions and monitor for deviations to the baseline
NIST 800-53 REV 4	AC-3 - Access Enforcement - Determine if the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies	Analyzes and reports on user access to information systems and alerts on significant changes in access activities
NIST 800-53 REV 4	AU-6 - Audit Review, Analysis, and Reporting - Determine if the organization reviews and analyzes information system audit records for indications of organization-defined inappropriate or unusual activity with the organization-defined frequency	Provides records of information systems access for auditing to determine presence of unusual activity as measured against a known baseline and established policies

NIST 800-53 REV 4	AU-13 - Monitoring for Information Disclosure - Determine if the organization employs automated mechanisms to determine if organizational information has been disclosed in an unauthorized manner	Provides constant automated monitoring of user behavior including information accessed
NIST 800-53 REV 4	CM-5 - Access Restrictions for Change - Determine if the organization enforces logical access restrictions associated with changes to the information system	Changes in user access restrictions are baselined and referenced for analysis of future user access activity
NIST 800-53 REV 4	IR-6 - Incident Reporting - Determine if the organization employs automated mechanisms to assist in the reporting of security incidents	Provides automated information on user activity related to information security incidents
NIST 800-53 REV 4	PS-2 - Position Risk Designation - Determine if the organization assigns a risk designation to all organizational positions	Risk-score employees by incorporating roles, use analysis, and outside information such as performance reviews
NIST 800-53 REV 4	SI-4 - Information System Monitoring - Determine if the organization monitors the information system to detect, in accordance with organization-defined monitoring objectives attacks and indicators of potential attacks	Analysis of user behavior can uncover attacks in progress or indicate potential attacks based on user risk score
ISO 27001-2013	A.6.1.2 - Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets	Monitors and reports on violations of organizational-defined information system separation of duties
ISO 27001-2013	A.7.2.1 - Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization	Monitors for employee information system misuse within established policies and procedures

ISO 27001-2013	A.8.1.3 - Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented	Monitors for employee information system misuse within established policies and procedures
ISO 27001-2013	A.9.1.2 - Users shall only be provided with access to the network and network services that they have been specifically authorized to use	Ensures actual access activities of users are authorized
ISO 27001-2013	A.9.2.5 - Asset owners shall review users' access rights at regular intervals	Continuous monitoring if user access behavior
ISO 27001-2013	A.9.4.1 - Access to information and application system functions shall be restricted in accordance with the access control policy	Ensure actual user behavior matches required information system restrictions
ISO 27001-2013	A.12.4.1 - Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed	Provides a detailed log of user activities
FACTA	Red Flag Rule - Implement reasonable policies and procedures for detecting, preventing, and mitigating identity theft	Analyze new and existing accounts at financial institutions to detect variations in usual customer behavior that may indicate identity theft
FERPA	Conditions under which student records may be released	Monitoring of employee access to and manipulation of student electronic records
NIST Cybersecurity Framework	PR.AC-4 - Access permissions are managed, incorporating the principles of least privilege and separation of duties	Ensures proper management of access permissions through analysis of access events
NIST Cybersecurity Framework	PR.DS-5 - Protections against data leaks are implemented	Examines and reports on information manipulation by users

NIST Cybersecurity Framework	PR.DS-6 - Integrity checking mechanisms are used to verify software, firmware, and information integrity	Reports on unauthorized changes to files
NIST Cybersecurity Framework	PR.PT-3 - Access to systems and assets is controlled, incorporating the principle of least functionality	Verifies access to systems is controlled by comparing user access actions to established corporate security policy
NIST Cybersecurity Framework	DE.AE-1 - A baseline of network operations and expected data flows for users and systems is established and managed	Establishes a baseline of normal user activity
NIST Cybersecurity Framework	DE.CM-3 - Personnel activity is monitored to detect potential cybersecurity events	Monitors personal activity for anomalies
Indian Gaming Regulatory Act	2706-b - Monitoring; inspection of premises; investigations; access to records; mail; contracts; hearings; oaths; regulations	Monitors internal controls of gaming systems
FFIEC Cybersecurity Assessment Tool	D3.PC.Im.B.7 - Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored	Monitors system administrator use behavior
FFIEC Cybersecurity Assessment Tool	D3.PC.Am.B.1 - Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege	Ensures actual employee access behavior conforms to established policies and baselines
FFIEC Cybersecurity Assessment Tool	D3.PC.Am.B.2 - Employee access to systems and confidential data provides for separation of duties	Ensures actual access conforms to separation of duties

FFIEC Cybersecurity Assessment Tool	D3.PC.Am.B.3 - Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls)	Monitors elevated privilege account actions for deviations from baseline and expected behavior
FFIEC Cybersecurity Assessment Tool	D3.PC.De.B.1 - Controls are in place to restrict the use of removable media to authorized personnel	Monitors user behavior for unauthorized attempts to use removable media
FFIEC Cybersecurity Assessment Tool	D3.PC.De.E.4 - Controls are in place to prevent unauthorized individuals from copying confidential data to removable media	Monitors user behavior for unauthorized attempts to copy confidential data
FFIEC Cybersecurity Assessment Tool	D3.DC.An.B.1 - The institution is able to detect anomalous activities through monitoring across the environment	Constant monitoring of user activities
FFIEC Cybersecurity Assessment Tool	D3.DC.An.B.5 - Elevated privileges are monitored	Establishes a baseline of normal user activity
FFIEC Cybersecurity Assessment Tool	D3.DC.Ev.B.1 - A normal network activity baseline is established	Analysis of user activity can detect insider activity
FFIEC Cybersecurity Assessment Tool	D5.DR.De.E.1 - The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction	Analysis of user activity can detect insider activity

Appendix B – Supplemental Information & Resources

References

Armerding, T. (2016, May 14). Top 15 Security Predictions for 2016. Retrieved November 7, 2016, from CSO Online: http://www.csoonline.com/article/3013060/security/top-15-security-predictions-for-2016.html

Ashford, W. (2015, August 3). Why the Time is Ripe for Security Behaviour Analytics. Retrieved November 7, 2016, from ComputerWeekly: http://www.computerweekly.com/news/4500251006/Why-the-time-is-ripe-for-security-behaviour-analytics

BakerHostetler. (2016). 2016 Data Security Incident Response Report. Retrieved November 7, 2016, from Baker & Hostetler: https://bakerlaw.com/files/uploads/Documents/Privacy/2016-Data-Security-Incident-Response-Report.pdf

Dell. (2016). 2016 Dell Security Annual Threat Report. Retrieved November 7, 2016, from SonicWall: https://www.sonicwall.com/whitepaper/2016-dell-security-annual-threat-report8107907

IBM and Ponemon Institute. (2016). 2016 Cost of Data Breach Study: Global Analysis. Ponemon Institute. Retrieved November 7, 2016, from https://securityintelligence.com/media/2016-cost-data-breach-study/

Information Security Forum Limited. (2016). Threat Horizon 2016 - On the Edge of Trust. Retrieved November 7, 2016, from Information Security Forum Limited: https://www.securityforum.org/research/threat-horizondge-of-trust-2/

Institute for Information Security and Privacy. (2016). Emerging Cyber Threats Report 2016. Retrieved November 7, 2016, from Georgia Tech Institute for Information Security and Privacy: http://www.iisp.gatech.edu/2016-emerging-cyber-threats-report

Lemos, R. (2015, March). The Hunt for Data Analytics-Is Your SIEM on the Endangered List? Retrieved November 7, 2016, from TechTarget SearchSecurity: http://searchsecurity.techtarget.com/feature/The-hunt-for-data-analytics-Is-your-SIEM-on-the-endangered-list

Mandiant Consulting. (2016). M-Trends 2016. Retrieved November 7, 2016, from FireEye: https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf

Privacy Rights Clearinghouse. (2016). Privacy Rights Clearinghouse. Retrieved November 7, 2016, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breaches

Reiner, R. (2016, January 4). Is the Password Dead? The Future of Web and Mobile Authentication. Retrieved November 7, 2016, from Techcrunch: http://techcrunch.com/2016/01/04/is-the-password-dead-the-future-of-web-and-mobile-authentication/

RightScale. (2016). 2016 State of the Cloud Report. Retrieved November 7, 2016, from RightScale: https://www.rightscale.com/lp/state-of-the-cloud

Rogers, E. M., & Shoemaker, F. F. (1971). Communication of Innovations. New York: The Free Press.

Rouse, M. (n.d.). What is User Behavior Analytics (UBA)? Retrieved November 7, 2016, from SearchSecurity - TechTarget: http://searchsecurity.techtarget.com/definition/user-behavior-analytics-UBA

Shackleford, D. (2015, November). 2015 Analytics and Intelligence Survey. Retrieved November 7, 2016, from SANS: https://www.sans.org/reading-room/whitepapers/analyst/2015-analytics-intelligence-survey-36432

Society for Human Resource Management. (2016, January 7). Using Social Media for Talent Acquisition - Recruitment and Screening. Retrieved November 7, 2016, from Society for Human Resource Management: https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/pages/social-media-recruiting-screening-2015.aspx

U.S. Bureau of Labor Statistics. (n.d.). Information Security Analysts. Retrieved November 7, 2016, from Occupational Outlook Handbook: http://www.bls.gov/ooh/computer-and-information-technology/mobile/information-security-analysts.htm

Verizon. (2016). 2016 Data Breach Investigations Report. Retrieved November 7, 2016, from Verizon: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

The following companies where invited to participate in this report by completing an RFI created by CISOs:

- Bay Dynamics
- Dtex Systems
- E8 Security
- Exabeam
- Fortscale
- Gurucul
- Interset
- LightCyber
- LogRhythm
- Niara
- NuData Security
- Preempt Security
- Prelert
- RedOwl
- Securonix
- Splunk
- Sqrrl
- Varonis
- Veriato

Appendix C – Vendor RFIs

COMPANY					
Exabeam 1 Waters Park Drive San Mateo, CA 94403 USA					
WEBSITE					
www.exabeam.com					
CONTACT					
Rick Caccia CMO 844.EXABEAM 650-899-2228 rick@exabeam.com					
INVESTMENT INFORMATION					
Founded in 2013					
Privately Held					
OFFICE LOCATIONS					
Headquarters 1 Waters Park Drive San Mateo, CA 94403 USA	**R&D** 1 Waters Park Drive San Mateo, CA 94403 USA	**Support** 1 Waters Park Drive San Mateo, CA 94403 USA			
MANAGEMENT TEAM					
Nir Polak CEO	Sylvain Gil VP Products	Domingo Mihovilovic CTO	Ralph Pisani EVP Field Operations	Rick Caccia CMO	Patrick Zanoni VP Finance
EMPLOYEES					
Total Number: 100	**Total Technical:** 50	**Total Support:** 7			
CUSTOMER BACKGROUND					
Total Customers: 75	**Total UBA Customers:** 75	**Total UBA POCs:** 120			
Markets: Banking Consumer	Engineering Energy (Oil & Gas) Finance	Government (Federal) Healthcare Insurance	Manufacturing Retail Technology		

CUSTOMER UBA INFORMATION

Average End-user Revenue: $5B	**End-user Employees:** 25,000	**Regulations:** PCI, SOX for Banking SOX for Energy SOX, Dodd-Frank, PCI for Finance	FISMA for Government SOX, HIPAA for Healthcare SOX for Insurance SOX for Manufacturing	PCI, SOX for Retail SOX for Technology

UBA PRODUCT OVERVIEW

Exabeam User Behavior Analytics
Exabeam Threat Hunter

Launched on:
February 1, 2015
February 19, 2016

PRODUCT OVERVIEW

• Exabeam UBA	Exabeam UBA improves security via a patented session data model that connects activities into coherent user sessions, builds baselines of normal behavior for each user, then detects anomalous and risky behavior. Exabeam UBA accelerates post-incident investigations by presenting a logical story of the attack, from beginning to end, reducing hiring pressure for the SOC.	General Availability Date: February 1, 2015
• Exabeam Threat Hunter	Exabeam Threat Hunter brings proactive query, pivot, and drill-down capabilities to any analyst in the SOC. With Threat Hunter, analysts can proactively find and respond to adversaries on the network. Threat Hunter uses Exabeam's patented session data object to query sessions by any combination of attributes or activities, without requiring an analyst to understand the underlying log query language.	General Availability Date: February 19, 2016

PRODUCT DESCRIPTION

Exabeam UBA

Exabeam UBA uses a combination of machine learning and research-driven security rules to derive context around user and entity behavior and the network environment. While Exabeam uses many cutting-edge techniques, such as peer group analysis, supervised and unsupervised learning, host classification, etc., the greatest strength of the product is the capability to produce, in plain English, a coherent story of an attack. The result is an investigation timeline, produced in seconds instead of days.

Application Development Process

PRODUCT ACQUISITION		
Exabeam User Behavior Analytics	Built in-house	
Exabeam Threat Hunter	Built in-house	

UBA PRODUCT ROADMAP & DEVELOPMENT

As a private company, Exabeam does not divulge product roadmaps in a non-confidential setting

Exabeam is a rapid-release development organization, producing minor releases approximately every six weeks.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

- Exabeam performs machine-learning and security research-driven analytics of user behavior, based on a patented session data model

Integration

- Exabeam can ingest any type of data, including log, endpoint, DLP, physical badge reader, and network data.

Platform

- Elegant and intuitive browser-based GUI

Platform (In-house)

- Self-contained physical or virtual appliance

Platform (Cloud)

- Virtual appliance can be deployed in any cloud

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Communication applications such as email and Skype
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems (Raytheon Websense, Zscaler for example)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Machine fingerprint
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank certain countries higher risk than other
- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

Exabeam installs in several hours and typically produces learning-driven models and results within two days.

Baseline Process

Exabeam creates sessions from each user's activities, then uses those sessions to create normal baselines on a per user basis. New activity is compared to the baselines to identify behavior that is anomalous and risky. If desired, baselines can be updated with specific sessions.

REPORTS

Administrators

- Risky users, watchlist users, unusual account lockouts, geographical access points, top talkers, most accessed systems, etc.

Security Executive

- Risky users, watchlist users, unusual account lockouts, geographical access points, top talkers, most accessed systems, etc.

C-Suite

- Risky users, watchlist users, unusual account lockouts, geographical access points, top talkers, most accessed systems, etc.

Board of Directors

- Risk at a department or geographical level

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Total users
- Users with threats
- Total devices
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

- Bi-directional integration to SIEM consoles

ADDITIONAL INFORMATION

Awards

- Gartner Cool Vendor in Security Intelligence, 2015

DIRECT QUESTIONS

Rick Caccia
CMO
844.EXABEAM
650-899-2228
rick@exabeam.com

COMPANY

Fortscale
1400 Fashion Island Blvd. Suite 810
San Mateo, CA, 94404
USA

WEBSITE

www.fortscale.com

CONTACT

Alex Berger
Director of Product Marketing
(914) 420-5569
alexb@fortscale.com

INVESTMENT INFORMATION

Founded in 2013

Privately Held

OFFICE LOCATIONS

Headquarters
1400 Fashion Island Blvd. Suite 810
San Mateo, CA, 94404
USA
+1 650 397-9630

R&D
19D Habarzel St.
Tel Aviv
6971025
Israel
+972 (3) 600-6078

Support
275 Grove Street
Suite 2-400
Boston, MA, 02466
USA

MANAGEMENT TEAM

Idan Tendler CEO & Cofounder	Dr. Yona Hollander COO & Cofounder	Kurt Stammberger CMO	Ophir Rachman CTO, VP R&D	David Somerville SVP Global Sales	Tzlil Perker CFO

EMPLOYEES

Total Number: 44 | **Total Technical:** 29 | **Total Support:** 3

CUSTOMER BACKGROUND

Total Customers: 14	**Total UBA Customers:** 14	**Total UBA POCs:** 44			
Markets: Automotive Banking	Consumer Finance Healthcare	Insurance Manufacturing Retail	Technology Telecom		

CUSTOMER UBA INFORMATION

Average End-user Revenue: $1B	**End-user Employees:** 3,500	Sarbanes-Oxeley, Graham Leach Bliley, EFT, PCI-DSS, FACTA, FISMA for Banking GLB, PCI-DSS, COPPA, FACTA for Consumer SOX, GLB, EFT, PCI-DSS, FISMA for Finance	21CFR11, HIPAA, HITECH, CFATS for Healthcare SOX, Graham Leach Bliley, FACTA, HIPAA, HITECH for Insurance SOX, CFATS for Manufacturing PCI-DSS, EFT, GLB, COPPA for Retail	SOX, GLB, EFT, PCI-DSS, COPPA for Technology SOX, GLB, EFT, PCI-DSS, COPPA for Telecom

UBA PRODUCT OVERVIEW

Fortscale 2.5 (current release)

Launched on:
June 15, 2015

PRODUCT OVERVIEW

• Fortscale	Fortscale detects insider threats by identifying anomalous behaviors that correlate with the theft or abuse of legitimate credentials within the network. It does this completely autonomously, via advanced machine learning techniques, and without relying on human-generated rules or policies. As a result, Fortscale's software tends to be "quieter" and more accurate than other UBA offerings, helping analysts stay sane and be more productive by blocking false positives that plague other UBA's. Because there are no rules to write, customers save BIG on professional services and scaling costs. Fortscale offers the easiest setup and fastest install experience among the major UBA players, with the fastest time-to-value in the UBA market. Ultimately, Fortscale lowers security analysts stress levels and helps the whole SOC work better.	General Availability Date: June 15, 2015

PRODUCT DESCRIPTION

Fortscale

Fortscale has four main components: ingestion, enrichment, behavior modeling & analysis, and alerts & reports. Raw Logs are ingested directly from the customer's existing SIEM. (Fortscale is opimized for SPLUNK and IBM QRADAR, but can work with other SIEMS too.) Fortscale can be configured to ingest virtually any data source, including contextual, authentication, access and configuration data. Once ingested, Fortscale enriches the data by tagging and appending it as much as possible against local LDAP and Active Directory records. This aids with machine learning, semantic resolution for alerts, and organizational peer group formation and validation. Tags can be gathered from the environment or be completely arbitrary to accommodate organization-specific behavioral models. Enriched data is then fed into our proprietary autonomous machine-learning engine for behavior modeling & analysis. Fortscale builds a separate model for each user or entity on the fly and begins to form a "machine opinion" about what is "baseline" behavior for that user. Baselines are continuously updated. Fortscale's machine-learning engine create peer groups autonomously, based on observed behaviors, not human constructs like "job title". This delivers dramatically better output than rule-based UBA peering. Fortscale's global models also look at the entire organization, and are able to recognize larger patterns that are true to significant, yet non-obvious, subsets of the user population. Statistical analysis on behavioral anomalies is correlated with contextual information to inform the risk rating eventually assigned to a given "indicator". Each Alert is generated based on the consideration of many seemingly unrelated individual indicators together. Each Alert is scored and prioritized before it ever lands on the Analysts' console, helping harried analysts intelligently parse their time. Analysts can "drill down" into any alert with a single click to examine the indicators that built it. Finally, a generous collection of pre-formatted Reports help analysts communicate risks to their teams - and to executive management - in compelling, easy to understand terms.

PRODUCT ACQUISITION

Fortscale	Built in-house

Application Development Process

UBA PRODUCT ROADMAP & DEVELOPMENT

- Q2'16: New Alert Types, New Data Sources.
- Q3: Multiple Install & Ease-of-Use Enhancements; we want Fortscale to be the ""Easy, Hands-Free UBA"". New UI pivots on User Scores. UBA--> XBA. Analyst Tuning.
- Q4: Cloud behavior analysis. Smarter Peering. Semantic Alerts. Custom Tags. Alert Resolution in SIEM. Enhancements for SPLUNK Users.
- Q1'17: Enterprise Apps behavior analysis. Spontaneous Multialert Grouping. Arbitrary Data Ingestion. Enhancements for IBM QRADAR Users

Fortscale uses an agile development process. Our development philosophy has two main foci: flexibility and quality. Product management, engineering, and development teams work in tandem to finalize features based on a prioritized roadmap. We support two different types of releases: - Quarterly Releases - these releases contain our major new features, existing feature enhancements, and general product maintenance. - Patch Releases (as needed) - our support engineers are always on the lookout for feedback from our customers, and when issues are discovered in the product, we are quick to address them via a patch.

All releases undergo thorough QA
- Unit tests are performed regularly by engineering
- Code reviews are a mandatory check-in step during development
- All functionality undergoes regression testing prior to release

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

Fortscale's unique anomaly detection engine synthesizes the rarity and risk of an event into a distinctive normalized score based on three layers of machine learning analysis:

1. Parameter-level modeling - Detects deviations from baseline behaviors based on parameters (i.e. IP addresses, locations, timestamps, etc.) combined with historical data.
2. Group-level modeling - Uses data-clustering techniques to assess environmental rarity of a user's activity relative to overall organizational activity.
3. Statistical modeling - Synthesizes behavioral deviations across multiple dimensions to generate a unified final threat score reflecting threat level.

Fortscale's analytics algorithms were built to provide generalizable user behavior analytics for any network environment. Our algorithms are designed to be application-agnostic, enabling quick adaptation, easy re-tasking and painless re-deployment in new environments without having to start from scratch with a new rule-list. Custom tweaks to scoring models can be made according to customer requests."

Integration

Fortscale digests logs from virtually anything that produces them (e.g., big-data repositories, Hadoop, SIEM/Splunk). A collection module receives structured and unstructured data that can either be streamed or batch-loaded, according to customer needs. Data can be loaded into Fortscale using a built-in syslog connector or using a destination folder monitoring service. A standard deployment of Fortscale includes log ingestion of Kerberos and NTLM authentication, SSH, and VPN (Cisco ASA, Juniper, F5, and more), Windows Events (Account Management, group changes, password changes/resets, account lockouts) and printing logs. CRM and other proprietary sub-system (enterprise applications such as Oracle DB and Salesforce) logs can also be ingested, preferably via SIEM (Splunk and IBM QRADAR are our favorites).

Presentation

Fortscale has several advanced capabilities that help security personnel rapidly see the full context of user actions and make fast, appropriate decisions. These features include Fortscale SMART Alerts, which provide semantic information to aid in analyst understanding and prioritization; and an alert-based dashboard with single-screen investigation, allowing analysts to dive into the details of an alert through a single pane of glass. In addition to the real-time alert and investigation capabilities, Fortscale offers analysts in-depth reports. These reports give additional insights into historic anomalous behaviors across all data sources, and are always supported by contextual data to shed light on potentially hazardous conditions that exist in the environment.

Platform (In-house)

Fortscale is an on-prem software solution. The solution is a self-contained installation on a RedHat server, but can also be deployed directly to a Virtual Machine. The system provides fully independent data storage and querying solutions using MongoDB as an online pathway and Hadoop as an offline pathway. When you're ready to deploy, Fortscale will recommend specific hardware spec for your Fortscale instance, and our professional services team will work with you to install the software itself, as well as any adjacent systems you might need (such as Cloudera Hadoop). Fortscale's professional services team will also provide on-site training and ongoing support.

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Communication applications such as email and Skype
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems (Raytheon Websense, Zscaler for example)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Geographic location
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank certain countries higher risk than other
- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules only as an "after filter" (Machine Learning Engine does the heavy lifting)

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

Fortscale customer success engineers typically "prime" a new Fortscale instance with a few months worth of the customer's own access and authentication logs. This enables the Fortscale machine learning system to grow from an "infant" to a "teenager" overnight, with a fairly good starting model of the users in the systems and their baseline behaviors. During the first week or two, Fortscale engineers monitor your new instance remotely via VPN, and help it "learn" as efficiently as it can, correcting the nascent ML system when it makes naive mistakes, but also striving to let the system "grow up" unhindered as much as possible. Less interference usually results in a better performing, more accurate and more automatomous ML UBA in the end.

Baseline Process

Fortscale immediately begins to build behavioral models of every entity (user, machine, server) in the environment once it's installed. These models consist of three main components; the entity itself, the type of behavior (e.g. logins), and a measurement of the behavior (i.e. time of day, geographic location, etc.). Over time, more data is added to the model and each model represents the behavioral baseline of the entity. When Fortscale detects a deviation from these baselines, it labels the deviation as an "indicator", but not yet an "alert". Many UBA products surface these types of anomalies to users as alerts, but these indicators are triggered all the time during normal business processes. For example, when an employee travels to an office in another location, an indicator may be triggered based on the fact that they are logging in from a different location. Fortscale is unique in that it builds a secondary baseline for each entity based on the indicators commonly triggered. This creates a much more accurate portrayal of the entity's baseline behavior, thereby improving accuracy and limiting false positives.

REPORTS

High Privileged Users

- Admins – Information about Admins risky behaviors
- Executives – Information about Executives risky behaviors
- Service Account – Information regarding a service account risky behaviors

Top Suspicious Users

- Top Suspicious Users
- SSH – Top Suspicious Users - The users with the highest risk scores in SSH
- VPN – Top Suspicious Users - The users with the highest risk scores in VPN
- Kerberos – Top Suspicious Users - The users with the highest risk scores in Kerbe

External Access to the Network

- Suspicious Amount of Data Over VPN – Used to identify an abnormal amount of data that is transferred out of the organization in a VPN session
- VPN Geo-Hopping – Used to identify abnormal VPN connections for users who are connecting from various countries in a short and unreasonable timeframe

Device Investigation

- IP Investigation – Used to summarize important information that was gathered for a specific IP address
- Suspicious Device Access – Used to identify abnormal access to endpoints in the organization Sensitive Resources Monitoring - Summary of information about machines which were tagged as sensitive by the customer

Stale Accounts

- Disabled Accounts – Summary of relevant and up to date information regarding users whose Active Directory accounts are disabled
- Inactive Accounts – Summary of relevant and up to date information about accounts which are inactive, but are not disabled
- Disabled Accounts with Network Activity – Summary of relevant and up to date information regarding users whose Active Directory accounts are disabled, but still show activity

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Total users
- Users with threats
- Total devices
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

SIEM:

- Best integrations are with Splunk and IBM QRADAR Siems.
- Lesser integrations available for other SIEMS.

QUESTIONS

Alex Berger
Director of Product Marketing
(914) 420-5569
alexb@fortscale.com

COMPANY

LogRhythm, Inc.
4780 Pearl East Circle
Boulder, Colorado, 80301
USA

WEBSITE

www.logrhythm.com

CONTACT

Mark Settle
Product Marketing Team Manager
720.403.9025
Mark.Settle@LogRhythm.com

INVESTMENT INFORMATION

Founded in 2003

Privately Held

OFFICE LOCATIONS

Headquarters 4780 Pearl East Circle Boulder, Colorado, 80301 USA 303.413.8745	**R&D** 4780 Pearl East Circle Boulder, Colorado, 80301 USA 303.413.8745	**Support** 4780 Pearl East Circle Boulder, Colorado, 80301 USA 303.413.8745				

MANAGEMENT TEAM

Andy Grolnick CEO	Chris Petersen CTO / Co-Founder / SVP Support	Mike Reagan CMO	Mark Vellequette CFO	James Carder CISO	William Smith SVP WW Field Ops	Chris Brazdziunas SVP of Products

EMPLOYEES

Total Number: 550	**Total Technical:** 110	**Total Support:** 100				

CUSTOMER BACKGROUND

Total Customers: 2,800	**Total UBA Customers:** 1,100					
Markets: Banking Education	Engineering Energy (Oil & Gas) Finance	Government (Federal) Government (Local)	Healthcare Insurance Manufacturing	Media Retail Technology	Telecom	

CUSTOMER UBA INFORMATION

Average End-user Revenue:	End-user Employees:	Regulations:		
>$1B	>100,000	SOX, PCI, GBA for Banking PCI for Education SOX, NERC CIP for Engineering NERC CIP, SOX for Energy SOX, GLBA, PCI for Finance	FISM for Government HIPAA, PCI for Healthcare HIPAA, PCI, SOX for Insurance NIST 800-53, NIST CSR, NERC CIP for Manufacturing SOX for Media	PCI for Retail NIST 800-53, NIST CSF, NERC CIP for Technology NIST 800-53, NIST CSF, NERC CIP for Telecom

UBA PRODUCT OVERVIEW

LogRhythm Security Intelligence Platform
AI Engine
User Threat Detection Module

Launched on:
October 2005 (Security Intelligence Platform)
June 2010 (AI Engine)
July 2013 (User Threat Detection Module)

PRODUCT OVERVIEW

• Security Intelligence Platform (Version 7.2)	LogRhythm's unified Security Intelligence Platform is the foundation for our User Behavior Analytics (UBA) solution. It delivers next-generation SIEM, log management, endpoint/network monitoring and forensics, security analytics (including UBA, network threat detection, and endpoint threat detection), and end-to-end threat lifecycle management. The platform provides profound visibility into threats and risks to which organizations are otherwise blind. Designed to help prevent breaches before they happen, it detects an extensive range of early attack behavior, enabling rapid response and neutralization. The deep visibility and understanding delivered by LogRhythm's Security Intelligence Platform empowers enterprises to secure their environment and comply with regulatory requirements.	General availability date: October 2005 Last updated: November 2016
• AI Engine	AI Engine is our proprietary and patented, stream-based machine analytics technology that provides real-time, automated analysis of contextualized machine and forensic data received from Data Processors. AI Engine supports a variety of automated analytic techniques and generates risk-prioritized alarms that are transmitted to our Platform Manager. Multiple AI Engine nodes can be deployed to support distributed analysis and workload scaling.	General availability date: June 2010 Last updated: November 2016
• User Threat Detection Module (Version 3.0)	User Threat Detection Module (UTDM) is a highly specialized and advanced set of prepackaged content that gives users extensive visibility into user activity and related threats. It leverages several machine analytics techniques to detect threats such as insider threats, compromised accounts, and privilege abuse. The module is provided to customers as part of their support and maintenance plan, at no additional charge. The content is fully customizable by customers. Corresponding modules are available for network threat detection and endpoint threat detection, enabling customers to expand their security analytics capabilities over time.	General availability date: July 2013 Last updated: December 2016

Application Development Process

PRODUCT DESCRIPTION

LogRhythm User Behavior Analytics (UBA)

LogRhythm User Behavior Analytics (UBA) provides deep visibility into user activity, helping detect insider threats, compromised accounts, privileged account abuse, and other user-based threats. It leverages identity and access management information, internal and external context, and machine data collected from across the enterprise to understand user behavior and identify unusual user activity. LogRhythm UBA uses both machine learning to detect anomalies without pre-knowledge of attack techniques and rules-based analytics to detect known threat activity patterns.

LogRhythm UBA leverages user authentication and activity logs, and can be enriched with the collected and generated endpoint and network data to support the identification, corroboration and prioritization of alarms.

LogRhythm automates the association of even anonymous data to specific identities by applying multiple techniques across current and historic activity LogRhythm can infer additional identity information from unauthenticated logs by analyzing an individual's behavior relative to learned ad hoc groups LogRhythm also integrates with user directories such as Active Directory to provide group and subgroup membership data for individual users.

LogRhythm UBA is designed to address the following use cases and indicators of compromise:

- Insider Threats IOCs (e.g., unusual file modifications, unusual file accesses, data exfiltration)
- Account Takeover IOCs (e.g., abnormal authentication activity, abnormal user application behavior, compromised hosts, lateral movement following an attack, concurrent logins from multiple locations, account activity from blacklisted locations, brute force attacks)
- Privileged Account Abuse IOCs (e.g., suspicious temporary account activity, unusual account privilege escalation, abnormal account administration)

- LogRhythm's full UBA solution has been developed in-house. For certain components, it leverages open source software (e.g., Elasticsearch powers our persistence tier). But ultimately, everything has been developed from the ground up by LogRhythm developers, including the Security Intelligence Platform, AI Engine, and our User Threat Detection Module. This eliminates the integration challenges of bolt-on UBA offerings, delivers a seamless analyst experience, and ensures the long-term continuity of the teams that have developed these tools. Analytics techniques include:

- Behavioral profiling: Behavioral profiling allows LogRhythm to learn from activity across users, networks, endpoints and applications, such as the systems a user typically accesses or the processes typically running on an endpoint. For example, a user accessing the VPN from a new country may be one activity used as part of a corroborated event.

- Learned and static whitelists & blacklists: Users can leverage learned and pre-set whitelists and blacklists to create rules that trigger or corroborate alarms. An example of a blacklist may be millions of IP addresses or domains inserted into a List from an open source or commercial threat feed.

- Statistical trending: AI Engine uses statistical trending on any quantitative metadata field to learn of peer activities and alarm on deviations, such as recognizing when the number of failed logins by an admin user over the last X days is significantly higher than other peer admins.

- Statistical analysis: Live activity can be measured against a histogram of baselined metadata information. AI Engine can look for deviations to the histogram itself as a metric of significant change (e.g. the types of log activities from a group of systems changing) or recognize individual outliers (e.g. a user is accessing files in a cloud sharing application at a greater rate than peers).

- Corroborated Events: AI Engine's ability to feed events back into itself allows for analytics to capture multiple AI Engine events occurring within a short period of time or perform other analytic techniques (e.g. trends) of AI Engine events. The benefit of a corroborated rule is that the user does not need to program a time sequence like a pattern. AI Engine can recognize multiple AIE Events within a short period of each other with a commonality (e.g. activities with the same user or endpoint)."

PRODUCT ACQUISITION

LogRhythm User Behavior Analytics (UBA)	Built in-house

UBA PRODUCT ROADMAP & DEVELOPMENT

Since first beginning to develop our Security Intelligence Platform over 13 years ago, LogRhythm has been on the leading edge of Security Intelligence, providing actionable intelligence to our enterprise customers. LogRhythm has a proven track record of delivering new capabilities and innovations in each of our major and minor releases as evidenced by our continued growth and industry and customer recognition. LogRhythm is currently on the seventh major release of our award-winning Security Intelligence Platform and we have successful implementations with over 2,800 customers, including some of the largest enterprise organizations, worldwide.

LogRhythm has an aggressive product roadmap and we anticipate continuing to deliver innovations that empower our customers to improve their mean-time-to-detect and respond to threats.

LogRhythm adheres to a standardized release schedule that includes major releases every 6-12 months while minor updates are released 1 to 2 times during that time period. LogRhythm is currently on major release 7.2.2, our most feature-rich and powerful release to date. LogRhythm follows an Agile development methodology which includes change/control management, QA cycles, and takes into account customer feedback provided via our portal, LogRhythm User Groups, Support Tickets, Online Community and other methods for feature requests when developing subsequent releases.

LogRhythm continues to focus research and development efforts to introduce new innovations for next generation SIEM, Log Management, machine analytics, endpoint monitoring and forensics, and network monitoring and forensics. LogRhythm's history of innovation has led to numerous industry awards, including being listed as a leader in the Gartner Magic Quadrant for SIEM from 2012 through 2016; Champion in 4 of 5 use cases in Info-Tech Research Group's 2015 SIEM Vendor Landscape Report, additionally in April of 2015 LogRhythm received recognition from the SANS Institute as "Best SIEM" for 2014, as well as SC Magazine Reader's Trust Award for Best SIEM. These awards are given to organizations with both a history of and expected future of continued innovation and success.

LogRhythm will continue to provide many years of best-in-class products through innovation, industry leading customer-service and an unwavering commitment from every employee to delivering industry leading Security Intelligence solutions on a global scale.

LogRhythm welcomes additional discussion regarding our roadmap under mutual NDA.

LogRhythm adheres to an Agile development methodology for product releases. Within this cycle there is an iterative process for development, which includes the product, engineering, QA and other required teams. Development unit and test code reviews are performed prior to handoff to QA. A fulfilment review then takes place and includes individuals from QA, Development, Engineering and other technical disciplines.

LogRhythm's Security Operations team follows the OWASP Top 10 guidelines at a minimum, as well as more in-depth testing when assessing all LogRhythm web applications. They perform static code review using commercial and open source toolsets for automated analysis, along with manual code review and peer review. In addition to automated security testing, Security Operations performs vulnerability scanning and in-depth penetration testing against the entire product line.

LogRhythm provides customers with periodic updates for upgrades and patches to the LogRhythm platform. Updates are released on an as-needed basis and are thoroughly tested by the Quality Assurance team prior to being approved for installation.

LogRhythm systems are patched using System Center Service Manager in an automated fashion. Critical bugs and vulnerabilities are fixed once they are known to exist, typically via hotfix downloads. Non-critical bugs are fixed once they are known to exist, and fixes are incorporated into upcoming minor releases / updates.

In addition to patches and upgrades, LogRhythm also provides customers with daily Knowledge Base updates. Upgrades and patches are available free of charge as long as maintenance is current. Each update consists of a set of programs and/or files that are posted on the LogRhythm Support Portal. Updates are accompanied by release notes detailing any problems resolved or significant operational changes that may be the result of an update.

LogRhythm utilizes various processes to facilitate continuous improvement. These include but are not limited to our formal and informal conversations with customers, the sponsoring of LogRhythm User Group events, our Executive-level Customer Advisory Board, and others. Feedback also comes in through our support forum in the form of comments, feature requests, etc., and is reviewed by our organization in consideration for product enhancements. As we also use our own product internally, we have hands-on experience about what we like best and what we feel could be improved based on a continuing, real-world use case.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

LogRhythm uses its patented machine analytics technology, "AI Engine", to perform real-time, stream-based analytics across security events, log data, and other forensic machine data.

LogRhythm's AI Engine is able to detect threats and build user and peer profiles using multiple anomaly detection methods, including:

1. 1. Dynamic baselines (e.g., how often a user accesses certain systems)
2. 2. Histograms (e.g., how many files individual members of a peer group typically access)
3. 3. Automatic and/or expiring whitelists and blacklists (e.g., normal application traffic)

Integration

LogRhythm's patented machine data processing technology creates a consistent Machine Data Intelligence Fabric (MDIF) that is leveraged for both machine-based and search-based analytics. The MDIF provides a consistent view of processed log and machine data across all LogRhythm customers. This consistent view enables the delivery of prepackaged security analytics modules, which include Machine Analytics Rules, Searches, Reports, and Dashboards.

Presentation

LogRhythm UBA event details can be reviewed through event drill-down. This capability empowers analysts with user behavior details via a dashboard with visualizations, along with machine access to all relevant machine data (metadata, raw logs). This information is quickly and easily accessible to the analyst as it is stored in LogRhythm's machine data persistent store, which is based on Elasticsearch. Tools include:

- Dashboard widget library: LogRhythm provides a library of Dashboard widgets, each with customization options, to present analysts with highly concerning activities. All widgets allow for immediate drill-down to underlying data for immediate forensic analysis. The Analyze view has its own set of widgets to best provide a representation of search results, or alarm or dashboard drill-down.
- Centralized search: LogRhythm provides robust forensic analytics and centralized search capabilities that enable security and operational personnel to rapidly investigate and respond to threats. Our interface allows for quick creation of simple or even complex unstructured and/or contextualized structured data searches. This eliminates the need to understand complex scripting or SQL languages. Several pre-built investigations are available via LogRhythm's support portal, and included in specific KB modules.
- Pivot & drill-down: Analysts can pivot from a search using one or more fields, allowing them to quickly extend a search with highly targeted criteria. For example, an analyst can pivot on an origin user identified in a search to view all activities by this user. Using drill-down, an analyst can rapidly pull up other details (including the raw log message), or drill into an AI Engine event to help determine the exact pattern of logs causing a rule to fire.

Platform (In-house)

Most LogRhythm customers begin with an all-in-one (XM) appliance configuration and are later combined with additional components to increase capacity, performance, and fault tolerance. As the deployment grows, customers can expand the deployment with other components. The platform performs data collection and generation, processing, indexing, machine analytics, search, incident response orchestration, and automated response.

Platform (Application as a Service)

Select LogRhythm MSSP partners offer LogRhythm via an application-as-a-service model.

Platform (Cloud)

LogRhythm supports Amazon AWS and uses the platform for cloud-based POCs. LogRhythm has certified partners who provide software installation services across other cloud-based services. In addition, a number of LogRhythm Managed Service Partners utilize LogRhythm in public/private cloud environments for selling hosted SIEM Services, including Optiv, Secure24, QinetiQ, RKON, CGSI, and others..

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Communication applications such as email and Skype
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems
- Proxy servers
- Mobile Device Management systems
- Virtual machine management
- Cloud services
- Network infrastructure
- Social media
- Documentation
- Inputs of other data
- Machine Fingerprint
- Geographic location
- Inputs of other data

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank certain countries higher risk than other
- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules only as an "after filter" (Machine Learning Engine does the heavy lifting)

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

Learning periods are configured on a per-rule basis and thus do not require an all-or-nothing approach. Learning periods can be adjusted or restarted on the fly.

Baseline Process

Baselines are configured per rule and can be set to analyze one or more data points and grouped by customizable fields. For example a user can baseline port and host activity for the entire network, or per host. Time criteria are set per rule and can be modified by the user.

REPORTS

Administrators, Security Executives, C-Suite, Board of Directors

LogRhythm provides access to several sets of reports through Modules available through its Knowledge Base. Additionally, analysts can use customizable dashboards to provide real-time visibility.

Users can clone and modify over 1,200 reports for security, compliance, risk management, and other purposes. These reports provide visibility into the threats targeting your organization, your team's response efforts, the health of your security intelligence platform, and more. Diverse information visualization options provide appropriate detail for various audiences, all the way up to the executive suite. All reports can be assigned specific permission levels to ensure proper visibility.

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Users with threats
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

- LogRhythm's UBA functionality is fully integrated into our Security Intelligence Platform. Analysts can view this data alongside other data in out-of-the-box general dashboards and UBA dashboards, and they can also customize and clone dashboards as they see fit.
- LogRhythm Client Console Dashboards and LogRhythm Web Console Dashboards available out of the box. Can be configured to forward to other systems for additional integration.

ADDITIONAL INFORMATION

In addition to LogRhythm's native User Behavior Analytics (UBA) capabilities, the platform can collect events and other telemetry from third-party UBA solutions via standard data collection methodologies, such as syslog. LogRhythm's real-time analysis functionality can contextualize third-party UBA events, corroborate user-related compromises or incidents, prioritize these events relative to others based on risk, and expedite the triage, investigation and remediation of user-related security events.

At the time of our response to this RFI (i.e., April, 2016), LogRhythm supports integration with CyberArk and Varonis. The development of these integrations was completed per requests from customers that had invested in these platforms prior to deploying LogRhythm.

QUESTIONS

Mark Settle
Product Marketing Team Manager
720.403.9025
Mark.Settle@LogRhythm.com

COMPANY

NuData Security
#550 – 999 Canada Place
Vancouver
BC V6C 3T4
Canada

WEBSITE

www.nudatasecurity.com

CONTACT

Lisa Baergen
Marketing Director
604-674-7684
778-240-2444
lisa.baergen@nudatasecurity.com

INVESTMENT INFORMATION

Founded in 2008

Privately Held

OFFICE LOCATIONS

Headquarters
550-999 Canada Place
Vancouver
BC
V6C 3T4
Canada
1 (604) 800-3711

MANAGEMENT TEAM

Michel Giasson CEO	Christopher Bailey CTO	Jules Campeau CRO	Curtis Sikorsky CFO	Ryan Wilk VP, Customer Success	Robert Capps VP Business Development	Lisa Baergen Director Marketing

EMPLOYEES

Total Number: 58	**Total Technical:** 35	**Total Support:** 8				

CUSTOMER BACKGROUND

Total Customers: 68	**Total UBA Customers:** 63					
Markets: Banking Consumer	Energy (Oil & Gas) Finance Healthcare	Insurance Media Retail	Technology Telecom			

CUSTOMER UBA INFORMATION

Average End-user Revenue:	End-user Employees:	Regulations:	
$600K - $3M	~	Banking Consumer Healthcare Insurance	Retail Technology

UBA PRODUCT INFORMATION

NuDetect
NuCaptcha

Launched on:
2008
2013

PRODUCT OVERVIEW

• NuDetect	NuDetect is a behavior analytics platform that monitors user interactions in and across website, mobile, and application environments to identify legitimate known users and detect automated, anomalous, or fraudulent behavior. We specialize in good user verification to truly understand how banks and Financial Institution users behave and if it is truly the good user behind the device. NuDetect builds upon a solid architecture of four distinct layers to improve confidence in identifying good users. Even in less than ideal circumstances. This behavior is monitored in real-time, enabling banks and FIs to do three key things: 1. Verify legitimate known users 2. Identify higher risk activities 3. Leverage extensive behavioral network	General Availability Date: 2008
• NuCaptcha	NuCaptcha is an interdiction module contained as part of the NuDetect Behavioral Analytics platform. The Captcha module is used on specific pages that may be subject to automation, such as Login and Account Creation. NuDetect uses multiple systems to detect non-human behavior and anomalous activity to determine if a Captcha should be displayed, and if so, what security features should be present in the Captcha. This determination is made in part by the NuDetect behavioral analytics engine, and in part by custom customer based rule configuration. As such, the Captcha acts as a low-friction test for users associated with suspect behavior, enabling an additional realtime metric to verify the scoring provided by NuDetect and reduce the impact of false positives.	General Availability Date: 2013

Application Development Process

PRODUCT DESCRIPTION

NuDetect

The vendor pioneered the use of User Behavior Analytics for Cybersecurity. Over the last eight years, the solution suite has demonstrated an impressive ability to analyze large volumes of data at-scale, and in real-time, to establish a baseline of normal users and system behavior. This sophisticated artificial intelligence platform utilizes network, device and human interaction intelligence to detect cyber threats in real time, and flag suspicious behavioral anomalies for further remediation. Due to this compelling set of capabilities, vendor clients are uniquely positioned to identify higher risk activities before the transaction occurs, allowing for opportunistic application of friction on suspect transactions, while allowing a much better, often frictionless experience for legitimate, known users.

PRODUCT ACQUISITION

NuDetect	Built in-house
NuCaptcha	Built in-house

UBA PRODUCT ROADMAP & DEVELOPMENT

- Q1: Accelerated deployment options and intelligence dashboard workflows. User interdiction options. Full entity linking search functionality.
- Q2: NuData Platform partnerships: Data enrichment: KYC etc. ; and advanced technology enhancements (e.g. Advanced GeoLocation).
- Q3: Extended PII data collection: expanded 3rd party partnerships; digital fingerprints; Self-service policy creation and Cross-client network effect 2.0
- Q4: Self-service modeling portal

As NuDetect provides risk scoring and behavioral analystics at the application level it is possible to to leverage this across all 10 areas of the OWASP. This is important not just in the case of web applications but mobile as well when determining the validity of the user including the characteristics of the device. Being able to differentiate between automation and a "real person" is important in understanding when "ATO" (account take over), malware or any type of malicious activity is occuring whether it is scripted using automation or a human using stolen credentials.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

NuDetect provides real time scoring that can be consumed in multiple forms. The real time risk assessment can be consumed by the client application to provide real time interdiction and mitigation. The NuDetect dashboard displays the score results in near real-time so that high-risk events can be evaluated and actioned. We can work with the customer to determine risk appetite to adapt outcomes of scores.

NuDetect passively collects non-PII user behaviour and intelligence at key interaction points between the user and an online property. This intelligence is then scored as varying degrees of bad or good behaviour against multiple contexts as follows:

- Against the users own history on the website or on the cloud
- Against the aggregate population of the website at the time and historically
- Against the aggregate population of the cloud at the time and historically

This intelligence score is immediate and in real time enabling the customer to call up a score at any time during the user's web session for example, at login. NuData's breadth of knowledge is significant due to the volume of profiling that we do. This is due to that fact that we are deployed in many of the largest online companies in the world.

Integration

The NuDetect Platform has the ability to ingest any and all data that the customer has available. Each additional data point passed to the tool can be incorporated into the model to strengthen its ability to understand behavior and identify risk.

Platform (In-house)

Possible to house the platform with the customer existing infrastructure leveraging the existing business continuity, disaster recovery and operational services they already have in place.

Platform (Cloud)

Many of our customer leverage our cloud based solution which leverages Amazon Web Services to provide a securely hosted option that also includes operational redundancy in the form of business and disaster recovery services.

DATA SOURCES

- SIEM and other log aggregator and analysis systems
- Cloud services (public/private)
- Machine fingerprint
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank certain countries higher risk than other
- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

There are three data sources for the collected data:
- Endpoint device characteristics;
- Endpoint device interactions;
- Application level data

For the first 30 days after production deployment NuDetect will run in a silent ghost mode, monitoring user behavior in the client's environment, but not yet passing back behavioral intelligence. During this phase the NuData Data Sciences team will review and analyze the client's user-behavioral data in preparation for the production model launch. It should be noted that NuDetect can identify anomalies such as various types of active malware and automation from day one. It takes approximately 30 days to build out a view of the unique behavioral interactions within the client's environment. At the end of the 30 day analysis NuData will launch the production scoring model and activate the real-time scoring functionality via the Score Call API.

Baseline Process

A NuDetect implementation is typically divided into five phases to ensure a successful engagement. The following section provides an outline of the five proposed phases spanning from launching the NuDetect in the FinishLine's web and mobile environment through full production deployment and collaborate model tuning.

- Phase 1: Technical Discovery & Project Kickoff

- Phase 2: Implementation & QA Verification
  NuDetect will be implemented into the identieid placements within the customersenvironment.

- Phase 3: Model Optimization
  NuData will monitor behavioral interactions in the FinishLine's web and mobile environment to identify valid customers, anomalous user behavior, and abuse. At the completion of the silent monitoring period NuData will active the live scoring API passing back user behavioral intelligence to the customer

- Phase 4: NuDetect Live Scoring Deployment
  At completion of the silent monitoring period NuData will launch production scoring and provide a traffic analysis report outlining the behavior observed during the silent monitoring period.

- Phase 5: Collaborative Model Tuning
  NuData works closely with its clients to ensure the behavioral intelligence being provided is directly solving the desired client use-cases. To maximize value NuData enters into a collaborative model-tuning phase, postproduction launch, working side by side with its clients to ensure maximize value is being realized.

- Phase Implementation Expanded: NuDetect User Behavioral Profiling & Project Deliverables

REPORTS

The NuDetect dashboard provides a simple and intuitive interface to view and sort aggregate data. The NuDetect dashboard has a flexible querying system that allows customers to specify the date range for reports. By default, the dashboard displays a monthly view and easily allows the user to dive into weekly, daily or hourly views. All data from the NuDetect Dashboard can be exported in a variety of formats for use with other reporting tools. The NuDetect dashboard has a flexible querying system that allows customers to specify the date range for reports. By default, the dashboard displays a monthly view and easily allows the user to dive into weekly, daily or hourly views

Administrators

The NuDetect dashboard has a flexible querying system that allows customers to specify the date range for reports. By default, the dashboard displays a monthly view and easily allows the user to dive into weekly, daily or hourly views

The NuDetect dashboard continuously updated and is accessible via a customer portal by anyone to whom RBDF's wishes to grant access. It serves two primary purposes:

- Provide management reports on key metrics and reports for the previous 30 days, 24 hours, etc.:
- Score bands with breakdowns for all website traffic
- Regions – source locations for all website traffic
- Signals – types of attacks against the website, e.g.,
  - Login Account Cycling
  - Login Velocity
  - Input Scripted Curl
  - Login Failure Velocity
  - Account Harvesting
  - Provide fraud teams with a tool for detailed analysis of specific events and for forensic investigation purposes, for instance:
- Anchor Data Points
- Session Event Timeline
- Endpoint Details
- Account Details
- Passive Biometric Details

Security Executive

The NuDetect dashboard has a flexible querying system that allows customers to specify the date range for reports. By default, the dashboard displays a monthly view and easily allows the user to dive into weekly, daily or hourly views

The NuDetect dashboard is continuously updated and is accessible via a customer portal by anyone to whom the enterprise wishes to grant access. It serves two primary purposes:

- Provide management reports on key metrics and reports for the previous 30 days, 24 hours, etc.:
- Score bands with breakdowns for all website traffic
- Regions – source locations for all website traffic
- Signals – types of attacks against the website, e.g.,
  - Login Account Cycling
  - Login Velocity
  - Input Scripted Curl
  - Login Failure Velocity
  - Account Harvesting
  - Provide fraud teams with a tool for detailed analysis of specific events and for forensic investigation purposes, for instance:
- Anchor Data Points
- Session Event Timeline
- Endpoint Details
- Account Details
- Passive Biometric Details

C-Suite & Board of Directors

The NuDetect dashboard provides a simple and intuitive interface to view and sort aggregate data. The NuDetect dashboard has a flexible querying system that allows customers to specify the date range for reports. By default, the dashboard displays a monthly view and easily allows the user to dive into weekly, daily or hourly views. All data from the NuDetect Dashboard can be exported in a variety of formats for use with other reporting tools.

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Users with threats
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

- Due to its open architecture many customers have integrated NuDetect with their existing enterprise SIEM and fraud detection systems to include behavioural biometrics to compliment their existing device/endpoint security with this additional level of intelligence. We have many customers who have integrated NuDetect into existing environments where this is already present using Rest API calls. NuDetect provides real time scoring that can be consumed in multiple forms. The real time risk assessment can be consumed by the client application to provide real time interdiction and mitigation. The NuDetect dashboard displays the score results in near real-time so that high-risk events can be evaluated and actioned. Clients can control the levels of alerts and what those alerts can trigger. NuDetect empowers clients to decide what to do and when to do it.

ADDITIONAL INFORMATION

Top 3 Technical Differentiators

Real time Monitoring/Integration – The solution monitors online activity in real-time within a single management interface that negates the need for more expensive security controls such as data mining and knowledge-based authentication. A unique score and set of risk signals is attributed to every user interaction and a customized risk model provides actionable intelligence that is business specific and can be consumed within a customer's existing fraud and case management systems.

User Behavioral Profiles – The solution is equipped with pattern matching and entity linking so that even partial matches in a user's behavioral profile can be identified across the solution's service so that a threat, bad-actor, or even a nefarious pattern of behavior on one website will be recognized and then flagged when observed on other vendor-protected websites.

Scalable Behavioural Network – Since 2013 the number of behavioural events that have been scored each year has more than doubled from 7 Billion in 2013, 18 Billon in 2014, to 38 billion in 2015 and is estimated to be 80 billion for 2016, providing highly accurate, actionable behavioural intelligence for the customer."

QUESTIONS

Lisa Baergen
Marketing Director
604-674-7684
778-240-2444
lisa.baergen@nudata.com

COMPANY

Prelert, Inc.
20 Speen Street #200
Framingham, MA, 01701
United States

WEBSITE

www.prelert.com

CONTACT

Trey Lang
Marketing Associate
508-319-5319
tlang@prelert.com

INVESTMENT INFORMATION

Founded in 2009

Privately Held

OFFICE LOCATIONS

Headquarters 20 Speen St. #200 Framingham, MA, 01701 US 508-319-5300	**Headquarters** 20 Speen St. #200 Framingham, MA, 01701 US 508-319-5300	**Support** 20 Speen St. #200 Framingham, MA, 01701 US 508-319-5300		

MANAGEMENT TEAM

Mark Jaffe CEO	Stephen Dodson CTO	John O'Donnell CFO	Sophie Chang VP of Engineering	Mike Paquette VP of Products	John Sullivan VP of Sales	

EMPLOYEES

Total Number: 30	**Total Technical:** 15	**Total Support:** 4				

CUSTOMER BACKGROUND

Total Customers: > 100						
Markets: Banking Consumer	Education Engineering Energy (Oil & Gas)	Finance Government (Federal)	Government (Local) Healthcare	Insurance Media Manufacturing	Retail Technology Telecom	Transportation

CUSTOMER UBA INFORMATION

Average End-user Revenue: N/A	**End-user Employees:** N/A			

UBA PRODUCT INFORMATION

Behavioral Analytics for the Elastic Stack
Anomaly Detective App for Splunk
Anomaly Detective API Engine

Launched on:
2016
2013
2014

PRODUCT OVERVIEW

• Behavioral Analytics for the Elastic Stack	The Prelert Behavioral Analytics for the Elastic Stack product analyzes any kind of time-series based data residing in Elasticsearch to identify user and entity based anomalies and correlate influential entities enabling your data to provide behavioral insights into advanced cyberthreats activities and IT operational problems (i.e. performance, KPI, etc.) that previously would take insurmountable manual human effort.	General Availability Date: 2016
• Anomaly Detective App for Splunk	The Anomaly Detective App for Splunk product analyzes any kind of time series based data residing in Splunk to identify user and entity based anomalies and correlate influential entities enabling your data to provide behavioral insights into advanced cyberthreats activities and IT operational problems (i.e. performance, KPI, etc.) that previously would take insurmountable manual human effort.	General Availability Date: 2013
• Anomaly Detective API Engine	The Anomaly Detective API Engine is a technology platform that provides a REST interface for OEM and Customers to embed within an existing product for the purpose of allowing Prelert analytics to identify user and entity based anomalies and correlate influential entities enabling time series based data to provide behavioral insights into advanced cyberthreats activities and IT operational problems (i.e. performance, KPI, etc.). The Engine is a key component of both the Splunk and Elasticsearch products.	General Availability Date: 2014

Application Development Process

PRODUCT DESCRIPTION

Prelert analyzes an organization's log data, finds anomalies, links them together and lets the data tell the story behind advanced security threats, IT performance problems, and business disruptions. Leveraging machine learning anomaly detection and other behavioral analytics capabilities, the solution automates the analysis of massive data sets, eliminating manual effort and human error. Hundreds of progressive IT organizations rely on Prelert to detect advanced threat activity, reduce false positive alerts and enable faster root cause analysis. Prelert lets your data tell the story with the following key capabilities:

- Unsupervised Machine Learning
  Prelert's machine learning algorithms automate the analysis of massive sets of machine data, building and maintaining accurate statistical models of your data without the need for training. Even better, organizations don't need a team of data scientists to use Prelert effectively.
- More Accurate Anomaly Detection and Alerting
  Prelert's sophisticated machine learning anomaly detection provides you with accurate information (read: fewer false positives) so you can quickly detect, investigate and respond to anomalous activity. Automated analytics eliminates manual effort writing rules and human error parsing alerts.
- Organization-Specific Insights
  One of the top challenges for IT security is baselining "normal" behavior in order to detect abnormal behavior. Our threat Insights and causal insights let your data tell the story. Arranged in time order and grouped by common entities, automated insights tell you what you need to know now and what requires further investigation.
- Faster Data Analysis
  At the scale and complexity of modern IT environments, an overwhelming volume of data and alerts tells you nothing. Our platform is designed to analyze massive, high-cardinality data sets in moments, visually showing you what you need to know and making it easy to investigate and explore, uncovering what is worthy of your attention.

PRODUCT ACQUISITION

Behavioral Analytics for the Elastic Stack	Built in-house
Anomaly Detective App for Splunk	Built in-house
Anomaly Detective API Engine	Built in-house

UBA PRODUCT ROADMAP & DEVELOPMENT

- Roadmap discussions can be provided under NDA.

We follow an agile development process that enables rapid response to customer requests and market changes. While we are completely capable to deliver continuous development, we generally market product updates for major releases and minor releases. Major releases for each product occur at minimum of once per year and minor releases occur several times per year. We offer support and maintenance of two major releases back however new algorithmic development and process/workflow refinements are primarily packaged for new releases.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

Prelert provides proprietary unsupervised machine learning capabilities, including automatic periodicity detection and quick adaptation to changing time series data. These algorithms and capabilities developed internally by Prelert, determine anomalies and correlate statistical influencers and have been proven on real-world data over the past 5 years.

Integration

Any timeseries data (e.g. syslog, application logs, firewall logs, DNS logs, etc.)

Presentation

Anomaly Results Summary, Anomaly Explorer, Entity View, Insight Storyline

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems (Raytheon Websense, Zscaler for example)
- Proxy servers
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)
- Proxy servers
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

There is no hard requirement for the learning period of live or historical data. Prelert's analytics "know" how well its baseline models are converging, and won't generate anomaly alerts until a converged model is achieved. For automatic periodicity detection, 2-3 times the period is recommended.

Baseline Process

The baselining process is proprietary but is largely influenced by the analytical function applied on the data.

REPORT

The end result of incorporating Prelert into the security analytics process is to be able to highlight relevant elementary attack behaviors that are consistent with an attack. In so doing, Prelert can be incorporated into a customers reporting process readily.

Administrators

All Views

Security Executive

Insight Storyline

C-Suite

Insight Storyline

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Users with threats
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

- On Splunk, Prelert's Anomaly Detective for Splunk App will incorporate results into Splunk Enterprise Security under relevant Notables.

ADDITIONAL INFORMATION

Prelert has established a Security Use Case portal that quickly and accurately enables customers to deploy Prelert machine learning Use Cases in their environments that would enable detection of elementary attack behaviors consistent with attack progression stages such as infiltration, reconnaissance, tunneling and exfiltration.

The Security Use Case web site is: http://info.prelert.com/behavioral-analytics-for-security-use-cases

QUESTIONS

Trey Lang
Marketing Associate
508-319-5319
tlang@prelert.com

COMPANY

Securonix
14665 Midway Road - Suite #100
Addison, TX, 75001
USA

WEBSITE

http://www.securonix.com

CONTACT

Sharon Vardi
CMO
+1 (310) 641-1000
svardi@securonix.com

INVESTMENT INFORMATION

Founded in 2008

Self Funded

OFFICE LOCATIONS

Headquarters 14665 Midway Road - Suite #100 Addison, TX, 75001 USA	**R&D** 14665 Midway Road - Suite #100 Addison, TX, 75001 USA	**Support** 5777 W. Century Blvd - Suite #360 Los Angeles, CA, 90045 USA	**R&D** 6th Floor Corniche Towers. Kalyani Nagar, Pune Maharashtra, 411006 India	**R&D** 210A Twin Dolphin Dr Redwood City, CA, 94065 USA	

MANAGEMENT TEAM

Sachin Nayyar CEO	Tanuj Gulati CTO	Chris Bell COO	Sharon Vardi CMO	Darren Gaeta VP Partnership & Alliances	Ken Mermoud VP Products

EMPLOYEES

Total Number: 250	**Total Technical:** 170	**Total Support:** 22			

CUSTOMER BACKGROUND

Total Customers: 100	**Total UBA Customers:** 90	**Total UBA POCs:** 180			
Markets: Automotive Banking	Consumer Education Engineering	Energy (Oil & Gas) Finance Government (Federal)	Government (Local) Healthcare Insurance	Manufacturing Media Retail	Technology Telecom

CUSTOMER UBA INFORMATION

Average End-user Revenue:	End-user Employees:	Regulations:
>$5B	10,000	FISMA for Finance HIPAA for Healthcare PCI for Retail

UBA PRODUCT OVERVIEW

Securonix Enterprise
SNYPR

Launched on:
February 1, 2011
March 30, 2016

PRODUCT OVERVIEW

• Securonix Enterprise	Securonix Enterprise is a behavior-based threat prediction, detection and prevention engine that mines, enriches, analyzes, prioritizes, and transforms machine data into actionable intelligence. Using patent pending signature-less anomaly detection techniques that track user, account, system, device, application and transaction behavior, Securonix Enterprise automatically and accurately detects the most advanced and sophisticated insider threats and cyber attacks. • Detect insider threats and cyber attacks that go undetected by traditional security technologies • Focus on protecting the data that is the most valuable to the organization • Dramatically reduce the number of false positives, alerts and incidents that warrant investigations The Securonix platform makes available a list of pre-packaged analytics apps that include: • Insider Threat • Data Security Analytics • Identity and Access Analytics • Trade Surveillance Analytics • Fraud Analytics • Privileged Account Analytics • Cyber Security Analytics • Application Security Analytics • Cloud Security Analytics • Healthcare Analytics	General Availability Date: February 1, 2001
• SNYPR	SNYPR is a Big Data Security Analytics platform running natively on a Hadoop backend that collects, stores and analyzes log data to detect advanced threats. It delivers the proven power of Securonix analytics with the speed, scale, and affordable, long-term storage of Hadoop in a single, out-of-the box solution. SNYPR is capable of ingesting petabytes of data generated by large organizations, processes it and analyzes it in real-time leveraging a combination of user and entity behavior analytics (UEBA), unsupervised machine learning, and dynamic threat modeling to deliver true predictive threat detection and unprecedented historical investigation capabilities. **What does SNYPR mean for enterprise security?** • A holistic enterprise security analytics platform that marries best-of-breed Big Data and analytics technologies • Detect the most sophisticated advanced persistent threats and "low and slow" attacks over extended periods of time • All historical, security-relevant data is available for investigation	General Availability Date: March 30, 2016

Application Development Process

PRODUCT DESCRIPTION

Securonix Enterprise

Securonix Enterprise provides a security analytics platform with purpose-built analytics for cyber threat, insider threat, fraud detection and prevention. The security analytics platform aggregates and correlates identity, security events, activity, access, threat intelligence and asset data. The solution applies machine learning based analytical techniques to detect anomalies and identify threat patterns to risk rank insider and cyber threats.

Securonix Enterprise has a robust policy engine with different types of policies and analytical techniques including rule-based policies, identity correlation policies, peer-based policies, behavior-based policies, multi-tiered policies, and threat chains. For all behavior-based policies, the platform automatically creates a behavior baseline (what's 'normal') for every user/system/IP address (minimum of 10 data points), and then looks at deviations (frequency spikes, amount spikes, rarity, robotic behavior, etc). The behavior profiles are automatically created and updated every time there is new data ingested into the platform.

Securonix Enterprise comes with a comprehensive set of out of box policies and threat chains (800+) for advanced threat detection. In addition to the out of box policies, the Securonix Enterprise policy engine allows customers to create their own set of policies (rule-based, peer-based, behavior-based, etc) in the Securonix Enterprise web-based GUI without any code changes in the platform.

Securonix continuously updates the set of out of box policies and threat chains and has created a threat exchange community to collect, productize, and share the latest content to Securonix customers and partners directly through the Securonix Entreprise GUI. Customers and partners can also contribute and share their own set of policies and threat chains.

SNYPR

The SNYPR Big Data Security Analytics Platform is the industry's first unified security analytics platform that harnesses the power of distributed processing provided by Hadoop. The SNYPR platform provides real time event monitoring and also has machine learning based behavior analytics and advanced entity analytics needed to detect unknown threats and rank entities. The SNYPR platform has the following capabilities

- Runs completely on Hadoop and harnesses the distributed processing capabilities to analyze big data (10 - 500 Terabytes / day)
- Provides super enrichement of events in real time at the time of ingestion
- Uses several machine learning based analytical techniques including unsupervised behavioral analytics, peer analytics and bayesian classifiers to detect anomalies
- Associates threats to entities (users, devices) and risk ranks threats for expedient response
- Provides indexed searching of raw events (Over 8 Billion Events searched within 0.5 seconds)
- Enables advanced visualizations of events and threats including capabilities to generate dashboards with drill-downs

PRODUCT ACQUISITION

Securonix Enterprise	Built in-house
SNYPR	Built in-house

UBA PRODUCT ROADMAP & DEVELOPMENT

Securonix uses Jira for release management and tracking for each of the Securonix product lines (Securonix Enterprise, SNYPR, Content) with dedicated projects and owners. The tool holds a backlog of all features and enhancement requests. For every product release, an initial set of requirements is prioritized in the tool (Epic, New Feature, Enhancement) that will define the overall scope of a release, giving visibility to the entire team (developement, QA, documentation, product management). Any changes in the scope of a release, dependencies, blockers will be identified and discussed during the daily scrum meeting, assuring that everybody in the team is aware of any change in the product release scope or timing.

Securonix has a defined security assurance program that follows a set of industry-leading standards, technologies, and practices aimed at fostering security innovations, reducing the incidence of security weaknesses in Securonix products, and reducing the impact of security weaknesses in released products on customers. The program includes the following components:

- Personnel security standards
- Secure development standards
- Security validation
- Secure delivery process
- Secure operation initiative
- Flaw remediation

As part of the personnel security standards component, Securonix defines specific job roles (security architect, security test manager, security code reviewer) and assigns the roles based on product components and security sensitivity levels. As part of the on-the-job training, Securonix R&D follows the OWASP guided training program to be aware of all the recent attack trends, security vulnerabilities, best coding practices, etc.

Securonix provides regular hotfixes and patches to customers (hotfixes are available to a single customer, patches are combinations of multiple fixes available to all customers). Once a patch has been made available to customers, the changes made for the patches will be integrated into the following major/minor release or service pack. The Securonix Quality Assurance team builds new test cases for every patch delivered to customers to avoid any regression in future releases.

Patches are released to customers primarily to address any important product bug or security vulnerability detected in one of the components packaged as part of the Securonix products. Securonix also publishes a list of all known vulnerabilities that the Securonix products interact with (e.g. operating system, database, etc) and the list is available to all customers and partners on the support portal.

Securonix uses its customer support portal (support.securonix.com) to interact with all Securonix customers and partners. Securonix customers and partners have the ability to create new tickets for enhancement requests on the portal. The Securonix product management team continuously reviews enhancement requests and adds them into future product release versions, as needed. Product enhancements will be scheduled for future major and minor product versions, sometimes in service packs depending on the criticality and the demand of the request coming from the customer.

In additional to the customer support portal, Securonix organizes customer advisory boards and user groups throughout the year to receive feedback and enhancement requests from all customers. After discussion and review of every request, the Securonix product management team will follow the same process as described above.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

- Securonix has a collection of purpose-built analytics (frequency-based, volume-based, peer-based, robotic, sequencing, DGA, etc.) depending on the type of data sources and use cases, with different type of machine learning based algorithms
- Securonix provides hundreds of packaged threat models that translate individual threat indicators and anomalies into real threats
- Securonix supports both near real-time inline analytics as well as batch analytics
- With SNYPR, all analytical techniques are fully distributed in a Hadoop environment
- The Securonix platform is extensible and easily allows customers to plug-in their own algorithms

Ingestion

- 200+ out-of-box connectors for data source described in 5b.
- Supported data format: file, syslog, database, XML, JSON, CEF, LEEF, API
- Custom connector (parser) creation in Securonix GUI without code changes
- Data ingestion in real-time or batch

Correlation

- Correlate multiple data sets to entities at ingestion time
- Multiple third party intelligence data source consolidation

Export

- Out-of-box setting to export data such as policy violations to file, syslog, or third-party applications

Web-Services APIs

- Large set of APIs for third-party applications to retrieve data from Securonix, such as user risk score, threat indicators, metadata
- API-based cloud application connectors for AWS, Box, Google Apps, O365, etc.

Securonix uses several Web 2.0 technologies on the user inetrface to provide a rich user experience. To begin with, the Securonix platform is built on an MVC architecture and uses the boostrap framework to provide a responsive UI. This means that the Securonix user interface self adapts to the device it is run on - mobile, tablets, laptops/desktops. The Securonix application has in-built charting and reporting frameworks that are extremely agile and allow rapid and flexible development of new components. With tabbed views and timeline views, the Securonix application enables rapid investigations and response. The Securonix Investigation workbench is an engineering marvel that allows visual link analytics between millions of objects.

Securonix Enterprise Platform

- Relational database deployment architecture (Master-Child architecture)
- Child Nodes: data ingestion and first layer analytics
- Master Nodes: end-user interaction (GUI), storage of entity meta data, historical entity behavior profiles and risk scoring trends, second layer analytics.
- Platform scales horizontally by adding more child nodes for data ingestion

SNYPR Platform

- Big Data (Hadoop) deployment architecture
- Ingestion Nodes: ingestion of data
- Analytical Nodes: data enrichment and analytics
- Master Nodes: end-user interaction (GUI) and management
- Platform scales at a big data scale by adding more ingestion and analytical nodes

SaaS Platform (Securonix Enterprise)

- Master nodes for the SaaS infrastructure management (Securonix or Partner)
- Child nodes + possibly 1 master node at client's prem
- All client raw data is processed and stored on different child nodes
- All client meta data (policy violations, users, etc) is controlled, enforced, and audited with access control
- Option to host the child nodes for data ingestion within the SaaS infrastructure

SaaS Platform (SNYPR)

- Master nodes for the SaaS infrastructure management (Securonix or Partner)
- All data from client is stored in the SaaS infrastructure and completely separate from other clients in the Hadoop infrastructure (multi-tenant)

The Securonix application is a multi-tenant platform that allows user and data level segregation across multiple tenants. The Securonix platform is available as a hosted service on public and private clouds. The cloud architecture requires the customers to forward their events to a dedicated syslog receiver that parses and normalizes the events prior to the applicaton of analytical techniques. The data is stored in sharded data repositories and the users can access a dedicated user interface. The analytical layer shares computing resources amongst multiple tenants.

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Communication applications such as email and Skype
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems (Raytheon Websense, Zscaler for example)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank certain countries higher risk than other
- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs
- Incorporates business-specific rules

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

To create a baseline, the application requires a minimum of 10 data points to create a valid cluster and hence a baseline. Depending on the type of data source and time dimension used to create the baseline, the period of time to learn the 'normal' behavior will vary. For example, if we are looking at the total number of failed login attempts by user by day, then we will need at least 10 days (or 2 weeks if there is no user activity over the weekend) to create a baseline. If we are looking at the total number of bytes in/out for a firewall on a weekly basis, then we would need to wait 2.5 months to get 10 data points to derive the normal behavior for that firewall.

Baseline Process

Securonix learns about what is normal for every entity (user, account, resource, hostname, IP address) as new data is being ingested in the application. Once the initial baseline has been established, the baseline will be updated on a continuous basis as new activity/log data is ingested by the application. Once configured in the system, this process is completely automated and the end user does not need to make any modifications manually. The log data ingestion in the Securonix application is configured in such a way that every data source will have different flavors of baselines (e.g. volume-based, frequency-based) and time ranges (e.g. hourly, daily, day of the week, weekly) based on the use cases.

Securonix can set up multiple types of baselines for the same data source (called behavior profiles). For example with ATM transaction logs, there could be a baseline of the number of transactions per day by ATM machine, and at the same time the total dollar amount for all the transactions by ATM machine. The administrator/configurator of the Securonix application can also create new behavior profiles through the application GUI for any use cases that are not part of the out-of-the-box content."

REPORTS

Administrators

Securonix provides a set of out-of-box reports & dashboards for operational monitoring of the application. The list includes (but not limited to):

- Application summary: license, application, job summary by data source
- Data import trends: user, access, activity import trends by data source
- Peer groups and organizations trends: metrics around number of peer groups, organizations
- Policy violation trends: metrics around number of policy violation by data source over time
- Reports can be scheduled on a daily/weekly/monthly basis to provide a summary and aggregation of historical data, such as the history of all the policy violations and threat indicators for every employee, the risk score trend for an organization or business unit, and operational metrics.

Security Executive

Securonix provides a set of out-of-box reports & dashboards for the security management team with metrics around:

- High-risk entity summary: Total number of risky users, accounts, resources, IP addresses
- Top N threats: Top N threats across the organization (threat modeling)
- Risk trending over time: Overall risk and metrics around number of threats and anomalies detected in the organization
- Organization risk over time: Risk ranking and grade per organization/department and ability to drill down to specific areas of concern

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Total users
- Users with threats
- Total devices
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Solution integrates into existing dashboards

Primary examples:
- Securonix App for Splunk (https://splunkbase.splunk.com/app/3007/)
- Securonix App for IBM Qradar (https://exchange.xforce.ibmcloud.com/hub/extension/Securonix:Securonix%20-%20Security%20Analytics%20Delivered)
- Bi-directional and GUI Integration with HPE ArcSight ESM (https://www.protect724.hpe.com/docs/DOC-10371)

ADDITIONAL INFORMATION

Privacy and Data Encryption:

- Securonix provides very comprehensive controls to ensure employee privacy. This is done via a combination of granular access control and data level encryption capabilities.
- With granular access control, the vendor ensures that only the apporpriate personnel can view the information for other employees. This includes the ability to control what users can be viewed by which security personnel and what data for these users can be viewed.
- The data is encrypted by the solution at rest as well as on the user interface. Additionally, the solution provides the ability to configure the need for approvals prior to the data becoming unencrypted for view.
- The solution has the ability to restrict the unencryption capability only to the violators so adhoc data snooping is avoided.

Industry Standards and Certification:

- Common Criteria EAL 2+ (Scope: Penetration Testing, Security Architecture, Development, Product Delivery & Configuration management) - February 13th 2015: https://www.cse-cst.gc.ca/en/publication/securonix-security-intelligence-platform-40
- FIPS 140-2 Cryptography Conformance - February 28th 2014: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0018.pdf
- Section 508: VPAT created by Accessibility Partners LLC and able to be provided as required based on request
- Vulnerability Assessment:
- EWA Infrastructure Vulnerability Assessment (Scope: Application + Appliance): November 2014
- Fortify Code Vulnerability Scan: March 2015
- E&Y Vulnerability Assessment: February 2015, March 2015
- Customer Scans (4): October 2013, August 2014, June 2015, November 2015""
- Fortify Dynamic Scan: June 2016

QUESTIONS

Sharon Vardi
CMO
+1 (310) 641-1000
svardi@securonix.com

COMPANY

Sqrrl
125 Cambridge Park Dr.
Cambridge, MA, 02140
USA

WEBSITE

www.sqrrl.com

CONTACT

Paul Lynch
VP of Sales
(781) 864-1607
paul@sqrrl.com

INVESTMENT INFORMATION

Founded in 2012

Privately Held

OFFICE LOCATIONS

Headquarters
20 Speen St. #200
Framingham, MA, 01701
US
508-319-5300

MANAGEMENT TEAM

Mark Terenzoni CEO	Adam Fuch CTO	Ely Kahn VP of Business Development	Ari Daskalakis VP of Field Operations	Paul Lynch VP of Sales	Brien Wheeler VP of Engineering	Luis Maldonado VP Products

EMPLOYEES

Total Number: 53	**Total Technical:** N/A	**Total Support:** N/A				

CUSTOMER BACKGROUND

Total Customers: > 30	**Total UBA Customers:** > 30	**Total UBA POCs:** > 45				
Markets: Banking Education	Energy (Oil and Gas) Finance Government (Federal)	Healthcare Manufacturing Retail	Technology Telecom			

CUSTOMER UBA INFORMATION

Average End-user Revenue:	End-user Employees:	Regulations:
N/A	N/A	FIPS 140-2, FISMA for Government (Federal) HIPAA for Healthcare

UBA PRODUCT INFORMATION

Sqrrl Enterprise

Launched on:
2013

PRODUCT OVERVIEW

• Sqrrl Enterprise	Sqrrl's industry-leading Threat Hunting Platform unites User and Entity Behavior Analytics (UEBA), link analysis, and multi-petabyte scalability capabilities into an integrated solution. Unlike many UBA products that focus on users and user activity, Sqrrl is designed to uncover the links amongst various entities - a concept we refer to as the Behavior Graph. With this unique approach, Sqrrl provides analysts with a platform that detects adversarial tactics, techniques and procedures (TTPs), identifies risk to enterprise assets, provides full contextual awareness and enables intuitive, visual exploration of the relationships amongst enterprise assets.	General Availability Date: 2013

Application Development Process

PRODUCT DESCRIPTION

Sqrrl Enterprise

Sqrrl leverages numerous UEBA capabilities in order to facilitate and automate incident investigation and threat hunting processes. A core capability of Sqrrl Enterprise is an array of adversarial behavior detectors that identify threat actor TTPs including lateral movement, malicious beaconing, data staging, data exfiltration, DNS Tunneling, and the use of Domain Generation Algorithms (DGA). Sqrrl leverages a combination of analytics including both unsupervised and supervised Machine Learning, behavioral base-lining, peer group analysis, signal processing, time series analysis, computational statistics, graph theory and advanced correlation for determining risk and locating patterns and indicators of compromise. Sqrrl provides security analysts with workflow-oriented interfaces such as risk dashboards, entity and behavior profiles, ad hoc outlier detection tools, investigation journal, dynamic reports and dashboards, query and search tools and programmatic APIs. Sqrrl's back end infrastructure provides an industry leading approach to securing data at the field or "cell" level as opposed to common row-level security approaches. Sqrrl is proven to perform at petabyte scale deployments, where all capabilities and data are available interactively and in real-time.

PRODUCT ACQUISITION

Sqrrl Enterprise	Built in-house

UBA PRODUCT ROADMAP & DEVELOPMENT

Sqrr'ls 2017 roadmap includes key integration solutions with major SIEM, Identity, Endpoint Detection & Response (EDR), networking and Threat Intelligence vendors, as an addition to those that have already been developed in the past year. In continuing to work with these solutions, Sqrrl will be applying existing and new behavioral capabilities to address key analyst pains in managing alerts and in integrating multiple security data domains to identify adversarial activity.

Sqrrl operates a SCRUM-based agile development process. This process enables great flexibility in accommodating changes to our development plan of record. This flexibility is applied judiciously, as change requests are weighed against customer and market needs as well as strategic product development goals. Similar to enhancement requests, change requests proceed through triage, filtering and prioritization processes to ensure any changes are applied in a controlled and coordinated fashion. Approved changes are planned, built and tested prior to full rollout. Change control is managed at all points of the process to enable back out and/or mitigation paths.

Sqrrl maintains diligent approaches to application security. Besides its data-centric security-based architecture developed at the NSA, Sqrrl has applied controls to the entire system stack, including data confidentiality and integrity protection, inter and intra- process communication, user and privilege management, web application security, system administration and 3rd party software. Sqrrl's specific approach to OWASP Top 10 risks is confidential.

Sqrrl's internal patch management process is divided into two areas: servers and every day use machines.

All our servers, whether bare metal in our colo facility or deployed as virtual machines or in containers, use a gold image Linux build. We use a configuration management suite that allows for automated delivery of operating system level updates. These updates both come primarily from the OS provider but we are also able to deploy emergency fixes for critical severity issues. As part of our patch management process, we include regularly scheduled updates at least once quarterly to ensure compliance with the latest security best practices.

Our developer machines and other laptops follow a similar patch management process. All machines use approved OS images and endpoint protection software. We also enforce that any machines connecting to our colo via VPN adhere to security policies - those machines with out of date operating system or application patch levels are denied access to the VPN.

Sqrrl maintains an Enhancement Request process for all internally or externally-sourced product improvement submissions. In front-end stage of the process, incoming requests are de-duped, grouped and triaged. Requests are prioritized in accordance with various factors (market impact, product roadmap, customer needs etc.). Request are converted into user stories, groomed and estimated then incorporated into development team SCRUM backlogs. Status is communicated to requested along the process, including upon delivery of the feature.

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

Sqrrl's analytics leverage both unsupervised and supervised Machine Learning, behavioural base-lining over a given time span, peer group analysis, signal processing, time series analysis, Bayesian statistics, and advanced correlation for determining risk, locating patterns, and indicators of compromise.

Integration

Sqrrl can integrate with a wide variety of data. Core data integration is with proxy, netflow, and windows event logs as well as SIEM data feeds. Enrichment sources include geoIP, threat intelligence, asset management information, user attributes, email and more. Common data formats and transports include CEF, CSV, delimited files, JSON and Syslog. Finally, Sqrrl provides an extensible data integration layer that enables support for most structured and semi-structured data sources.

Presentation

Sqrrl provides numerous data visualization interfaces that support detective, investigative and forensic workflows. These include risk dashboards, behavioral profile pages, entity context views, activity timelines, raw data tables, interactive graph visualizations, dynamic reports and investigation journaling with DVR-like replays.

Platform (In-house)

Sqrrl is deployed on commodity hardware running Linux operating systems. The Sqrrl technology stack can be installed on existing commercial and open source Hadoop infrastructure or provided with a pre-configured Hadoop distribution.

Platform (Application as a Service)

Sqrrl can be deployed in managed environments (e.g. MSSPs) from commercial service providers.

Platform (Cloud)

While Sqrrl is not currently offered as a cloud service, Sqrrl is deployed to cloud environments such as Amazon Web Services for testing and proof of concept deployments as well as for select production deployments.

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Communication applications such as email and Skype
- Identity Access Management systems
- SIEM and other log aggregator and analysis systems
- Data Loss Prevention systems
- Intrusion Prevention and/or detection systems
- Firewalls
- Web filter systems (Raytheon Websense, Zscaler for example)
- Proxy servers
- Mobile Device Management systems (Good, for example)
- Virtual machine management (hypervisor for example)
- Cloud services (public/private)
- Network infrastructure (Netflow, router logs, etc.)
- Social media (Facebook, Twitter, LinkedIn, Instagram, etc.)
- Geographic location
- Documentation (performance reviews, expense reports, etc.)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Rank risk scores based on applications within a specific environment
- Ability to adjust predetermined risk scores
- Ability to adjust predetermined risk scores incorporated into the modelling process
- RESTful API allowing for the incorporation of custom data feeds/logs

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

Some analytics (e.g. beaconing and DNS tunneling) do not require a learning period and begin producing results immediately. For others, a 7 day learning period is recommended. Sqrrl will continue to refine the baseline over the previous 6 months of data to ensure good adjustment for seasonal behaviors.

Baseline Process

In order to detect anomalies, Sqrrl's analytics establish baselines of normal observed activity in a number of ways depending on the type and application of the analytic. Baselining procedures observe raw data features and learn distributions across multiple dimensions such as time, frequency, rarity, graph structure, volume etc. System analytic results are fed back into baselining processes to enable continuous algorithmic tuning. Baselining procedures are automatic and only require minimal user input in identifying false positives and whitelisting tolerable activities.

REPORTS

Administrators

Sqrrl provides numerous operational facilities and for monitoring and managing the Sqrrl platform. These facilities include managing and monitoring data loading, analyst queries, analytic job execution, and platform infrastructure monitoring and control.

Security Executive

Sqrrl has a rich and extensible reporting framework for security management and executive users. Sqrrl has built in reporting for key metrics of enterprise assets such as users, hosts, IP addresses and URIs. These reports include summaries of risk, aggregate behavior, and relations to other entities. Sqrrl also provides metric based reports across multiple data domains including network activity, web content, user accesses, and alerts. Users may easily extend this set with custom reports on metrics, analytics and aggregations that are germane to their organization. All reports are dynamic, provide "drill down" to exploration and assessment workflows and can be exported for inclusion in more traditional reporting systems.

C-Suite

Sqrrl's reporting framework can be customized by users to provide reports relevant to the C-suite. Sqrrl supports common report visualizations typically required in C-Suite level summaries (tables, bar charts, pie charts, etc). These reports can be presented as interactive dashboards or exported / printed for offline analysis. C-Suite teams may leverage security executive reports which include metrics such as aggregated risk, and also consume reports that identify risk to key crown jewel assets and their impact to other system assets and users.

Board of Directors

Much like for the C-suite, Sqrrl's reporting framework can be customized by users to provide reports relevant to the board of directors. Sqrrl supports common report visualizations typically required in C-Suite level summaries (tables, bar charts, pie charts, etc.). These reports can be presented as interactive dashboards or exported / printed for offline analysis. In addition to leveraging C-Suite metrics, BOD personnel may also consume custom reports on risk to key business assets.

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Total users
- Users with threats
- Total devices
- Device anomalies
- Endpoint threats
- Network threats
- Total sessions
- Anomalous sessions
- Session lengths per user
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

SIEM Integration with QRadar and ArcSight; data visualization integration with Tableau

QUESTIONS

Luis Maldonado
VP Products
(617) 902-0784
luis@sqrrl.com

COMPANY

Varonis
1250 Broadway, 29th floor
New York, New York, 10001
USA

WEBSITE

www.varonis.com

CONTACT

David Gibson
VP of Strategy and Market Development
877-292-8767
dgibson@varonis.com

INVESTMENT INFORMATION

Founded in 2005

Publicly Held

OFFICE LOCATIONS

Headquarters 1250 Broadway, 29th floor New York, NY, 10001 USA 877-292-8767	**Office** 2250 Perimeter Park Drive Suite 150 Morrisville, NC 27560 USA 919-701-3300	**Office** 529 SW 3rd Avenue Suite 300 Portland, OR USA 503-305-9600	**Varonis France SAS** 13-15 rue Jean Jaures (1er Etage) Puteaux 92800 France 33-184-88-56-00	**Varonis UK Ltd.** Golden Cross House 8 Duncannon Street London WC2N 4JF UK 44-203-695-3900	**Varonis Deutschland GmbH** Terminalstrasse Mitte 18 Munchen 85356 Germany 49-89-38037990	**Office** 7 Arie Shenkar St. Gav-Yam Bldg 2 Golden Cross House 8 Duncannon Street Herzliya 46733 Israel 972-9-971-3300

MANAGEMENT TEAM

Yaki Faitelson Chief Executive Officer, President, Co-Founder and Chairman of the Board	Ohad Korkus Chief Technology Officer and Co-Founder	Gili Iohan Chief Financial Officer	Jim O'Boyle Senior Vice President of Worldwide Sales	David Bass Senior Vice President Of Engineering	Gilad Raz CIO and Vice President of Technical Services	David Gibson Vice President of Strategy and Market Development
Ken Spinner Vice President of Global Field Engineering	Seth J. Gerson Vice President and General Counsel	Dana Shahar VP of Human Resources	Eric Mann Chief Operating Officer	Yzhar Kaysar Chief Architect	Tami Bronner Vice President of Product Management	

EMPLOYEES

Total Number: **>1,000**	**Total Technical:** N/A	**Total Support:** N/A				

CUSTOMER BACKGROUND

Total Customers: >5,000						

Application Development Process

CUSTOMER BACKGROUND (CONT.)

Markets: Automotive Banking	Consumer Education Engineering	Energy (Oil and Gas) Finance	Government (Federal) Government (Local)	Healthcare Insurance Manufacturing	Media Retail Technology	Telecom Transportation

CUSTOMER UBA INFORMATION

Average End-user Revenue: N/A	**End-user Employees:** N/A	**Regulations:** FIPS 140-2, FISMA for Government (Federal) HIPAA for Healthcare				

UBA PRODUCT INFORMATION

DatAlert Suite

Launched on:
2016

PRODUCT OVERVIEW

• **DatAlert Threat Model**	Varonis UBA threat models uncover security issues quickly, and give context around metadata and what's actually happening on your file and email servers, SharePoint, and Active Directory.
• **Varonis behavior research laboratory**	A dedicated team of security experts, analysts, and data scientists who stay up-to-date on the latest security issues, APTs, and insider threats, and how to defend against them. The laboratory continually introduces new threat models to DatAlert – including the latest threat model introduced in 6.2.51 that actively detects patterns and user actions that resemble ransomware.

DatAlert Suite

DatAlert Suite protects enterprise file and email servers from cyberattacks, insider threats, ransomware, and potential security breaches. DatAlert monitors enterprise assets for suspicious activity and unusual behavior, detecting critical events and compromised assets. It automates threat detection with predictive threat models built on advanced analytics, user behavior and machine learning. Unlike many UBA and SIEM solutions, Varonis is not dependent on external data sources. This, and years of experience collecting, storing and analyzing file system activity, differentiate Varonis. Varonis Metadata Framework platform is a unique differentiator, the ability to capture high-fidelity auditing data directly from disparate monitored systems, and combine that information into Varonis DatAlert for a holistic analytical view across an organization's unstructured data.

UBA PRODUCT ROADMAP & DEVELOPMENT

As a public company, Varonis cannot divulge roadmap information without a confidentiality agreement. However, we have a proven track record of innovation over the past 10 years, expanding functionality and platform coverage across six product families. We have provided no indication that we plan to cease or slow innovation.

Configuration Management process – there is a dedicated CM team responsible for CM tools (TFS), build machines, configuration and change management and SW build process and repository.

All the source code is stored in TFS , every code change is registered via tfs and all the details about the code change (the delta that was changed, timestamp, name of the developer, etc.) are stores and can be reviewed.

The code change usually are linked to relevant tfs item that stores information regarding change reason and new behavior and – bug or feature request .
Most of the code changes are developed on a dedicated branch, which is later synced and merged with the main branch of the release : the merge process is done using TFS abilities through full tracking of code changes that were made during the merge.
Configuration Management process – there is a dedicated CM team responsible for CM tools (TFS), build machines, configuration and change management and SW build process and repository.

All the source code is stored in TFS , every code change is registered via tfs and all the details about the code change (the delta that was changed, timestamp, name of the developer, etc.) are stores and can be reviewed.

The code change usually are linked to relevant tfs item that stores information regarding change reason and new behavior and – bug or feature request .
Most of the code changes are developed on a dedicated branch, which is later synced and merged with the main branch of the release : the merge process is done using TFS abilities through full tracking of code changes that were made during the merge.

We currently don't have a formal vulnerabilities testing process. The Veracode certification was done on one of the last versions as a specific project.

In cases when customers report major issue that require code change or urgent feature request and patch delivery the following process is executed:

1. The bug/feature request is registered in bug /feature management system (tfs)
2. Test case for bug/feature verification are registered in test management system (mtm based on tfs)
3. The branch for patch development is created from the version that is currently installed on customer's site.
4. The relevant dev and qa teams provide effort estimation and commitment dates
5. The dev teams develop the change and delivers to QA
6. Patch information is registered on a patch management site along with the patch executables and installation instructions
7. QA teams test the patch
8. A dedicated team performs version checklist on the system with customer version the new patch installed
9. The patch is delivered to the customer by CS group
10. The code change is integrated to the next main release in order to make sure that the customer will have the fix after the upgrade

Feature Change Management process – after the requirements of the feature were specified sometimes a change request might be required by Product Manager/QA/Dev engineers. In this case a requirement change is evaluated by feature team and their managers, business justification, cost and risks of the requested change are accessed. In case the change request is approved by the engineering and product managers – the requirements change is documented in spec doc, work plan of dev and QA is being updated and the change is developed and tested as a part of further feature development. The change is registered in feature documentation like Spec, Dev Design and QA Plan (MTM).

UBA PRODUCT SYSTEM ATTRIBUTES

Analytics

Varonis captures high-fidelity access data across multiple platforms without the use of native auditing. Varonis feeds the audit trail, along with user information, data access rights, and file content information into a machine learning and behavior analysis to engine. Using multiple metadata streams allows Varonis to derive a more complete baseline of the environment, understand how users behave discretely, and also relative to similar individuals. The multi-dimensional analytics enables Varonis to detect when behaviors change across disparate platforms to identify insider threats – including when authorized users become compromised, or abuse their access to sensitive data.

Integration

Varonis integrates with industry-leading SIEM and threat analytics solutions. Varonis supplies results from our behavioral analytics platform via Syslog, SNMP, and email. DatAdvantage includes a reporting API, giving customers access to our rich data and analytics without complicated customized database work.

Presentation

Varonis DatAdvantage has single pane of glass interface to visualize the activity for all users, across all the platforms. The Varonis threat models automatically learn normal behavior, and analyze all access activity so it only alerts on suspicious behavior. The intuitive interface helps security staff can focus on the right information without sorting the noise of constant alerts. If more detailed information is necessary, DatAdvantage provides drill down capabilities through a single interface to answer the most difficult questions – such as who accessed what data, when, how did they god access to the data, and was the data sensitive.

Platform (In-house)

The Varonis metadata framework is a distributed, highly-scalable architecture designed from the ground up to accommodate big data processing from heterogeneous platform types – including Windows, NAS, Exchange, Active Directory, and Unix/Linux – and present the data back through a single interface. Varonis runs on standard Windows servers, either physical or virtual, giving organizations maximum deployment flexibility – there is no need for specialized hardware or network taps to capture data. The Varonis architecture scales to monitor the data wherever it lives, and can easily adapt as organizations grow and change.

DATA SOURCES

- Operating systems, such as workstations, servers and appliances
- Data Loss Prevention systems
- Cloud services (public/private)
- Inputs of other data (CSV formatted files, etc.)

FINE GRAINED CONSTRAINTS (CUSTOMIZABLE)

- Installation of an agent
- Incorporates business-specific rules

UBA SET UP, ADMINISTRATION & REPORTING

Learning Period

DatAlert Analytics provides a number of different threat models for behavior analysis. Each threat model (for instance, abnormal access to sensitive data) has minimal and optimal learning periods. For most models, the minimum learning period is 10-20 days, while the optimal learning period is 180 days.

Baseline Process

The baselines process is different for different threat models, since the data used for behavioral analysis is different depending on the threat model. Broadly, file and email activity on monitored platforms is collected and analyzed over time in conjuction with Active Directory changes, file system permissions and other platform metadata, and content sensitivity on supported platforms.

REPORTS

Administrators

Because Varonis collects a complete map of all users, groups, direct and effective permissions, content sensitivity, and access activity, there are a large number of out of the box reports available to administrators. Report categories include, user activity, statistics, group membership, file system permissions, behavior analytics, behavioral alerts, inactive resources, management and ownership, and tredning.

Security Executive

KPI reports include general file system stattistics, statistics on sensitive data, statstics on open and overesposed access, file system trends, storage use and unuse, and action items per business unit. Security exetives can also find valued in detailed statstics about data use, group access, and behavioral alerting broken down by user, group, business unit, or platform.

C-Suite

KPI reports include general file system stattistics, statistics on sensitive data, statstics on open and overesposed access, file system trends, storage use and unuse, and action items per business unit.

Board of Directors

KPI reports include general file system stattistics, statistics on sensitive data, statstics on open and overesposed access, file system trends, storage use and unuse, and action items per business unit.

FEATURES IN THE DAY-TO-DAY MANAGEMENT DASHBOARD

- Total threats
- Threat types
- Total anomalies
- Total users
- Users with threats
- Total sessions
- Anomalous sessions
- Threat level (Level of urgency)

DASHBOARD INTEGRATION

Varonis integrates with industry-leading SIEM and threat analytics solutions. Varonis supplies results from our behavioral analytics platform via Syslog, SNMP, and email. DatAdvantage includes a reporting API, giving customers access to our rich data and analytics without complicated customized database work.

ADDITIONAL INFORMATION

Varonis DatAlert Analytics does not compete with more traditional UBA products, since the behavioral analysis it does is based on proprietary metadata--user and group information, file system heirarchies and permissions, content sensitivity, and data access activity--collected by other Varonis technology. This makes DatAlert Analytics unique in that the data sources it uses for behavioral analaysis, specifically file and email access activity, are not available to other UBA products. DatAlert threat models were developed using actual production data from a variety of varonis customers to minimize false positives and identify threats that otherwise would remain invisibile to traditional UBA technologies.

QUESTIONS

David Gibson
VP of Strategy and Market Development
877-292-8767
dgibson@varonis.com

SECURONIX
Security Analytics. Delivered.

Securonix Security Analytics Platform:

Behavior Anomaly Detection and Peer Group Analysis Through User Behavior Analysis

The Securonix Security Analytics Platform is a purpose-built advanced security analytics technology that mines, enriches, analyzes, scores and visualizes data into actionable intelligence on the highest risk threats from within and outside their environment. Using signature-less anomaly detection techniques that monitor users, account, and system behavior, Securonix is able to automatically and accurately detect the most advanced data security, insider threats and fraud attacks.

- Signature-less behavior based analytics for detecting insider and targeted cyber attacks
- User centric monitoring across hosts, network and applications
- Privileged account monitoring and misuse detection
- Over 90% reduction in security events warranting investigations

INSIDER THREAT MANAGEMENT

Securonix automatically and accurately identifies inside threat actors by delivering behavior anomaly detection capabilities in an out-of-the-box solution that does not require manual sifting through data or rules. Using purpose-built data mining, correlation, enrichment, and analytics, Securonix detects not only users with high risk identity profiles, but also high risk activity, access, and events in your organization associated with insider threats.

IDENTITY & ACCESS MANAGEMENT

Securonix uses highly sophisticated algorithms that automatically detect high privileged accounts for proactive monitoring while identifying and risk ranking rogue access assignments for cleanup or certification. Securonix integrates with every major IAM and identity access governance product while connecting natively to major business applications and systems. It delivers automatic identity and access intelligence allowing improved access management compliance through user and resource centric views of access risk, automated access cleanup and risk-based, streamlined access request processes.

APPLICATION SECURITY

Securonix protects enterprise applications by monitoring critical applications and systems at the transaction, data set, and sensitive user record level to identify anomalies that indicate a threat. Suspicious application-based behaviors are correlated with continuously generated risk profiles of users, access, and activities associated with sensitive data and transactions.

NETWORK SECURITY

Securonix couples the latest advances in machine learning and artificial intelligence with advanced anomaly detection techniques that rapidly detect known and unknown threats – without relying on signatures, policies or rules. By correlating anomalous behaviors with context rich intelligence, Securonix reduces false positives by up to 90 percent, enabling security teams to concentrate on real, high-risk threats to the organization.

PRIVILEGED ACCOUNT MANAGEMENT

Securonix removes the cloak of privilege that allows most high privileged accounts to operate with a high-risk measure of anonymity by detecting anomalous behaviors associated with insider and external attacks. Abnormal account activity is flagged automatically and accurately, and risk-ranked with context-rich intelligence that correlates user, network, system and physical data with HR tips and clues.

THREAT INTELLIGENCE

Securonix provides innovative behavior-based techniques in conjunction with peer group analysis measures to detect any variation in normal patterns for access and usage of internal data sources. By comparing not only historical usage, but usage of colleagues and team members also, the Securonix solution is able to remove the noise associated with incremental changes in user behavior for automatic, accurate detection of attacks.

securitycurrent

Security Current improves the way security, privacy and risk executives share information and collaborate to protect their organizations and their data. Its CISO-authored and peer driven proprietary content and events provide insight, actionable advice and analysis giving executives the latest information to make knowledgeable decisions.