Market Guide for User and Entity Behavior Analytics

Published: 23 April 2018 **ID:** G00349450

Analyst(s): Gorka Sadowski, Avivah Litan, Toby Bussa, Tricia Phillips

Security and risk management leaders considering UEBA will find that the market has fragmented, with a few pure-play vendors and a wide set of traditional security products that embed core UEBA technologies and features to benefit from advanced analytics capabilities.

Key Findings

- UEBA technologies are maturing, becoming more robust and valuable, and seeing broader adoption with forward-leaning organizations, especially as pure-play UEBA vendors morph into adjacent markets by building additional capabilities to try to replace legacy tools.
- UEBA capabilities are being adopted across a range of security technologies, such as SIEM, IDPS, DCAP, CASB, IAM and EDR.
- UEBA primarily relies on advanced analytics methods and approaches, such as machine learning, but vendor hype and use of terms such as "artificial intelligence" make it difficult for buyers to effectively evaluate vendor technologies and capabilities.
- Buyers find that UEBA deployment can be more time-consuming and labor-intensive than what vendors promise, even for core threat detection use cases. Also, adding custom or edge use cases can be an arduous process, requiring expertise such as data science and data analytics.

Recommendations

Security and risk management leaders involved with security operations and vulnerability management should:

- Initiate any UEBA project by clearly defining the use cases that need to be addressed, and by describing the desired output from the tool for each of these to ensure that it's delivering value against key pain points. Verify first whether your current tools like SIEM can solve these problems.

- Demand a clear answer from UEBA vendors and/or verify with testing that the solution can support the data sources for priority use cases, whether use cases can be implemented "as-is" with prepackaged analytics and the expected effort level for custom use cases.
- Include a proof of concept (POC) phase in your selection process, and structure the POC to maximize vendor knowledge transfer. Expect the POC process to take at least 30 days to give a solution's machine learning engine time to learn your organization's data and construct baselines using live or historical data, and for your organization to validate the UEBA solution and its outputs.

Strategic Planning Assumptions

By 2021, the user and entity behavior analytics (UEBA) market will cease to exist as a stand-alone market.

By 2022, core UEBA techniques and technologies will be embedded in 80% of threat detection and incident prioritization solutions.

Market Definition

UEBA solutions use analytics to build the standard profiles and behaviors of users and entities (hosts, applications, network traffic and data repositories) across time and peer group horizons. Activity that is anomalous to these standard baselines is presented as suspicious, and packaged analytics applied on these anomalies can help discover threats and potential incidents. The most common use cases sought by enterprises are detecting malicious insiders and external attackers infiltrating their organizations (compromised insiders).

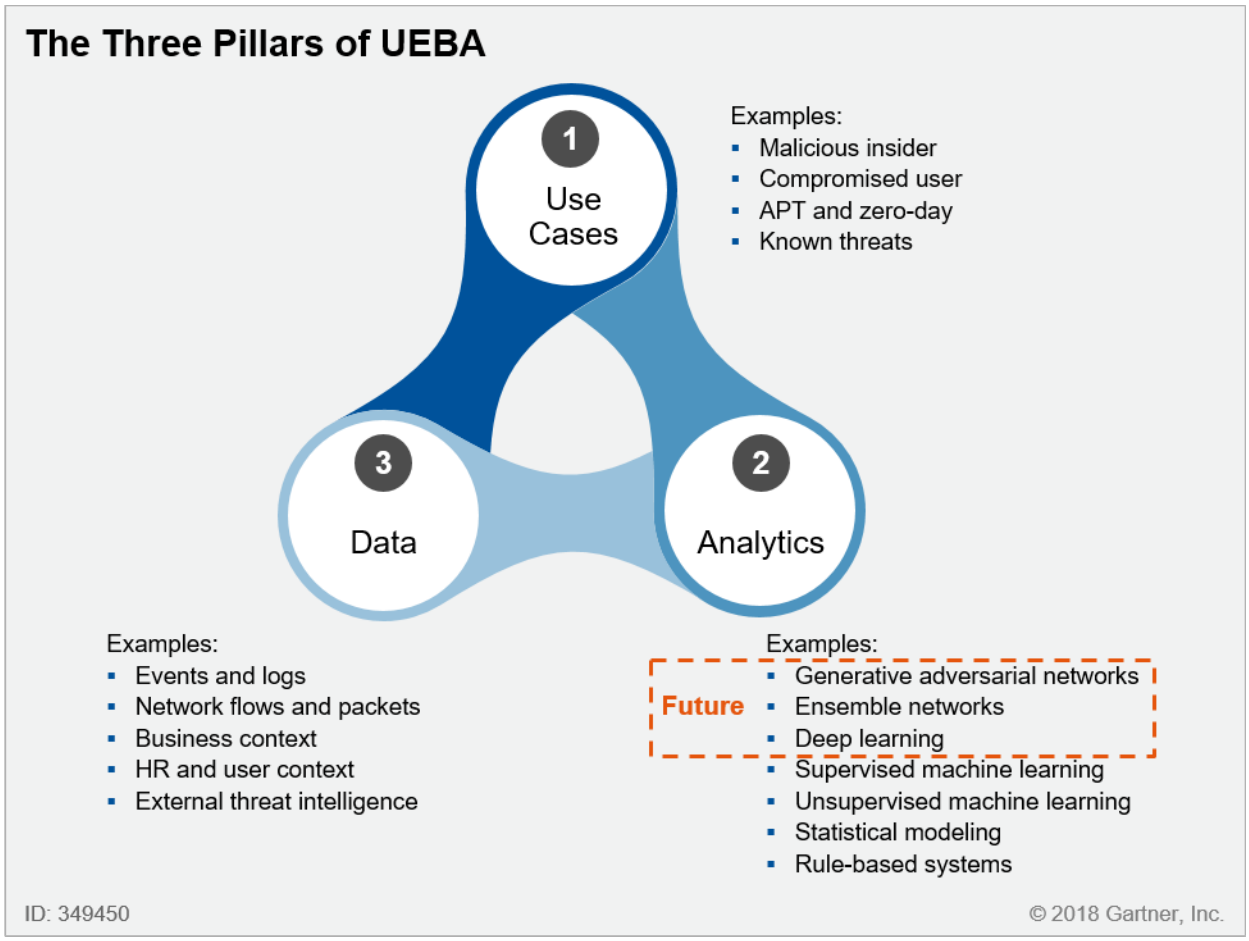
Market Description

Gartner views the UEBA market as including solutions that:

1. Solve multiple, distinct use cases such as privileged user monitoring or data exfiltration (for example, not just generically "monitoring for anomalous user activities")
2. Emphasize the use of advanced analytics (supported and enriched by basic analytics approaches as required)
3. Offer multiple ways for collecting data, including natively from data sources as well as from central log management (CLM), data lakes and/or security information and event management (SIEM), without forcing buyers to deploy dedicated instrumentation agents
4. Can be purchased and implemented as stand-alone solutions rather than embedded in other solutions

Gartner defines the pure-play UEBA solutions along these three dimensions of use cases, analytics and data sources as described in Figure 1.

Figure 1. The Three Pillars of UEBA



Source: Gartner (April 2018)

UEBA tools in scope for this Market Guide also need to be natively developed or fully acquired, and available as an independent solution that can be purchased separately from other feature sets available by the vendor.

Specifically, for each of these criteria, the tool should be available as a stand-alone offering and should encompass:

1. Use cases:
   - Provide insights on behaviors from both users and other entities.
   - Perform monitoring, detection and alerting for anomalous behaviors for both users and entities.
   - Do not focus only on a single use case (for example, tools that only focus on employee monitoring or trusted users or fraud would be out of scope for this Market Guide).

2. Analytics:
    - Detect anomalies using a variety of analytics approaches — primarily statistical models and machine learning (ML), but combined with rules and signatures, delivered as prepackaged analytics used to create and compare user and entity activity against their profiles and their peers' profiles.
    - Offer advanced analytics capabilities that are not uniquely based on rules, such as using clustering algorithms to offer dynamic peer grouping.
    - Correlate user and other entity activity and behaviors (for example, through Bayesian networks techniques), and aggregate individual risky behaviors, to highlight anomalous activity.
3. Data sources:
    - Ingest event data from user and entity activities, either natively from the data sources directly or through an existing repository (central log management [CLM], SIEM or data lake). The solutions should not rely primarily on network data as the main data source, and should not rely primarily on their own agents to collect telemetry data.
    - Enrich data about users and entities with contextual information, and support ingestion of both structured, real-time event data as well as structured and unstructured reference data from IT directories (for example, Active Directory) or other sources of machine-readable information (for example, HR databases).
4. Availability:
    - Offer the above in a solution that can be purchased separately, and not only embedded in feature sets of other point solutions. For example, this Market Guide does not include cloud access security brokers (CASBs) that have UEBA features embedded.
    - Offer the above in a solution that is developed natively by the vendor, not offering the feature set via resale or an OEM arrangement, or other partnership agreements.

There is also a growing number of vendors that have added user context and user and entity behavior analysis features to their existing solutions focused on a specific capability. These capabilities include employee monitoring, data-centric audit and protection (DCAP), identity and access management (IAM), and others (see the UEBA as a Feature Is Becoming More Widespread section).

UEBA is both a solution and a feature; in this update, we're focusing on the stand-alone solution vendors.

The UEBA Market Guide does not include vendors that:

- Do not profile both users as well as other entities to detect anomalies in user or entity behavior
- Only support security use cases through data mining, user-driven data exploration and visualization

- Only support one family of use cases, such as only fraud detection or only employee monitoring
- Use an OEM of another UEBA engine in their solution.

Market Direction

UEBA just passed the Peak of Inflated Expectations in Gartner's latest Hype Cycle (see "Hype Cycle for Threat-Facing Technologies, 2017") and is heading down the Trough of Disillusionment.

End-user spending on UEBA stand-alone solutions will grow at a compound annual growth rate (CAGR) of 48%, from $50 million in 2015 to $352 million in 2020 (see "Invest Implications: 'Forecast Snapshot: User and Entity Behavior Analytics, Worldwide, 2017'").

However, the number of pure-play UEBA solution vendors has continued to decrease in 2017 and 2018, largely due to acquisition activity. Gartner expects continued consolidation in that space, while the number of vendors touting UEBA techniques used in their products serving adjacent segments like endpoint protection platform/endpoint detection and response (EPP/EDR) or CASB has seen substantial increase.

The lists in the UEBA as a Feature Is Becoming More Widespread section provide numerous examples of such tools and vendors for several categories of solutions. Some UEBA vendors are now focusing their route to market strategy on embedding their core UEBA technology in other vendors' more traditional security solutions (for example, Fortcale's Presidio embeddable UEBA engine prior to the RSA acquisition).

Gartner sees this trend sustaining throughout 2022, when UEBA will be superseded by more encompassing security analytics technologies.

Market Analysis

Changes Since the Last Market Guide for UEBA Update

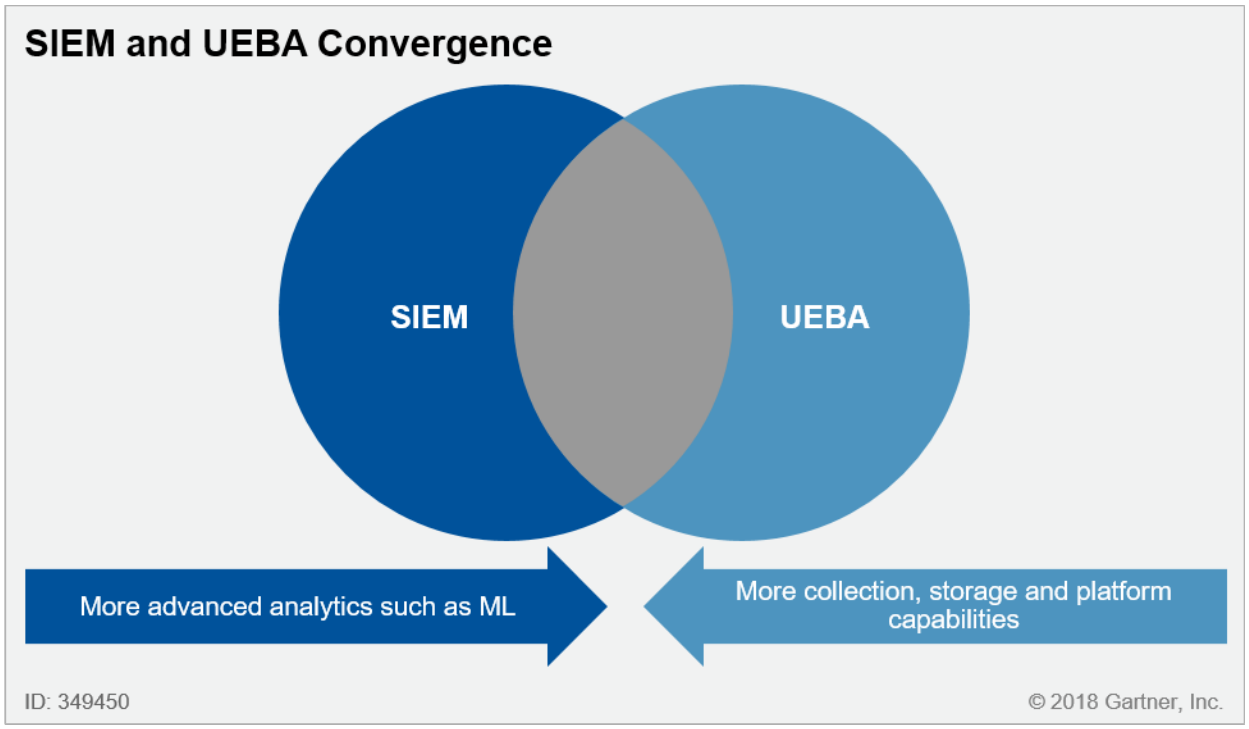
Exabeam and Securonix are now tracked in Gartner's SIEM Magic Quadrant as they expanded their UEBA focus and developed SIEM capabilities. Niara was acquired by Aruba, a Hewlett Packard Enterprise (HPE) company. Balabit was acquired by One Identity. E8 Security was acquired by VMware. Fortscale was acquired by RSA.

SIEM and UEBA Are Converging

During 2017, we have seen all the SIEM vendors in the Leaders or Visionaries quadrant in Gartner's Magic Quadrant for SIEM offer UEBA or user behavior analytics (UBA, a UEBA focused on user behavior) capabilities. Their approach is to either (1) develop this functionality organically; (2) integrate other UEBA solutions through an OEM arrangement or (3) partner with a UEBA vendor on a tightly coupled offering. Conversely, we saw UEBA solution vendors expanding their original

scope and offering SIEM-like functionality and feature set. Vendors such as Exabeam and Securonix have now developed SIEM capabilities robust enough to be tracked in Gartner's SIEM Magic Quadrant, while IBM and LogRhythm are developing UEBA features (see Figure 2).

Figure 2. SIEM and UEBA Convergence



Source: Gartner (April 2018)

This puts pressure on remaining UEBA vendors to adopt the SIEM and UEBA convergence approach, or become more general-purpose security analytics companies by offering advanced analytics beyond UEBA and/or expanding on use cases they can solve out of the box with prepackaged models.

Main Use Cases Are Solidifying

UEBA solutions can support a variety of use cases; however, there is consensus among Gartner clients that the primary use case involves detection of different categories of threats, achieved through visibility into and analysis of often-correlated user and other entity behavior. Gartner continues to see use cases such as monitoring for unauthorized data access and movement, suspect privileged user activities, malicious or unauthorized employee activities, unusual cloud resource access and usage, and generally getting better detections out of existing security technology investments (for example, CASB, IAM). Finally, there are also a set of typically non-cybersecurity-centric use cases for which UEBA solutions can sometimes be used. However, these often require either non-IT and nonsecurity data sources, or require very specific analytics models derived from deep domain expertise, such as fraud or employee monitoring.

Specifically, the five primary domains and use cases that the stand-alone UEBA vendors and their users most frequently align with are:

- **Malicious insider:** UEBA vendors targeting this use case monitor staff and trusted external parties only for unusual, bad or abusive behavior. Vendors in this domain do not monitor or analyze service accounts or other nonhuman entities to inform their analysis. Largely because of this, they are not oriented toward detecting advanced threats where hackers take over existing user accounts, but are oriented instead toward finding insiders engaged in malicious activities.

  Essentially, malicious insider threats emanate from trusted users with malicious intent who seek to impose damage on their employers. Since malicious intent is difficult to assess, best-in-class vendors in this category analyze contextual behavioral information not readily available in log files. Vendors in this domain also optimally ingest and analyze unstructured information, such as email content, performance reviews and social media information, for employee behavior context.

- **Compromised insider and advanced threats:** The use case here is to rapidly detect and analyze bad activities once an attacker has infiltrated an organization and is moving laterally around the internal IT infrastructure. Advanced persistent threats (APTs) and unknown or not-yet-understood threats such as zero-day attacks are notoriously difficult to detect, and often hide behind legitimate users or service accounts. These threats usually have a complex operational model such as the kill chain, or their behavior is not yet recognized as being bad, making them very difficult to detect using simple analytics such as pattern matching, thresholds or correlation rules. However, many of these advanced threats force assets to behave differently than what they usually do, often attached to unsuspecting users and identities — compromised insiders. UEBA techniques offer some interesting opportunities to detect these threats; improve signal-to-noise ratio; consolidate and reduce alert volume; prioritize alerts that remain; and facilitate efficient response and investigation. UEBA vendors that target this use case typically have tight two-way integrations with organizational SIEM tools.

- **Data exfiltration:** The use case in this domain is to detect the exfiltration of data in organizations. Vendors focused on this use case typically enhance existing data loss prevention (DLP) systems with anomaly detection and advanced analytics, thereby improving their signal-to-noise ratio, consolidating DLP alert volume and prioritizing alerts that remain. For additional context, they tend to integrate with, and rely more on, network traffic (for example, web proxy) and endpoint data, as the analysis of these data sources can help shed light on data exfiltration activities. Data exfiltration detection is used to catch both insiders and external hackers threatening an organization.

- **Identity and privileged access management (IAM and PAM):** Stand-alone UEBA vendors in this domain monitor and analyze user behavior against already-established access rights, with the goal of identifying excessive privileges or abnormal access. This holds true for all types of users and accounts, including privileged users and service accounts. Organizations have also used UEBA to help clean up dormant accounts and user privileges that are set higher than they need to be.

- **Incident prioritization:** In this use case, the goal is to help an organization prioritize the alerts that are being generated across all the solutions in its technology stack, and offer guidance on which incidents or potential incidents should be prioritized. UEBA tools and techniques are useful to understand what incidents are particularly abnormal or dangerous for a particular organization. In this case, the UEBA engine not only uses baselines and threat models, but also usually enriches these with knowledge about the organization's structure (for example, criticality of assets, and people's roles and access levels).

Analytics Methods Keep Getting More Sophisticated

The difficulty of solving the core UEBA use cases of incident detection, and the level of complexity of some of the latest attacks, is forcing vendors to implement ever more sophisticated algorithms to constantly improve the signal-to-noise ratio across multiple monitoring systems or other information sources that feed into their solutions (see "Focus on Use Cases to Select Your Security Analytics" and "Demystifying Security Analytics: Sources, Methods and Use Cases").

Advanced analytics and the type of ML used by vendors with UEBA functionality are key to their threat detection success and competitiveness in the industry. As of this Market Guide update, most stand-alone UEBA solution vendors are providing advanced analytics, while some vendors offering UEBA as a feature may have more work to do in that regard. Due to additional constraints such as potentially limited footprint and resources, or limited access to key data, some of these vendors still rely on basic analytics methods.

In the next few years, ML will start taking advantage of deep learning, where the models learn on their own from "training data," and select which attributes and variables to key their analytics off of. Gartner expects more buyers to become aware of and educated on the different types of analytics and their nuances. This will impact vendors that are not investing in more advanced analytics capabilities, as buyers tend to prefer vendors with advanced analytics over those with basic analytics.

Evolution From Rules and Notable Events to Advanced Analytics and Risk Scores

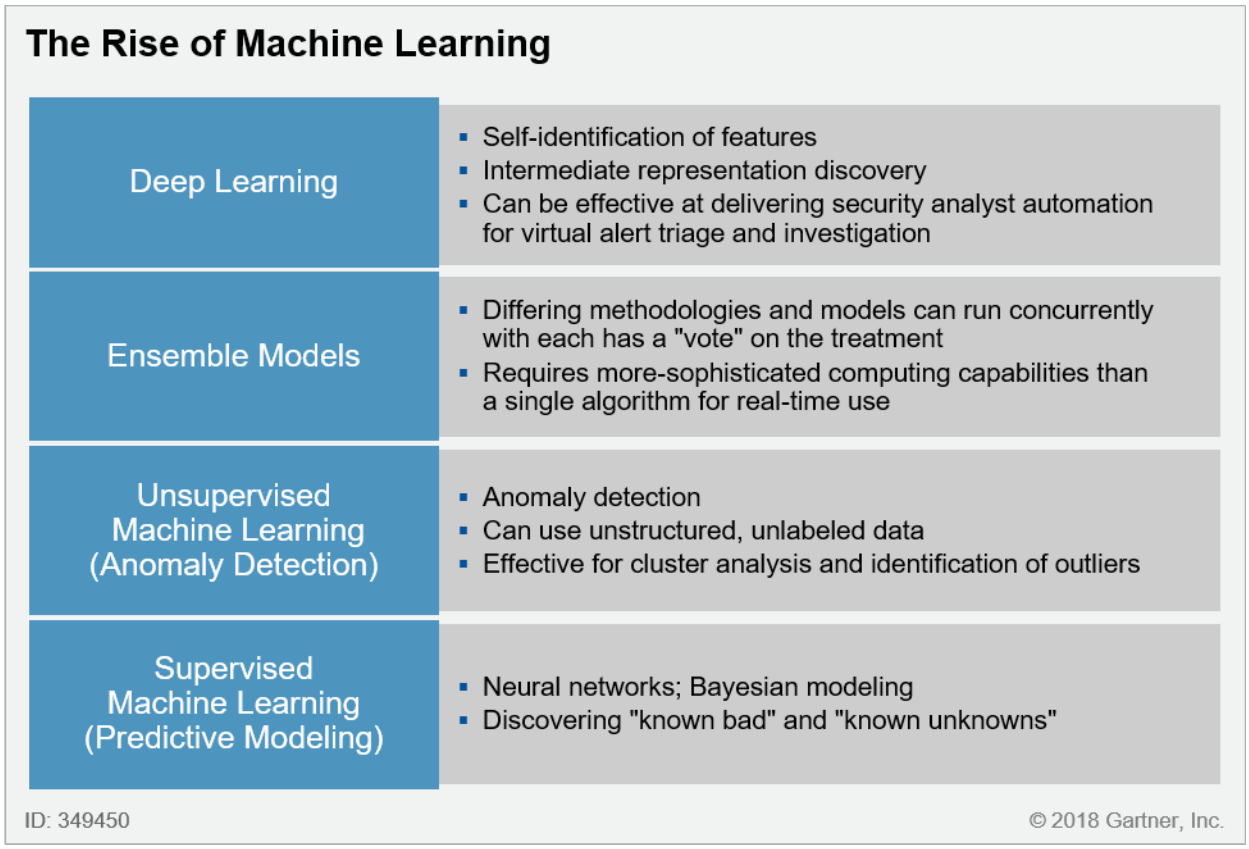
For the time being, UEBA vendors are mainly using ML and its three variants to perform the detection of anomalies. These variants are:

- Supervised ML: In this case, sets of known good behaviors and sets of known bad behaviors are fed to the system, which learns what good and bad behaviors look like. The tool can then detect bad behavior when it occurs. This approach often requires prior knowledge of what good and bad look like, so as to train the models. An alternate technique, mixing advantages of ML and rule-based techniques, are Bayesian networks; they could provide interesting insights into behavior modeling.
- Unsupervised ML: In this case, the system learns what normal behavior looks like, and can alert if the observed behavior is abnormal. The system will not know if a behavior is good or bad; it will just know that it is abnormal/anomalous. So the interpretation of the tool's output will be up to an analyst. UEBA vendors are improving upon this by offering models that focus on identifying anomalies that are indicative of threats so as to improve the signal-to-noise ratio.

- Reinforced/semisupervised ML: This is a hybrid model where unsupervised ML is used. Alert dispositions are fed back into the models to enable lower false positives and higher fidelity alerts. This "training on the fly" can take a long time before the models are efficient in detecting bad behaviors.

Figure 3 describes various analytics methods.

Figure 3. The Rise of Machine Learning



Source: Gartner (April 2018)

The net effect of these advanced analytics is to move away from the binary "all is fine"/"there is a threat" to an approach where each situation, user or asset carries a particular risk score based on the models and context of the organization.

Legacy analytics were deterministic by nature; when a rule triggers, then an alert is generated. Advanced analytics are heuristic by nature; models constantly compute the probability that an event is anomalous, the level of abnormality of the event and the likelihood that this anomaly is indicative of a threat. Hence, the notion of risk score based on these calculations, usually on a scale from zero (no risk) to 100 (extremely risky and extremely likely to be an active threat). Organizations can then transition from working alert by alert, and start focusing on entities, users or events with the highest score.

Defense in Depth for Analytics

Advanced analytics are complementary — not mutually exclusive — to simpler and more traditional analytics that have been used over the years. There is still a lot of value in using signatures, rules and thresholds to identify potential threats. Known threats, for example, can sometimes be described with signatures, and pattern matching makes for a cost-effective way to detect these threats in real time. Likewise, some abnormal business operations can be captured via rules and correlations, and threshold comparisons can have value in deciding what level of activity is unwanted.

UEBA vendors use a combination of several of these analytics methods for a "defense in depth" approach, where events go through several layers of analytics — from simple to more complex — rendering the identification of potential threats more efficient and more complete.

User Access to the Analytics

Vendors applying advanced analytics typically approach their development and refinement in the same way: Select a model; train, validate and refine the model; package the analytics for consumption in their solutions; and provide updates as they refine the model. However, differences exist in how users of the tools can interact with the analytics. Gartner defines this approach as:

- Closed — The vendor's analytics cannot be viewed or modified by users. Buyers must accept the use cases and models provided by the vendors, and are tied to their strategic direction and release schedule for new models and updates to existing models.
- Open — These products expose elements of the models to a user. Tools that use basic analytics tend to be open since the detection is primarily based on rules, signatures and pattern matching, which need humans to construct the rules to make the tools usable. UEBA tools that use more advanced analytics, like ML, may allow users to change the variables in models. This approach is not common in the marketplace, but increasingly Gartner sees vendors adopting a move from closed or partially exposed models to exposing almost full access to the underlying analytics and engine. Further, vendors are now considering the marketplace for exchange and monetization of security models.

Cautions About Profiling and Anomaly Detection

User and entity profiling and ML are still not sufficiently proven when it comes to detecting suspicious behavior among privileged users, developers and knowledgeable insiders. In these cases, organizations still have to rely partly on their own rules instead of solely on statistical analysis and ML. These rules can work well with vendor models, but users must take responsibility for writing and including them.

UEBA users should note that the behavior of privileged users, IT developers and others can be highly irregular depending on their job functions, making baselining user behavior through profiling and anomaly detection much more problematic.

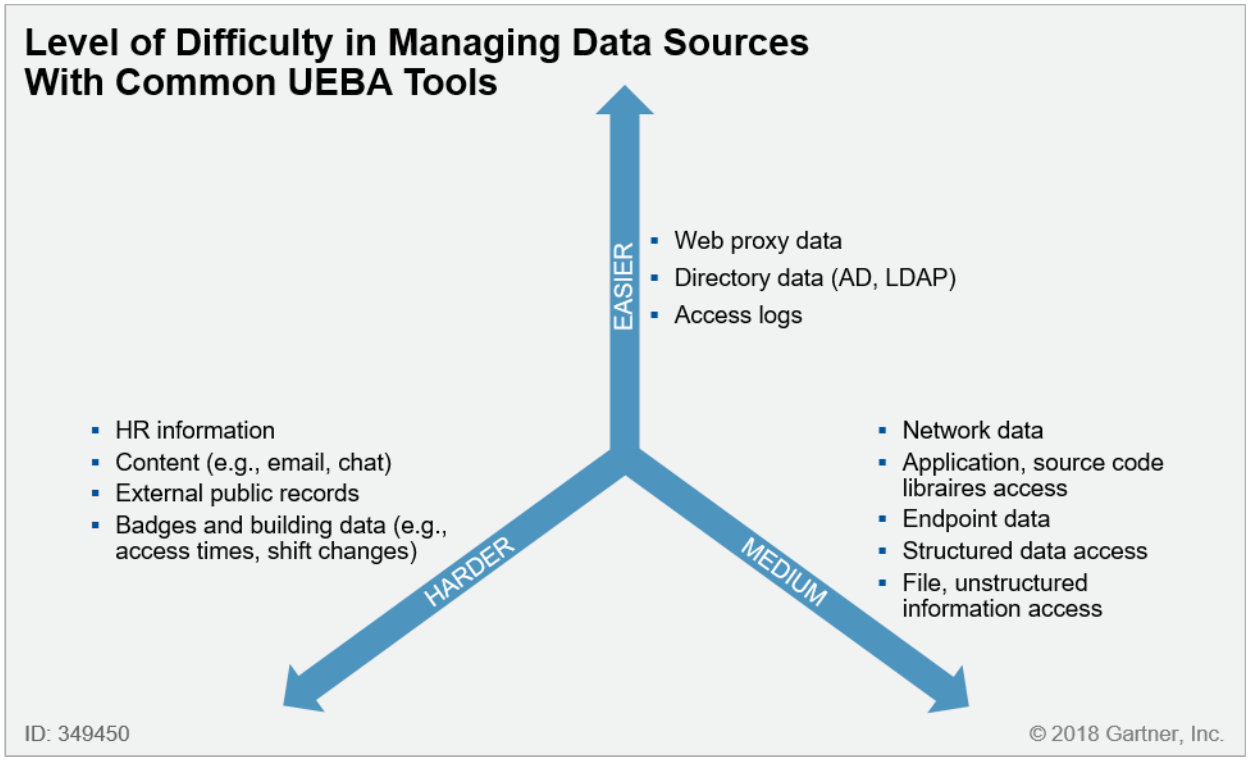
A given user or peer group can be bad from the start of profiling, so that ongoing bad behavior will not be noted as anomalous to the baseline. This caution applies to both privileged and

nonprivileged users. Re-profiling and re-establishing of baselines may be necessary. Determining the frequency of those activities, and whether they are built into the product or have to be planned for, is important.

Supported Data Sources Are Expanding to Provide Better Visibility

Likewise, in parallel with the complexity of the use cases and the sophistication of the analytics methods that need to be implemented, UEBA tools need ubiquitous access to more and more data. This can be raw data that is generated in real time such as logs from key devices and endpoints (for example, a native vendor app or an EDR agent), but also deep packet inspection of network traffic or context data that can be structured (such as HR databases) or nonstructured, such as Microsoft Skype IM messages. Many of these approaches demonstrate how stand-alone UEBA vendors, especially those with multi-use-case capabilities, are expanding their products' scope and removing their reliance on SIEM tools being their primary data sources (see Figure 4).

Figure 4. Level of Difficulty in Managing Data Sources With Common UEBA Tools



Source: Gartner (April 2018)

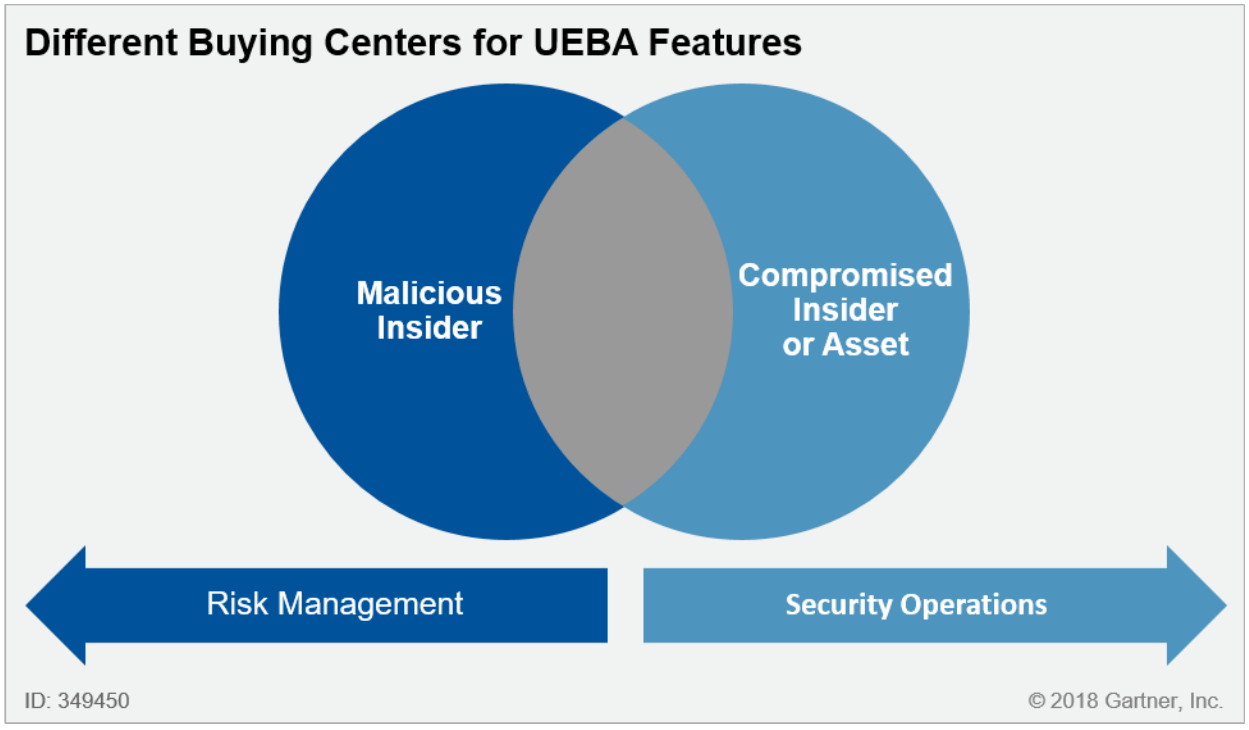
Who Buys UEBA?

Stand-alone UEBA tools currently appeal to mainly very large global organizations. Even among this group, interest is not ubiquitous, as UEBA solutions are expensive to acquire, implement, maintain and use, and represent yet another console while organizations are fighting portal fatigue. The tools'

varying investments in time and resources depend on the use cases and types of analytics employed. Buyers typically have specific drivers for purchasing a tool, such as improving their external threat detection capabilities by augmenting their SIEM solutions, or needing technology to support the build-out and running of an insider threat detection program. And some buyers are simply waiting for their SIEM to include UEBA features, while forward-leaning organizations pave the way, experiment and contribute to the emergence of best practices.

Different buying centers are looking at UEBA solutions, depending on organizations' use cases (see Figure 5). Security operations are primarily interested in improving the internal visibility for threat-detection-oriented use cases (i.e., the external attacker who has breached perimeter defenses and compromised an internal host and a user's credentials, and is using those to move laterally through an organization). Buyers oriented toward risk management responsibilities — especially in finance and healthcare — are focused on monitoring users to detect prohibited or unauthorized activities by trusted insiders, such as employees, contractors and external third parties. In some situations, buyers are interested in both use cases (for example, driven by a chief information security officer [CISO] with responsibilities for risk management and security operations), or have vague use cases around improving the security and risk management team's visibility of the IT environment. The two buyers may use the same tool to perform their jobs, but monitoring of trusted insiders is generally performed by a team that is distinctly separate from security operations due to the data sources typically involved, which raises privacy and regulatory issues for organizations, especially those operating in jurisdictions under tight regulatory schemes (for example, Europe).

Figure 5. Different Buying Centers for UEBA Features



Source: Gartner (April 2018)

How Is UEBA Implemented and Delivered?

Stand-alone UEBA tools are generally deployed on-premises or offered as a cloud-based service (with some requiring both). Often, stand-alone UEBA vendors require organizations to install appliances or deploy software for the core components of the solution, in addition to appliances (virtual or physical) for monitoring network traffic and endpoint agents. Some have specific requirements around data platforms, such as requiring that data be sent to a stand-alone data lake managed by the vendor.

Time to Value Is Often Underestimated

Contrary to many vendor claims, UEBA solutions are not "set and forget" tools that can be up and running in days. Gartner clients report that it takes three to six months to get a UEBA initiative off the ground and tuned to deliver on the use cases for which they were deployed.

In addition to the complexity of an organization's architecture, network topology and data governance issues, the ease and time of a UEBA implementation, and its future effectiveness, largely depend on:

- The sophistication of the vendor's analytics (that is, whether it incorporates statistical models and ML as opposed to just patterns and rules).
- How much of the analytics comes prepackaged (that is, the vendor knows which data to collect for the various use cases, and which variables and attributes are important to the analytics).
- How easy it is for the vendor to automatically integrate the required data and whether the customer can easily access that information. For example, if a UEBA solution uses an SIEM tool as its primary data source, is the SIEM tool already collecting the required data sources, and can the applicable log events and organizational context information be forwarded to the UEBA solution?
- How focused the organization's use case is, how many datasets the use case requires and how well the organization's use case aligns with the vendor's domain expertise.
- How much organizational involvement is required (for example, to write, evolve and tweak the rules and models, assign weights to variables selected for evaluation, and fine-tune the risk scoring thresholds).
- How scalable the vendor's solution and architecture is relative to the organization's current and future requirements.
- Time to build baselines, profiles and identify groups. Often, some vendors need 30 days (at a minimum, and sometimes up to 90 days) of data for their analytics before they can establish a "norm." Historical data can be used in batch mode to accelerate the training of the models. Interesting insights can be achieved more rapidly, but using rules (see the Defense in Depth for Analytics section).
- Level of effort to build dynamic peer grouping or account profiling (service/human) capabilities, which can vary greatly between solutions. Many vendors overstate their features here, so

organizations may be required to manually define, tune and clean up the groups, rather than relying on the tools to do this automatically.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

UEBA as a Feature Is Becoming More Widespread

Buyers must decide whether they will invest in a stand-alone UEBA solution or wait to see if products they already own will add UEBA functionality. Examples of where UEBA is being applied to specific use cases or where UEBA features are implemented to supplement basic analytics in other tools is addressed below.

Agent-Based Employee Monitoring

Gartner sees that tools focused on employee monitoring require very specific data that often require dedicated agents to be deployed to generate the necessary raw data. For example, employee monitoring solutions will, at times, need agents to reside in the endpoints to track mouse clicks and keyboard strokes for forensics purposes. In addition, UEBA functionality will be applied to these behaviors to detect anomalies.

Sample representative employee monitoring vendors that claim UEBA features include (see "Market Guide for Employee-Monitoring Products and Services" and "Market Insight: Increase Market Share With User-Aware and Bundled Endpoint Security"):

- Dtex Systems
- e-Safe Systems
- Forcepoint (formerly RedOwl, a UEBA solution)
- Haystax Technology
- ObserveIT
- Raytheon SureView
- Veriato (formerly SpectorSoft)

Agent-Based Endpoint Security

Sophistication of attacks to the endpoint, and the opportunity to detect misbehavior from malicious or compromised users within the endpoint themselves, requires the EPP/EDR vendors to get access to local data usually not provided by basic logs and visibility from the underlying OS. They will hence deploy agents in the endpoints to generate the necessary telemetry and data points. In the future, leading endpoint security (EPP/EDR) vendors may apply UEBA techniques to these data

points to provide advanced analytics capabilities for detection of anomalies for both users and entities.

Sample representative EPP/EDR vendors that claim UEBA features include (see "Magic Quadrant for Endpoint Protection Platforms"):

- Carbon Black
- Cisco
- CounterTack
- CrowdStrike
- Cybereason
- Cylance
- Rapid7
- SentinelOne

CASBs

Several CASB vendors claim varying degrees of UEBA capabilities by applying analytics techniques to observe how users interact with SaaS applications, and detecting risky or abnormal behaviors that indicate possible attacks. Gartner anticipates stand-alone UEBA solution vendors will expand their coverage to support CASB solutions as a data source.

Sample representative CASB vendors that claim UEBA features include (see "Magic Quadrant for Cloud Access Security Brokers"):

- Bitglass
- Forcepoint CASB (formerly Skyfence)
- Microsoft (formerly Adallom)
- Netskope
- Oracle CASB (formerly Palerra)
- McAfee (formerly Skyhigh)
- Symantec CloudSOC (formerly Elastica)

DCAP

Vendors that focus on improving the visibility of structured and unstructured data repositories have also begun to add UEBA functionality to their products, which has been noted as another component of the "entity" in the definition of UEBA. As an example, some vendors provide user

behavior analysis for monitoring of unstructured data access and use in various repositories. Others apply user behavior analytics to structured data being accessed via applications, with the ability to apply DCAP-type protections to the data, such as masking, tokenization and encryption.

Sample representative DCAP vendors that claim UEBA features include (see "Market Guide for Data-Centric Audit and Protection"):

- Datiphy
- Informatica
- SecuPi
- Symantec
- Varonis

Identity Governance and Administration (IGA)

Products that provide identity and privilege use analytics are also visible in the UEBA vendor space (see "2018 Planning Guide for Identity and Access Management"). Sample representative IGA vendors that claim UEBA features include (see "Magic Quadrant for Identity Governance and Administration" and "2018 Planning Guide for Identity and Access Management"):

- AlertEnterprise
- BeyondTrust
- CA Technologies
- Centrify
- Core Security
- CyberArk
- Micro Focus (through assets acquired from NetIQ)
- One Identity (through assets that came with the acquisition of Balabit)
- SailPoint
- SAP
- Saviynt
- Thycotic

Privileged Access Management (PAM)

Products that provide privilege use analytics can also embed UEBA features (see "2018 Planning Guide for Identity and Access Management"). Sample representative PAM vendors that claim UEBA features include (see "Market Guide for Privileged Access Management"):

- Core Security
- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Micro Focus (through assets acquired from Balabit)
- One Identity
- Thycotic

Intrusion Detection and Prevention Systems (IDPSs), and Network Traffic Analysis (NTA)

IDPS and NTA vendors offer network-based threat detection tools by applying UEBA features and techniques on network traffic instead of logs as their main source of data, often requiring dedicated instrumentation in the form of network appliances capturing specific network data. Network-centric tools also gather context on users from integration with Active Directory or other LDAP and IAM solutions deployed in organizations. This way, they can link IP addresses to user IDs, and network traffic is attributed to specific users, enriching the level of understanding of the network traffic and feeding visibility into potential anomalies.

Sample representative of IDPS and NTA vendors that claim UEBA features include (see "Magic Quadrant for Intrusion Detection and Prevention Systems" and "The Fast-Evolving State of Security Analytics, 2016").

- Arbor Networks
- BluVector
- Cisco (CTA)
- Darktrace
- Fidelis Cybersecurity
- Palo Alto Networks (formerly LightCyber)
- Phirelight
- ProtectWise
- SS8
- Vectra

SIEM

SIEM tools' natural extension is to always offer better analytics, so it is no surprise that SIEM vendors are embedding UEBA features as described in the SIEM and UEBA Are Converging section.

Sample representative SIEM vendors that claim UEBA features include (see "Magic Quadrant for Security Information and Event Management" and "Critical Capabilities for Security Information and Event Management"):

- Dell Technologies (RSA acquisition of Fortscale)
- Exabeam (also a stand-alone UEBA solution vendor; see Table 1 in the Stand-Alone UEBA Solutions Representative Vendors section)
- IBM
- FireEye
- LogRhythm (also a stand-alone UEBA solution vendor; see Table 1 in the Stand-Alone UEBA Solutions Representative Vendors section)
- McAfee
- Micro Focus ArcSight (via OEM of Securonix)
- Rapid7
- Securonix (also a stand-alone UEBA solution vendor; see Table 1 in the Stand-Alone UEBA Solutions Representative Vendors section)
- Splunk (also a stand-alone UEBA solution vendor after the Caspida acquisition; see Table 1 in the Stand-Alone UEBA Solutions Representative Vendors section)
- Venustech

Stand-Alone UEBA Solutions

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings, based on the criteria specified in the Market Description section. Some vendors are not captured in Table 1 (for example, solutions requiring dedicated sensors such as Microsoft Advanced Threat Analytics and Azure Advanced Threat Protection, or Preempt Behavioral Firewall). Please note that the use-case domains captured in Table 1 are not an exhaustive list of each vendor's capabilities.

Table 1. List of Representative Stand-Alone Pure-Play UEBA Solutions

Vendor	Solution Name	Year Founded	Domain No. 1	Domain No. 2	Domain No. 3	Delivery
Bay Dynamics	Risk Fabric	2001	Incident Prioritization	Data Exfiltration	Compromised Insider and Advanced Threats	On-premises/ Cloud
Exabeam	Advanced Analytics	2013	Compromised Insider and Advanced Threats	Malicious Insiders	Data Exfiltration	On-premises/ Cloud
Gurucul	Risk Analytics	2010	Advanced Threats	Malicious Insider	Data Exfiltration	On-premises/ Cloud
HPE Aruba-Niara	IntroSpect	2013 (Niara)	Compromised Insider and Advanced Threats	Data Exfiltration	Incident Prioritization	On-premises/ Cloud
Interset	Threat Detection Platform	2015	Malicious Insiders	Data Exfiltration	Compromised Insider and Advanced Threats	On-premises/ Cloud
LogRhythm	UEBA	2003	Malicious Insider	Compromised Insider and Advanced Threats	IAM and PAM	SaaS only
Securonix	UEBA	2008	Malicious Insider	Compromised Insider and Advanced Threats	Data Exfiltration	On-premises/ Cloud/SaaS
Splunk-Caspida	UBA	2014 (Caspida)	Compromised Insider and Advanced Threats	Malicious Insider	Data Exfiltration	On-premises/ Cloud

Source: Gartner (April 2018)

Market Recommendations

The following have been consistent attributes for the past two years of Gartner clients that have been more successful with their UEBA deployments. This list is not exhaustive, but rather offers pointers to help with the success of UEBA initiatives:

- Evaluate UEBA vendors with domain expertise that aligns with your primary use case. This includes, for example, improving security operations via anomaly detection; helping prioritize and enable more efficient response and investigations; monitoring use of privileges established in IAM systems; and pinpointing data exfiltration and leakage.
- Don't select a UEBA tool based on its ability to detect novel and interesting insights during the POC, but rather select a tool that delivers on your initial requirements, and demonstrates the ability to scale and evolve with your needs.
- When implementing a UEBA tool, start "small," with a narrow set of well-defined use cases and a limited set of data.
- Operationalize UEBA tools by integrating them with an SIEM, security orchestration, automation and response (SOAR) or service desk tool that provides ticketing and workflow capabilities, and allows continued monitoring of developer and privileged user behavior with current tools. UEBA anomaly detection is less reliable for these unpredictable users.
- Consider inclusion of network and endpoint data to gain additional visibility into user and application activity beyond what is present in log files. Also consider nonstructured behavioral information such as email, HR data and records, or social media activity to provide fuller context for user behavior analysis. However, be prepared for longer project timetables and the inability to fully automate their inclusion.
- Promote cultural change and executive-level interest in security and risk at your organization by using UEBA dashboards to present security and risk postures and indicators in a meaningful way to senior risk and security managers. This type of information presentation can be and has been used to promote organizations' continuing investments in UEBA solutions.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Focus on Use Cases to Select Your Security Analytics"

"Demystifying Security Analytics: Sources, Methods and Use Cases"

"Best Practices and Success Stories for User Behavior Analytics"

"Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management"

"Hype Cycle for Threat-Facing Technologies, 2017"

"Invest Implications: 'Forecast Snapshot: User and Entity Behavior Analytics, Worldwide, 2017'"

"Magic Quadrant for Intrusion Detection and Prevention Systems"

"The Fast-Evolving State of Security Analytics, 2016"

"Market Guide for Employee-Monitoring Products and Services"

"Market Insight: Increase Market Share With User-Aware and Bundled Endpoint Security"

"Market Guide for Data-Centric Audit and Protection"

"Magic Quadrant for Cloud Access Security Brokers"

"2018 Planning Guide for Identity and Access Management"

"Magic Quadrant for Identity Governance and Administration"

"Market Guide for Privileged Access Management"

"A Comparison of UEBA Technologies and Solutions"

"Market Guide for Online Fraud Detection"

Note 1 Representative Vendor Selection

Table 1 describes key attributes for the eight representative stand-alone pure-play UEBA solutions that comply with the four criteria established in the Market Description section. In addition, 57 representative vendors that embed UEBA features and functionality are listed across eight domains in the UEBA as a Feature Is Becoming More Widespread section.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp