Lookout®

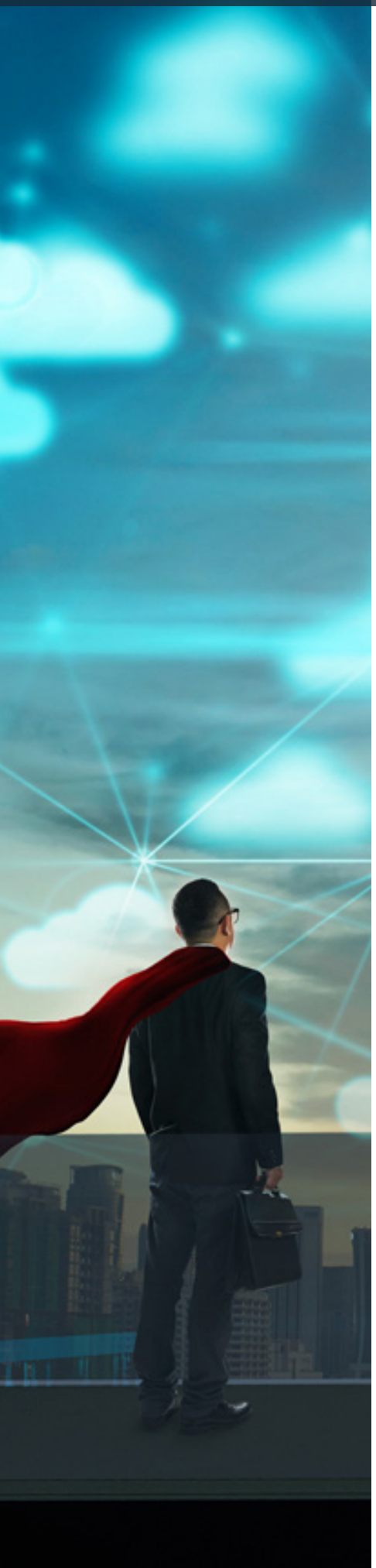
The Authoritative Guide to the Top CASB Use Cases

White Paper

Contents

Notice

Lookout publications are made available solely for general information purposes. The information contained in this publication is provided on an "as is" basis. Any additional developments or research since the date of publication will not be reflected in this report.



Overview

The move to the cloud has not been without significant challenges. Businesses are still deploying legacy security technologies that are designed to meet on-premise challenges. These legacy security architectures cannot meet the needs of the modern cloud with a mobile workforce and portable device environment. Cloud users are faced with a new set of opportunities for compromise, data breach, compliance failure, and loss of confidential information.

To meet these unique challenges, a new generation of technologies – called Cloud Access Security Brokers (CASB) – have emerged with the sole purpose of protecting corporations data when embracing cloud applications and services. This new technology introduces new use cases designed to address the most difficult problems in cloud computing. These use cases bring enhanced solutions for visibility, data protection, threat protection, and controls for comprehensive compliance support in order to allow successful and secure cloud deployments. The Lookout CASB platform expands traditional CASB capabilities with strong policy enforcement controls that are placed securely between the cloud providers and the customers that use them. CASB provides a wrapper to protect data and to insulate and isolate users from cloud threats and the inherent risks they bring to corporate networks.

"Use cases for CASB are critically important. Each CASB use case is centered around a problem statement, cost impact, and the well-defined benefits of using a CASB solution. Each of the Top Lookout use cases is driven by important return on investment. That's why companies of all sizes are driving the explosion in the CASB market."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

This white paper will share insight into the key use cases and overview the benefits that provide a strong return on investment for CASB users. The Top Threats Working Group of the Cloud Security Alliance published a comprehensive report on the Cloud Computing Top Threats and identified the most up-to-date, expert ranked understanding of cloud security risks. They include risks of cloud account hijacking, cloud data breaches, insecure application program interfaces (APIs), misconfiguration and administration errors, system vulnerability exploits, an expanded set of potential malicious insiders, advanced persistent threats, and much more. All of these well-defined threats are directly addressed within the CASB use cases and blocked by Lookout CASB deployment.

Important CASB Use Cases

These are the important CASB use cases for a CASB platform that would support multiple clouds. If you are looking for the use cases to support and protect a single cloud deployment such as Office 365, please refer to our separate documentation for that application. These are the use cases by category:

VISIBILITY	Securing Unsanctioned Clouds	Securing Sanctioned Clouds	Securing Custom Applications
Identify all clouds in use	✔	✔	✔
Identify the risks of the clouds in use	✔	✔	✔
Identify an audit trail of user activity for forensic investigation and e-discovery		✔	✔
DATA PROTECTION	**Securing Unsanctioned Clouds**	**Securing Sanctioned Clouds**	**Securing Custom Applications**
Implement policies for data loss prevention (DLP) for data uploaded and stored in the cloud	✔	✔	✔
Implement policies for collaborative governance with third parties and between internal groups		✔	✔
Implement policies to pseudonymize data using encryption to protect sensitive data		✔	✔
Implement policies to pseudonymize data using tokenization to protect sensitive data		✔	✔
Implement policies to provide data encryption key management, which eliminates cloud vendor access to your keys		✔	✔
Implement policies to provide digital rights management for digital documents		✔	✔
Implement policies for non-compliant devices using mobile device management		✔	✔
Implement policies for cloud governance to block access to cloud applications based on risk	✔		

THREAT PROTECTION	Securing Unsanctioned Clouds	Securing Sanctioned Clouds	Securing Custom Applications
Block threats from malicious insiders or compromised accounts based on activity before, during, and after login		✔	✔
Block malware and ransomware		✔	✔
Block APT attacks that target application program interfaces (APIs)		✔	✔
Block APT attacks that target cloud misconfiguration or administrative error		✔	✔
COMPLIANCE	**Securing Unsanctioned Clouds**	**Securing Sanctioned Clouds**	**Securing Custom Applications**
Implement policies to protect data using pseudonymization		✔	✔
Implement policies to prevent forced disclosure of your data by a cloud vendor		✔	✔
Implement policies for data sovereignty (data residency)		✔	✔
Implement policies for GDPR compliance for EU data privacy		✔	✔
Implement policies for HIPAA compliance for health care		✔	✔
Implement policies for PCI-DSS compliance in the financial industry		✔	✔
Implement policies for GLBA compliance in the financial industry		✔	✔
Implement policies for California Data Privacy compliance in 2020		✔	✔
Implement policies for Sarbanes Oxley Act compliance		✔	✔
Implement policies for FISMA compliance		✔	✔
Implement policies for ITAR compliance		✔	✔
Implement policies for NERC CIP compliance		✔	✔

Visibility Use Cases

Use Case #1 : Identify all cloud services in use

Problem Statement. The average enterprise may use hundreds of cloud applications of varying sizes, however in our estimate, the typical IT team has complete knowledge of only a small percentage of them. This automated discovery must find applications regardless of whether they are accessed from within the enterprise networks or remotely using mobile devices. Complete knowledge of all cloud usage is required to meet corporate governance, address compliance, utilize information technology and legal resources efficiently, and ensure that the security operations team integrates these clouds into their plans. All accessed clouds must be identified, categorized, and secured. If these are not authorized by corporate governance, then access must be shut down.

Problem Statement Example. A LATAM business unit has signed an agreement with a distributor in Europe and has bundled some of their software for resale in several countries including the European Community. This is a small contract and has not been visible to the governance and legal teams at corporate headquarters in the United States. The business unit uses a small third-party CRM application which they extend to the distributor in Europe for use in entering order data, including some elements of regulated data under the GDPR. The use of this application cloud creates a GDPR violation for the enterprise and violates data sovereignty, and creates the liability of a GDPR penalty if the data is subsequently breached or exposed.

Cost Impact if Unresolved. The cost of not identifying all of the clouds in use. The use of unsanctioned clouds exposes the enterprise to the unauthorized exposure or loss of sensitive, proprietary, and regulated data. By moving data into some of these unsanctioned clouds, enterprise employees might unknowingly be exposing the enterprise to compliance violations, which can result in large penalties, loss of reputation, and more.

Visibility

Current Solution. The current solutions in place rely on line of business executives and managers to identify unsanctioned (also referred to as "Shadow IT") clouds based upon their knowledge of use. Unfortunately, most of the time information technology, security operations, governance, and compliance teams are not receiving complete information. The use of dozens to many hundreds of clouds could go unreported. This happens for many reasons, including lack of visibility to what employees in their business unit are doing. The current solution relies too much on employee action based on understanding the policies.

CASB Solution and Benefits. CASB enables the automated discovery of all clouds in use in our organization. This benefits the enterprise by moving implementation of policies relating to unsanctioned cloud use from the discretion and action of personnel to automation which can identify this activity. If these unsanctioned clouds are not authorized by corporate governance, once identified access to these unsanctioned clouds can be shut down by CASB policy controls and your next-generation firewall system (NGFW). In contrast, sanctioned clouds are defined as those that are already configured and controlled by the CASB system.

Visibility

Use Case #2 : Identify the risks of the clouds in use by the enterprise

Problem Statement. It is important to understand the risks associated with the cloud currently in use, regardless of whether the clouds are sanctioned or part of Shadow IT usage. If the clouds are important to the enterprise, risks must be identified so they can be addressed appropriately.

Problem Statement Example. A major U.S. manufacturer has a small sales and marketing team. They maintain division social media accounts to connect with customers, prospects, partners, and suppliers. In order to assist with this process, a junior marketing team member has signed up to use an SaaS cloud service to assist with social media recruitment. This SaaS cloud service connects with their LinkedIn social media account and has access to all profile data. This SaaS cloud service appears to be legitimate, but unknown to the marketing team and the management of the division, the service does not have any certifications, does not have offsite disaster recovery, has minimal security capabilities, and the EULA was a click-through that was not reviewed from the corporate legal team before being accepted. All of these items combined elevate this cloud service to a significant risk and potential liability for the company.

Cost Impact if Unresolved. The cost of not identifying high-risk clouds in use could be substantial. The use of high-risk clouds exposes the enterprise to the unauthorized exposure or loss of sensitive, proprietary, and regulated data. By moving data into some of these high-risk clouds, enterprise employees might unknowingly be exposing the enterprise to data breach and the loss of high-value intellectual property as well as the sensitive and personal data of their employees, customers, and business partners. Once again, compliance violations brought by these high-risk clouds will also result in large penalties, loss of reputation, and more.

Current Solution. Most enterprises currently have no solutions in place to effectively ascertain high-risk cloud usage. Enterprise risks inherent in the administration and management of most cloud platforms and SaaS applications are unknown, especially to the line of business management that relies on them for critical enterprise operation. Unknowingly, the use of dozens of high-risk clouds continues with little additional security.

Visibility

CASB Solution and Benefits

CASB provides a comprehensive knowledge base for tens of thousands of cloud infrastructure and applications used globally. We constantly update this database with new SaaS applications and catalog the risk based on more than 60 attributes, including their known security vulnerabilities, attack vectors used, support for enterprise managed data encryption keys, use of end-to-end encryption, compliance capabilities, and more. This assessment produces a scoring which then enables the information technology team, security operations, governance, and compliance to view these in risk-based order, and can suggest alternative SaaS applications with lower risk potential. They can also make rapid decisions to remediate the risks using a full CASB implementation using data protection and threat protection features. This benefits the enterprise by building upon the use case for discoveryof unsanctioned cloud resources to now fully identifying and remediating risks on a prioritized basis. Once again, if the risks are high, and these clouds are not authorized by corporate governance they can be shut down once they are identified.

"VISIBILITY is critical to meeting cloud security and compliance. The IT and security operations center team must be able to identify all of the cloud services in use by an organization. They must be able to understand the risks of the clouds that are in use by your organization, and, they must have visibility to a complete audit trail of user activity to support forensic investigation. You must have all of this capability without compromise."

Sundaram Lakshmanan

Chief Technology Officer
Lookout

Visibility

Use Case #3 : Identify an audit trail of user activity for forensic investigation and e-discovery

Problem Statement. The typical enterprise may have one or more investigations ongoing which require some form of e-discovery. These may be driven by human resources, legal to satisfy a subpoena, governance, compliance, executive management, the board of directors, and other departments for a
variety of reasons. It is expensive and difficult to understand where all of the data is located. It is often more important to understand communications using corporate tools that reference that data and the history of access, duplication, download, and sharing of that data.

Problem Statement Example. There are many possible examples, some of which follow:

- The human resources team is investigating complaints that an employee was reviewing and downloading sexually explicit material using the company computers and networks.
- The office of the General Counsel is spearheading an investigation into the possible theft of confidential material and intellectual property by a past employee.
- The office of the General Counsel is involved in litigation and must comply rapidly and accurately with the requirements of a subpoena.
- The security operations team (SOC) has identified a cyberattacker that has been in the network for months, and during that time the cyberattacker obtained the credentials of several employees. The SOC team needs to understand all file and database access during that time period to restricted, confidential, and regulated data.
- The hospital compliance team is investigating a complaint that claims patient data was exposed in violation of HIPAA. They need an accurate and credible audit trail to determine exactly what data elements, if any, were actually exposed.

Cost Impact if Unresolved. The cost of not resolving these investigations in a timely way can be considerable. Ongoing cyberattack scenarios have a very high time-to-value ratio, as understanding the cyberattackers' activities are critical to securing data and resources at risk.

Current Solution. There are limited e-discovery tools used to examine email by keyword. IUt becomes more difficult, and at times impossible, to search the many other applications and the associated databases and file shares. It is often

Visibility

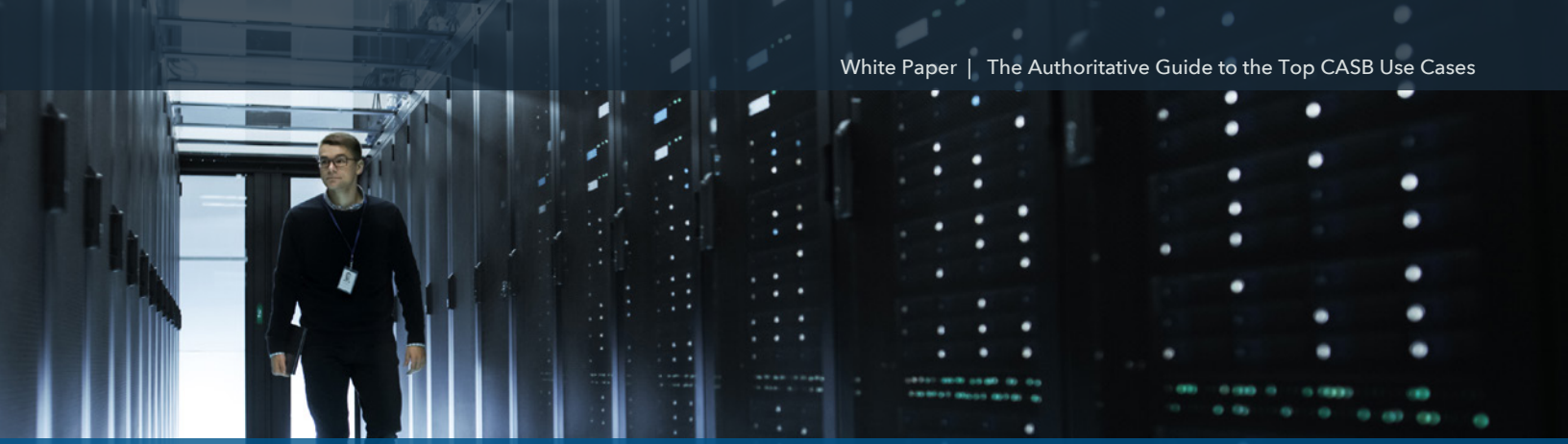
difficult to understand the trail of evidence that you must follow in terms of data and activity from application to application. The enterprise investigators need to be able to reconstruct the activity to understand what the user did with the content, by application, if the content was shared and by whom. The cost of doing this manually or using application-specific tools is substantial. These sorts of enterprise-wide investigations typically require the use of external law firms and on-site paralegals with attendant high cost. It also takes a long time to complete these manual investigations, typically many months.

CASB Solution and Benefits. CASB enables the e-discovery and audit of detailed cloud activity to include all applications and data elements. Activity can be reconstructed simply to understand resources accessed, by which user, by device, by IP address, time of day, which content, which application, and if the data was downloaded or subsequently shared. CASB+ accomplishes this analysis more completely and accurately, and in a more timely manner.

"Lookout is paving the way to a new era of secure multi-cloud adoption. CASB is the only solution that combines innovative capabilities with powerful data protection, completely protecting users, devices, and data in any cloud. We believe Lookout's position as a Visionary in the Gartner Magic Quadrant strongly validates our understanding and innovative approach to the cloud security market."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE



Data Protection Use Cases

Use Case #1 : Implement policies for data loss prevention (DLP) for data uploaded and stored in the cloud

Problem Statement. Typically, an enterprise has many types of sensitive and restricted data, including intellectual property, financial data, sensitive data as stipulated by compliance regulations, and more. If this data is not pseudonymized before being uploaded to the cloud, the data is not sufficiently protected, possibly resulting in theft of intellectual property and compliance failure. This problem occurs when employees use unsanctioned clouds, sanctioned clouds, and when deploying custom applications on Amazon AWS, Microsoft Azure, and Google Cloud Services platforms. This problem also happens when using applications such as Box.net, Dropbox, Exchange Online, Google Drive, Office 365, SkyDrive, Salesforce, Workday, SAP SuccessFactors, ServiceNow, and many others.

Problem Statement Example. Data with customer social security numbers should not be uploaded to the cloud. Several customer support representatives upload files to the corporate Box account and have accidentally included several documents with exposed social security numbers. This creates additional compliance failure as this data should not have been uploaded to the cloud before being protected by pseudonymization.

Cost Impact if Unresolved. In the event of a data breach, data that was not encrypted exposes the enterprise to penalties associated with compliance failure, breach notification, the risk to reputation and brand, and more.

Current Solution. Today, there are written policies requiring that employees be aware of these sensitive data types and how they may be uploaded to various sanctioned cloud services, with the specified levels of pseudonymization. These policies require employee judgment and are often accidentally overlooked or ignored.

Data Protection

CASB Solution and Benefits

Lookout DLP identifies restricted and sensitive content in real time. This includes support for data being uploaded to unsanctioned clouds, sanctioned clouds, and by custom cloud-based applications. For custom cloud-based applications, this includes both standard and custom native objects. This application awareness ensures that sensitive data is discovered in real time. When there are policy violations, Lookout DLP will enforce actions to include alerts, restricted sharing, or automatic encryption of sensitive files. Policies also can give the user time for self-remediation, which provides a time window to fix identified problems.

Lookout DLP also provides coaching coaching and guidance to employees so that better understanding and alignment with important enterprise data protection requirements are understood. Customers can also integrate DLP policies with existing on-premise enterprise DLP systems to preserve existing investments.

"DATA PROTECTION powered by end-to-end Zero Trust encryption has become essential for protection of data in the cloud. Data must be protected at rest in the database, in transit through the network, application program interfaces and more, and in use. Finally, under no circumstances should your data encryption keys be shared with any outside party. These are now essential elements of current best practices."

Mahesh Rachakonda

Vice President Product & Solution Engineering
Lookout

Data Protection

Use Case #2 : Implement policies for collaborative governance with third parties and between internal groups

Problem Statement. Typically, an enterprise has many types of sensitive and restricted data including intellectual property, financial data, sensitive data as stipulated by compliance regulations, and more. Policies for sharing data with third parties may vary considerably depending on governance and compliance requirements. There are also policies that require careful governance among internal groups.

Problem Statement Example. The enterprise is a public company and has financial statements ready for release followed shortly by the quarterly conference call. 16 (b) officers and senior staffers in the finance and sales departments have access to this information, but must not release it further within the company as it might result in illegal stock trades, done using this "insider information."

Cost Impact if Unresolved. In the event of an illegal stock trade or other use of insider information, there will be the costs resulting from negative publicity, damage to the brand, possible financial penalties, and more.

Current Solution. Today there are written policies that require employees tightly control this information before it is released at the end of a financial quarter. These policies require employee judgment and might be accidentally overlooked.

CASB+ Solution and Benefits. Lookout DLP can align with corporate governance on these policy requirements. Lookout DLP can identify restricted or sensitive content in real time. This application awareness ensures that sensitive data is discovered in real time. When there are policy violations, Lookout DLP will enforce actions to include alerts, restricted sharing, or automatic encryption of sensitive files. Policies also can give the user time for self-remediation, which provides a time window to fix identified problems. Lookout DLP also provides coaching and guidance to employees to foster better understanding and alignment with important enterprise data protection requirements. Customers can integrate DLP policies with existing on-premise enterprise DLP systems to preserve existing investments.

Data Protection

Use Case #3 : Implement policies to pseudonymize data using encryption to protect sensitive data

Problem Statement. Pseudonymization required by many compliance requirements. In some cases, only pseudonymization is requested, while in others use of encryption is requested. Pseudonymisation is the process whereby identifying fields within a database are identified and standards are replaced by non-identifying terms. The goal is to reduce concerns about the protection of data when in use, in transit, and at rest (in the database). Data must often be pseudonymized before being uploaded to the cloud to protect the data or avoid compliance failures and to eliminate data breach. Unauthorized access to pseudonymized data does not constitute a data breach or violation of compliance under most state, regional, industry, and national laws because the data is unintelligible.

Problem Statement Example. The GDPR requires that your business protect and pseudonymize data to be compliant. You have heard about GDPR, but you think that the data within your SaaS applications and other clouds is protected by the vendors. When you checked with them early in 2018, most of them appear not to encrypt data at all. The few that do encrypt data only encrypt it at rest in the database. During your trial implementation, you found that third-party software application functionality (you use several third-party plug-ins with just one of your major SaaS applications) no longer works. You have also lost functionality within the SaaS application.

Cost Impact if Unresolved. In the event of a data breach, data that was not encrypted exposes the enterprise to penalties associated with compliance failure, breach notification, the risk to reputation and brand, and more. Further, database-only encryption exposes your data to API-based attacks and compliance failure.

Current Solution. There is no current solution in place to support encryption of the data within most of your sanctioned clouds and custom applications hosted on Amazon AWS. You have one SaaS vendor that provides encryption; however, they request copies of your data encryption keys and still only manage to encrypt the data at rest (within the database). The requirement to have copies of your data encryption keys makes your solution non-compliant and exposes your data to forced third-party access.

CASB Solution and Benefits. Lookout provides Zero Trust end-to-end encryption in support of your sanctioned cloud applications and custom cloud-hosted applications. Zero Trust encryption starts at the enterprise "edge," so that all data entering the cloud is always encrypted. Zero Trust end-to-end encryption

Data Protection

meets all global compliance regulations and provides the highest levels of cyber threat protection because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The data is protected from the most complex threats and attacks, such as API-based attacks which target encrypted data. Further, Lookout CASB data encryption key management allows you to store your data encryption keys separately and never provide a copy to your cloud provider in violation of compliance requirements. Lookout's encryption and key management are held only by you.

"Lookout's Zero Trust end-to-end encryption encrypts or tokenizes the data at the enterprise "edge" before it leaves enterprise networks and enters the cloud. This allows the enterprise to retain encryption keys exclusively and continuously protects the data at rest, in use, and in transit through APIs, middleware, and the network. We believe that this is the stronge st and most comprehensive data protection available in the industry today."

Sundaram Lakshmanan

Chief Technology Officer
Lookout

Data Protection

Use Case #4 : Implement policies to pseudonymize data using tokenization to protect sensitive data

Problem Statement. There are many cases where an enterprise wants to mask or hide identifying data in an online cloud application. Tokenization replaces the original data with a "token," which contains no information from the original content. Unlike encryption, there is no mathematical tie between the token and the original data. Tokenization, also referred to as data masking, is commonly used to meet compliance requirements in countries or regions with strict data residency laws specifying that certain types of sensitive data cannot leave national boundaries.

In this case, if tokenized data from one country requiring "data sovereignty" is displayed through a browser in another country for which there is no agreement for data sharing, then there is no violation, as the tokenized data cannot be used to recreate the original data records and fields.

Problem Statement Example. An SaaS enterprise customer relationship management system includes sensitive billing data and financial account information about customers that should be visible only to select high-level managers in the organization. These fields must be restricted from the view of most customer service representatives, who might be located in one of several locations around the globe.

Cost Impact if Unresolved. In the event of a data breach, data that was not protected exposes the enterprise to penalties associated with compliance failure, breach notification, the risk to reputation and brand, and more.

Current Solution. There is no current solution in place to support most of your sanctioned clouds and custom applications hosted on Amazon AWS. You have one SaaS vendor that encrypts data at rest (within the database), but this not the same as tokenization. You need tokenization to meet several compliance requirements.

CASB Solution and Benefits. Lookout provides tokenization in support of your sanctioned cloud applications and custom cloud-hosted applications. Lookout CASB is the only cloud security platform that provides tokenization as an adjunct to encryption. Lookout's Global Data Security Report identified that almost 20 percent of enterprise customers required tokenization. In specific regions such as Europe and the Asia Pacific, tokenization was the only essential data tool for protecting the organization against accidental compliance violations. Tokenization is also often used for PCI compliance and meets Requirement 3 of the PCI Data Security Standard (PCI DSS) along with many other use cases.

Data Protection

Use Case #5 : Implement policies that restrict data encryption key management to internal use only

Problem Statement. Many cloud vendors require copies of your data encryption keys. Unfortunately, this opens you to data breaches due to misconfiguration, administrative error, or activities by malicious insiders that work for your cloud vendors. Finally, this opens you to forced disclosure of your data by these same cloud vendors, without your knowledge or permission.

Problem Statement Example. A malicious insider at one of your SaaS cloud vendors releases copies of the keys to a third party for financial gain.

Cost Impact if Unresolved. A resulting data breach could cause financial loss, reputational and brand damage, compliance penalties, and more.

Current Solution. There are very few solutions in place to encrypt your data within cloud applications. Further, there are even less that support your ability to completely control and manage your data encryption keys while you are using their cloud applications. You have one SaaS vendor that provides encryption, but still requests copies of your data encryption keys and still only manages to encrypt the data at rest (within the database).

CASB Solution and Benefits. Lookout provides Zero Trust end-to-end encryption in support of your sanctioned cloud applications and custom cloud-hosted applications. It starts at the enterprise "edge," so that all data entering the cloud is completely encrypted all of the time. Zero Trust end-to-end encryption meets all global compliance regulations and provides the highest levels of cyber threat protection because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The data is protected from the most complex threats and attacks such as API-based attacks which target encrypted data. Further, Lookout CASB data encryption key management allows you to store your keys separately and never provide a copy to your cloud provider in violation of compliance requirements. Lookout's encryption and key management are held with you only.

Data Protection

Use Case #6 : Implement policies to provide digital rights management for digital documents

Problem Statement. The enterprise wants to implement Digital Rights Management (DRM) to protect data across sanctioned clouds of all types. Digital rights management (DRM), originally designed for protecting copyrighted material in licensed distribution, allows enterprise and government to control access to digital documents which may contain copyright material, intellectual property, trade secrets, and other sensitive and confidential data. The purpose of enterprise DRM is to prevent unauthorized access, resharing, and redistribution of this digital data.

Problem Statement Example. A sensitive document is downloaded from one of your clouds onto a mobile device. The user then wants to email it to an outside party. Or a former employee wants to download cloud data and take it to a new employer, you have no way to restrict or control this transfer of your property.

Cost Impact if Unresolved. Data disclosure to an unauthorized third party could cause financial loss, reputational and brand damage, compliance penalties,| and more.

Current Solution. Today, many companies have written policies that require employees to be aware of sensitive data types and how they can be downloaded to mobile devices, personal devices, and, subsequently, shared with third parties. These policies require employee judgment and are often accidentally overlooked or ignored. There is also a DRM system in use in your legal department, but not used in conjunction with the cloud or other applications.

CASB Solution and Benefits. Lookoput's comprehensive data security also includes native DRM, which provides secure offline data access. Data that is downloaded from cloud applications to users' devices can still be protected, based on predefined policies. These policies can include defining what devices are allowed to access the data (for example, that users cannot use personal devices to access sensitive data). If downloaded data needs to be protected from misuse (for example, from a former employee taking customer data to their new employer), administrators can to retract access to the data, even if it was downloaded and copied to another device. Real-time key revocation can protect data even on lost and stolen devices. Lookout CASB is also integrated with major third-party DRM packages such as Microsoft's.

Data Protection

Use Case #7 : Implement policies for non-compliant devices using mobile device management

Problem Statement. Mobile devices might be stolen, "jailbroken," or in some other way deemed non-compliant. Jailbreaking mitigates security software restrictions by removing manufacturer or carrier restrictions from a mobile device platform. In this scenario, it is important to implement policies restricting access via the device and specifically blocking the download of content. Policies must allow the restriction of use and the download of data to bring your own device (BYOD - personal mobile device platforms), corporate owned personally enabled devices (COPE), or corporate owned business only (COBO) devices.

Problem Statement Example. A corporate mobile device has been lost and the administrator wants to suspend all access to corporate files from this device. In another example, the installed firewall is no longer working or is misconfigured.

Cost Impact if Unresolved. Data disclosure to an unauthorized party might cause financial loss, reputational and brand damage, compliance penalties, and more.

Current Solution. Today there might be written policies that restrict employees to the use of COBO, COPE, or BYOD devices, or some combination of them. Most of these are not well managed and rely on employee judgment and discretion. Cloud access seems to happen without much control or understanding of the devices used and their safety, let alone employee compliance with the existing policy.

CASB Solution and Benefits. Lookout device management brings support for internal and external collaborators, remote, real-time key revocation for lost or compromised devices, mobile and endpoint apps enabling file decryption by an authorized user. This is done by integration with VMWare Airwatch, a complete enterprise mobile device management enterprise-class application.

Data Protection

Use Case #8 : Implement policies for cloud governance to block access to cloud applications based on risk

Problem Statement. The average enterprise might use hundreds of cloud applications. Some unsanctioned cloud applications, based upon the judgment of management, might represent unnecessary risks to the organization for a variety of reasons. It is important that these designated high-risk clouds are not available for use from corporate networks, corporate devices, or used with corporate data.

Problem Statement Example. Let us consider an example in one company's marketing department. The marketing department is distributed and some of the marketing specialists have tried to use a lead gathering tool to work with social media. This company is based in Moscow, Russia, and in the opinion of management, this cloud application should not be used from any corporate network or computing platform. It also requires connection to corporate social media accounts, which management also believes presents a considerable risk.

Cost Impact if Unresolved. The cost of not stopping the use of a high-risk cloud application can be considerable. This application could provide unauthorized access to corporate data or expose the data with impact to reputation, civil litigation, and compliance penalties.

Current Solution. Today there are written policies that require employees to request approval for the use of outside clouds. These policies require employee judgment and are often overlooked or ignored as evidenced by the preponderance of Shadow IT clouds in production.

CASB Solution and Benefits. CASB enables the discovery and audit of detailed cloud activity to include all applications and data elements. Based upon a risk score initially provided by the Lookout database and subsequently updated and adjusted based upon customer input, all access to a designated "high risk" cloud application can be blocked automatically in real time. The application also provides user guidance and coaching, as it presents a message that may suggest sanctioned cloud applications. Risk scores are created from more than 60 attributes that include categories such as environment, compliance, privacy, and security.

Based upon your policy, integration between Lookout's CASB platform and your next-generation firewall (NGFW) can automatically block designated unsanctioned cloud use.

Threat Protection Use Cases

Use Case #1 : Block threats based on activity during and after login, and on parameters surrounding attempted login

Problem Statement. It is important to detect and respond to unusual employee activity which might suggest malicious behavior or compromised credentials and an ongoing cyberattack.

Problem Statement Example. An employee tries to log in to their account at 3:00 am from a personal device. The employee has worked for the enterprise for three years and has never logged in during this time period.

Cost Impact if Unresolved. In the event of a cyberattack, compromised credentials, or malicious employee behavior, there could be considerable financial loss, loss of reputation, damage to the brand, and fines due to compliance failure.

Current Solution. A few standalone IT tools provide this capability in part for on-premise software systems. A few can provide this sort of analysis for cloud-based applications, both for vendor-provided SaaS applications and in-house, custom-developed applications.

CASB Solution and Benefits. Lookout includes advanced threat protection capability to keep your sanctioned clouds and custom developed cloud-based applications secure and protected.

Our User Entity and Behavior Analytics (UEBA) capability uses machine learning to monitor user activity, including time of day of activity, attempts at bulk file download, and other anomalous behavior. UEBA can make real-time decisions to flag or block unusual activity based on variation from normal patterns.

Threat Protection

Our Adaptive Access Control (AAC) complements UEBA and adds capabilities to block access to what appears to be authorized users, based upon platforms used, originating location, and more that might suggest theft, compromise of authentication credentials, or a sophisticated cyberattack.

"In February 2016, the Top Threats Working Group of the Cloud Security Alliance® published the first edition of a comprehensive report on the Cloud Computing Top Threats. This document clearly identified the most up-to-date, expert-ranked understanding of cloud security risks. Lookout's CASB architecture was designed to directly address all cloud threats identified by the Cloud Security Alliance. Lookout CASB protects your sensitive data in the cloud from data breaches, insecure API interfaces, system vulnerabilities, account hijacking, malicious insiders, malware, advanced persistent threats, and much more."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

Our integration with VMware Workspace ONE (AirWatch) enables contextual 2-factor authentication. An enterprise can trigger 2-factor authentication selectively when a specific contextual factor, such as location, network, data or an abnormal user behavior is encountered. For example, employees logging into an application such as SForce, ServiceNow, or SAP SuccessFactors using an unmanaged device, or using a managed device but from a new location, could be asked to complete the 2-factor authentication process.

Threat Protection

Use Case #2 : Block malware and ransomware

Problem Statement. It is important to detect and respond to malware, ransomware, and other attacker tools that might be transported in within infected documents. Once in the cloud, if undetected, these tools can infect many documents and result in loss of data.

Problem Statement Example. A user uploads a document infected with ransomware into a corporate-sanctioned cloud. This cloud does not have the integral security to detect the ransomware which can now spread and wipe out the full repository of corporate documents.

Cost Impact if Unresolved. In the event of a cyberattack, compromised credentials, or malicious employee behavior, there may be considerable financial loss, loss of reputation, damage to the brand, and fines due to compliance failure.

Current Solution. There are standalone tools for on-premise threat detection. Similarly, cloud providers have an inconsistent mix of tools.

CASB Solution and Benefits. Virus, malware, and ransomware protection is provided by our anti-virus anti-malware (AVAM) scanning. This powerful option helps keeps cloud data safe. URL-based link protection and on-premise sandbox integration enable us to discover and remediate even the even Zero-Day threats. Lookout CASB provides one comprehensive and consistent approach for you to manage malware and ransomware threats for all of your sanctioned cloud applications and custom Amazon AWS, Microsoft Azure, or Google Cloud Services hosted applications.

Threat Protection

Use Case #3 : Block APT attacks that target application program interfaces (APIs)

Problem Statement. Advanced Persistent Threats often can invade cloud environments, seeking to compromise data. Once in the network, they can listen to network traffic, intercept additional credentials, and target and compromise even encrypted data through the application program interface (API). This needs to be secured to meet security and compliance requirements.

Problem Statement Example. API-based attacks are increasing. In 2018, the SForce marketing cloud experienced data exposure that would have allowed an API-based attack to access the internal encrypted database and then access data in an unencrypted format. Google Plus was similarly compromised according to a Wall Street Journal article in October 2018.

Cost Impact if Unresolved. In the event of a cyberattack, compromised credentials, or malicious employee behavior, there may be considerable financial loss, loss of reputation, damage to the brand, and fines applicable due to compliance failure.

Current Solution. There are very few solutions. Many SaaS application vendors provide database-only encryption but cannot detect, deter, or stop an API-based attack.

CASB Solution and Benefits. Lookout provides Zero Trust end-to-end encryption in support of your sanctioned cloud applications and custom cloud-hosted applications. It starts at the enterprise "edge," so that all data entering the cloud is completely encrypted all of the time. Zero Trust end-to-end encryption meets all global compliance regulations and provides the highest levels of cyber threat protection, because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The data is protected from the most complex threats and attacks, such as API-based attacks, which target the application interfaces to gain access to encrypted data at rest (in the database).

Threat Protection

Use Case #4 : Block APT attacks that target cloud misconfiguration or administrative error

Problem Statement. Advanced Persistent Threats often can invade cloud environments, seeking to compromise data. Once in the network, they can listen to network traffic and identify misconfiguration and administrative errors that allow access to data.

Problem Statement Example. There are many examples of misconfigurations resulting in data exposure and unauthorized access to cloud data. In November 2017, it was reported that the Pentagon accidentally shared 1.8 billion intelligence data objects in a database based on misconfigured Amazon S3 storage permissions. In October 2017, it was reported that Accenture inadvertently left a massive store of private data across four unsecured cloud servers, exposing highly sensitive passwords and secret decryption keys that could have inflicted considerable damage on the company and its customers. The servers, hosted on Amazon's S3 storage service, contained hundreds of gigabytes of data for the company's enterprise cloud offering, which the company claims provides support to the majority of the Fortune 100. In February 2018, it was reported that an affiliate of FedEx exposed the personal information of tens of thousands of users.

Cost Impact if Unresolved. In the event of a cyberattack, compromised credentials, or malicious employee behavior, there might be considerable financial loss, loss of reputation, damage to the brand, and fines due to compliance failure.

Current Solution. There are policies and procedures that attempt to minimize the occurrence of a misconfiguration, or administrative error. However, these depend on human behavior and judgment and cannot ensure the elimination of the problem. There are also automated standalone solutions for Cloud Security Posture Management (CSPM) that address this problem.

Threat Protection

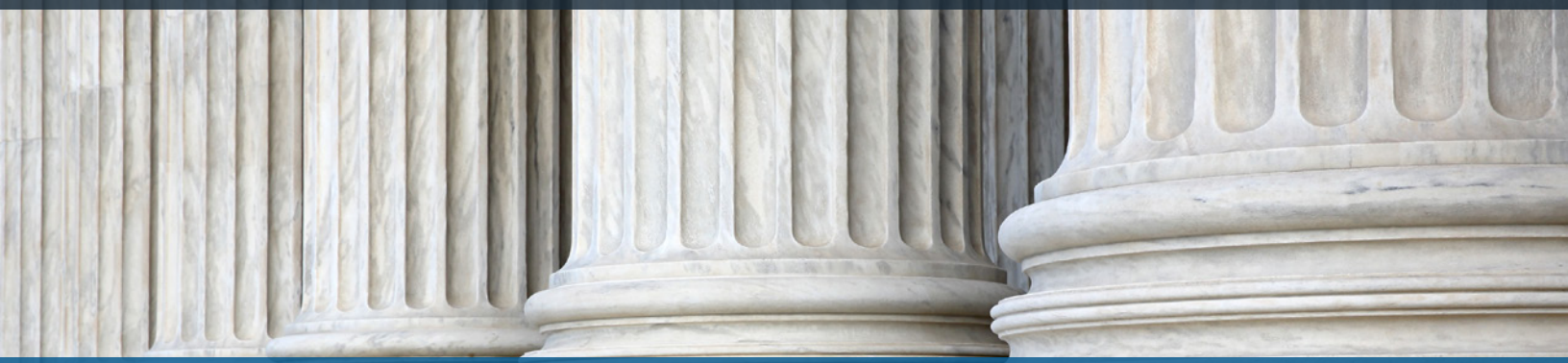
CASB Solution and Benefits. Lookout provides Zero Trust end-to-end encryption in support of your sanctioned cloud applications and custom cloud-hosted applications. It starts at the enterprise "edge," so that all data entering the cloud is always encrypted. Zero Trust end-to-end encryption meets all global compliance regulations and provides the highest levels of cyber threat protection, because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The data is protected from accidental exposure and subsequent breach through misconfiguration and administrative error.

"SaaS application vendors may request a copy of your data encryption keys to support their database encryption options. Respectfully submitted, this is something you should absolutely never do. This will open you up to additional risks which range from your vendor's malicious insiders, data exposure due to misconfiguration, the threat of forced disclosure without your knowledge, non-compliance with a multiplicity of different regulations, and more. Lookout CASB Zero Trust encryption ensures you never have to do this."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

Lookout also provides integration with CSPM that brings continuous oversight and real-time guardrails to protect critical administrative and configuration controls in your Amazon AWS, Microsoft Azure, and Google Cloud Services clouds. This affords yet another layer of protection for your cloud data.



Compliance Use Cases

Use Case #1 : Implement policies to protect data using pseudonymization

Problem Statement. Pseudonymization is required by many compliance requirements. In some cases, only pseudonymization is requested, while, in others, use of encryption, tokenization, or both is requested. Pseudonymization is the process whereby identifying fields within a database are replaced by non-identifying terms. The goal is to reduce concerns about the protection of data when in use, in transit, and at rest (in the database). Data must often be pseudonymized prior to uploading to the cloud to protect the data, avoid compliance failures, and eliminate data breach. Unauthorized access to encrypted data does not constitute a data breach or violation of compliance under the majority of state, regional, industry, and national laws because the data is unintelligible. Data might also be pseudonymized to meet the needs for data sovereignty (data residency), where data cannot be shared beyond the borders of a specific country or economic union.

Problem Statement Example. GDPR requires that your business protect and pseudonymize data to be compliant. You have heard about GDPR, but you think that data inside your SaaS applications and other clouds is protected by the vendors. When you checked with them early in 2018, it appeared that most of them do not encrypt data at all. The few that do encrypt data only encrypt the data at rest in the database. During your trial implementation, you found that software application functionality (you use several third-party plug-ins with one of your major SaaS applications) no longer works. You have also lost functionality within the SaaS application.

Cost Impact if Unresolved. In the event of a data breach, data that is not encrypted exposes the enterprise to penalties associated with compliance failure, breach notification, the risk to reputation and brand, and more.

Compliance

Current Solution. There is no current solution in place to support encryption of data within most of your sanctioned clouds and custom applications hosted on Amazon AWS. You have two SaaS vendors that provide encryption; however, they request copies of your data encryption keys and still only manage to encrypt the data at rest (within the database).

CASB Solution and Benefits. Lookout provides several solutions for pseudonymization that include Zero Trust end-to-end encryption and tokenization in support of your sanctioned cloud applications and custom cloud-hosted applications. It starts at the enterprise "edge," so that all data entering the cloud is always encrypted. Zero Trust end-to-end encryption meets all global compliance regulations and provides the highest levels of cyber threat protection, because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). Further, Lookout CASB data encryption key management allows you to store your data encryption keys separately and never provide a copy to your cloud provider in violation of compliance requirements. Lookout's encryption and key management are held only by you.

Lookout tokenization supports your sanctioned cloud applications and custom cloud-hosted applications. Tokenization, also referred to as data masking, is commonly used to meet compliance requirements in countries or regions with strict data residency laws specifying that certain types of sensitive data cannot leave national boundaries. If tokenized data from one country requiring "data sovereignty" is displayed through a browser in another country for which there is no agreement for data sharing, then there is no violation, as the tokenized data cannot be used under any circumstances to recreate the original data records and fields. Lookout's Global Data Security Report identified that almost 20 percent of enterprise customers required tokenization. In regionssuch as Europe and the Asia Pacific, tokenization was the only essential data tool for protecting the organization against accidental compliance violations. Tokenization is often used for PCI compliance and meets Requirement 3 of the PCI Data Security Standard (PCI DSS).

Compliance

Use Case #2 : Implement policies to prevent forced disclosure of your data by a cloud vendor

Problem Statement. Cloud vendors that hold your data in unencrypted format, or that hold a copy of your data encryption keys, can access your data or be compelled to access your data by government warrants and subpoenas. This can happen without your knowledge or permission.

Problem Statement Example. The U.S. government responds to a confidential EU request for data under the Clarifying Lawful Overseas Use of Data (CLOUD) Act. CLOUD Act allows federal law enforcement to serve warrants or subpoenas to cloud companies to provide requested data stored on cloud servers. These cloud companies must comply regardless of whether the data is stored in the U.S. or on foreign soil and regardless of whether the cloud companies are the data owners of record. The CLOUD Act may require a third party to release your data without your authorization or knowledge if they have the data encryption keys.

Cost Impact if Unresolved. In the event of a cyberattack, compromised credentials, or malicious behavior by employees of the cloud provider, there may be considerable financial loss, loss of reputation, damage to the brand, and fines due to compliance failure.

Current Solution. There is none unless the enterprise has 100 percent control of the data encryption keys and does not give them to the cloud provider.

CASB Solution and Benefits. Lookout provides Zero Trust end-to-end encryption in support of your sanctioned cloud applications and custom cloud-hosted applications. It starts at the enterprise "edge," so that all data entering the cloud is always encrypted. Zero Trust end-to-end encryption meets all global compliance regulations and provides the highest levels of cyber threat protection, because data must be encrypted while in transit (through the network), in use (on the client device), and at rest (in the database). The data is protected from exposure through forced disclosure by your cloud vendors, as they do not have access to the data encryption keys.

Compliance

Use Case #3 : Implement policies for data sovereignty (data residency)

Problem Statement. Many compliance regulations stipulate a requirement for data sovereignty (data residency). Data residency requires that all physical data be stored and maintained within the specified geographic borders or boundaries. These are often associated with the border of a country or economic union. One notable set of regulations is the EU General Data Protection Regulation (GDPR), which went into effect on May 28, 2018. The EU GDPR data privacy laws restrict organizations from transferring personal data that originated in Europe to any country with data protection laws deemed inadequate.

Problem Statement Example. Your company is a multinational organization based in Brazil. Personal data from customers in Germany must be restricted, and identifying data cannot be released. Manufacturing operations located in Brazil need to access the order number and parts listing to process it, but financial data, as well as other sensitive data, needs to be restricted from view in the Brazilian manufacturing facility.

Cost Impact if Unresolved. A violation of GDPR can have a massive financial impact – as much as four percent of annual global revenue.

Current Solution. GDPR is in full force and many companies do not have data sovereignty in place as required.

CASB Solution and Benefits. The Lookout CASB architecture uniquely enables the largest multinational company to deploy in alignment with complex compliance regulations, such as GDPR, HIPAA, PCI, GLBA, SOX, and many others around the world. Our unique hybrid deployment option allows any enterprise to manage one integrated secure deployment for key cloud applications across multiple countries, with controls and data encryption key management configurable to address a variety of regulatory requirements.

Each country might have different compliance controls for data privacy, data protection, data sovereignty, and data residency. The CASB platform can also support any combination of customer-controlled keys for multiple applications, in configurations that can include one or more on-premise key management systems.

Compliance

Many countries have data protection laws stipulating that processing of personal data for citizens occur within the country or within regions for which there is an adequate level of data protection (for example, GDPR). Most cloud providers cannot ensure this data residency because data can be moved between multiple regions, accessed by "command and control" in other countries, or accessed by remote support services offered across regions. Many global organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.

"COMPLIANCE remains the #1 driver for the implementation of CASB. This is because the web of cyber data privacy laws continues to grow both in number and complexity. This includes the EU General Data Protection Regulation that went into effect in May and the rapidly expanding tail of new legislation that includes the pending U.S. Cloud Act, the U.S. Encrypt Act, and California's new Consumer Privacy Act (effective 2020), and so much more. All of this new regulation sets the compliance bar higher than ever before for multinational companies around the world."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

Compliance

Use Case #4 : Implement policies for GDPR compliance for EU data privacy

Problem Statement. The General Data Protection Regulation (EU) 2016/679 (GDPR) regulates data protection and privacy for all individuals residing within the European Union. GDPR standardizes data protection law across all 28 EU countries and defines new rules for controlling and processing personally identifiable information (PII).

Problem Statement Example. A multinational company has headquarters in Argentina with business operations in Brazil, the United States, and the European Union. They must provide data sovereignty for the EU data and cannot share it with headquarters. Without a CASB product, this problem is almost impossible to solve without substantial impact on existing cloud-based SaaS and custom applications.

Cost Impact if Unresolved. A violation of GDPR can have a massive financial impact—as much as four percent of annual global revenue.

Current Solution. GDPR became operational on May 28, 2018. Many companies remain non-compliant today.

CASB Solution and Benefits. The Lookout CASB architecture enables the largest multinational companies to deploy in alignment with complex compliance regulations, such as GDPR. Our unique hybrid deployment option allows any enterprise to manage one integrated secure deployment for cloud applications across multiple countries, with controls and key management configurable to address a variety of regulatory requirements. Each country might have different compliance controls for data privacy, data protection, data sovereignty, and data residency. The CASB platform can also support any combination of customer-controlled keys for multiple applications, in configurations that can include one or more on-premise key management systems.

Many countries have data protection laws stipulating the processing of personal data for citizens must occur within the country or within regions for which there is an adequate level of data protection (for example, GDPR). Most cloud providers cannot ensure this data residency because data can be moved between multiple regions, accessed by "command and control" in other countries, or accessed by remote support services offered across regions. Many global organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.

> **"The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, providing that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."**
>
> European Union General Data Protection Regulation

Compliance

Use Case #5 : Implement policies for HIPAA compliance for health care

Problem Statement. HIPAA, the Health Insurance Portability and Accountability Act, defines the requirements for the protection of sensitive patient data. Regulated entities must ensure that all required physical, network, and process security measures are in place to adequately secure Protected Health Information (PHI).

Problem Statement Example. Regulated health care entities must provide policies for the implementation of HIPAA and a regular risk audit that comprehensively review information technology systems. Essential to all of this is the use of encryption to avoid the risk of data breach.

Cost Impact if Unresolved. The penalties for regulated entities (health care organizations) is based on the extent to which the HIPAA covered entity was aware that HIPAA rules were violated. The maximum civil penalty for knowingly violating HIPAA is $50,000 per violation up to a maximum of $1.5 million per violation category.

Current Solution. Use of the cloud has been difficult for health care companies. Security plans have generally been insufficient as far as preventing the breach of health care information stored in the cloud.

CASB Solution and Benefits. The Lookout CASB architecture enables any health care institution that seeks compliance cloud security to meet HIPAA requirements. Lookout CASB provides comprehensive end-to-end data encryption for cloud data to protect against cyberattack and the risk of data breach. This comprehensive protection enables health care institutions to address all identified cloud cyber risks with a comprehensive end-to-end strategy.

An essential requirement of HIPAA compliance is to maintain exclusive control of the data encryption keys. The CASB platform can also support any combination of customer-controlled keys for multiple applications, in configurations that can include one or more on-premise key management systems. Many health care organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.

Compliance

Use Case #6 : Implement policies for PCI-DSS compliance in the financial industry

Problem Statement. The Payment Card Industry Data Security Standard (PCI DSS) is required of companies that accept credit card payments. The Payment Card Industry Security Standards Council manages the Payment Card Industry (PCI) security standards. The PCI DSS is administered by the PCI SSC (www.pcisecuritystandards.org), an independent body formed by the major payment card brands to include Visa, MasterCard, American Express, Discover, and JCB. The PCI-DSS rules must be followed for a retail institution to use credit cards for payment by their customers.

Problem Statement Example. The PCI-DSS applies to every merchant who accepts payment cards, yet many merchants fail to understand the requirements for compliance. Many use cloud applications with a minimal understanding of how they can meet the requirements for card data security.

Cost Impact if Unresolved. Fines for PCI compliance failure can range from $5,000 to $100,000+. These fines are levied upon the merchant by their bank and may continue monthly until compliance issues are successfully addressed. At some point, for failure to comply, their ability to accept and process credit cards could be canceled.

Current Solution. Use of the cloud has been difficult for retail companies that must use card processing services. Security plans have generally been insufficient as far as preventing the breach of cloud-stored information.

"If clear-text account data is present (for example, in memory) in the cloud environment, or the ability to retrieve account data exists (for example, if decryption keys and encrypted data are present), all applicable PCI DSS requirements would apply to that environment."

PCI Security Standards Council

Compliance

CASB Solution and Benefits. The Lookout CASB architecture enables any financial institution that seeks compliance cloud security to meet PCI-DSS requirements. Lookout CASB provides comprehensive end-to-end data encryption and tokenization for cloud data to protect against cyberattack and the risk of data breach. This comprehensive protection enables financial institutions to address all identified cloud cyber risks with a comprehensive end-to-end strategy.

An essential requirement of PCI-DSS compliance is to protect stored cardholder data under requirement 3. Requirement 3 stipulates that protection methods such as encryption and data masking (tokenization) are critical components of cardholder data protection. As specified by PCI-DSS rule 3, if an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Lookout CASB enables financial institutions to maintain exclusive control of the data encryption keys. The CASB platform can also support any combination of customer-controlled keys for multiple applications, in configurations that can include one or more on-premise key management systems. Many financial and retail organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.

Compliance

Use Case #7 : Implement policies for GLBA compliance in the financial industry

Problem Statement. The Gramm-Leach-Bliley Act (GLBA) is the Financial Modernization Act of 1999. The GLBA requires financial institutions to explain how they share and protect their customers' private data. The Safeguards Rule requires that all financial institutions implement safeguards to protect customer information.

Problem Statement Example. Financial institutions must tell their customers how they share their customers' sensitive data, give customers the right to opt-out, and apply specifically defined protections to customer private data acording to an information security plan. This plan must identify and assess the risk to customer information within the information processing systems and share the current safeguards in place. They must design a safeguards program, using selected service providers, assess the risk and the program regularly, and test all safeguards regularly.

Cost Impact if Unresolved. Penalties for GLBA non-compliance could include imprisonment for up to five years as well as substantial financial penalties. A financial institution can be fined up to $100,000 for each violation. The officers and directors can be fined up to $10,000 for each violation of GLBA.

Current Solution. Most financial institutions have put a plan in place, but they do not have comprehensive security sufficient to safeguard cloud-based applications.

CASB+ Solution and Benefits. The Lookout CASB architecture enables any financial institution seeking compliance cloud security to meet GLBA requirements. Lookout CASB provides comprehensive end-to-end data encryption and tokenization for cloud data to protect against cyberattack and the risk of data breach. This comprehensive protection enables financial institutions to address all identified cloud cyber risks with a comprehensive end-to-end strategy.

Further, Lookout CASB enables financial institutions to maintain exclusive control of the data encryption keys. The CASB platform can also support any combination of customer-controlled keys for multiple applications, in configurations that can include one or more on-premise key management systems. Many financial organizations have not been able to adopt cloud applications without deploying additional security controls such as Lookout CASB.

Compliance

Use Case #8 : Implement policies for California Consumer Privacy Act compliance in 2020

Problem Statement. The California Consumer Privacy Act of 2018 was passed by the state of California legislature, and signed by its governor on June 28, 2018, and goes into full operation in January 2020. The Act gives California residents several basic rights in relation to their personal information. These include the right to know what data has been collected about them, the right to "opt out" of the sale of their personal data, the right to have business completely delete their personal data, and the right to receive equal service and pricing from a business, even if they exercise some or all of their rights under the Act.

Problem Statement Example. Companies across the United States are evaluating how to design and implement compliance with the CCPA. CCPA suggests the need for broadscale changes to corporate operating procedures within governance and compliance as well as changes to software systems and security infrastructure.

Cost Impact if Unresolved. The California Consumer Privacy Act of 2018 is similar in many ways to the European Union General Data Privacy Regulation (GDPR). GDPR fines can reach as much as four percent of a company's prior year global revenue. The California Consumer Privacy Act has a damage limit of $750 per person for each violation, but in some cases, the violation penalty can be much higher.

Current Solution. There are no current solutions in place.

CASB Solution and Benefits. The Lookout CASB brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support for all of your clouds. Lookout CASB brings powerful end-to-end Zero Trust encryption. This allows you to encrypt all of your sensitive data at the cloud "edge" so that at any time, and at any stage in the lifecycle of the data, it is encrypted and protected. This includes encryption at rest (in the database), in use, and in transit (middleware, API, network, etc.). Edge encryption is the only way to protect against API-based attacks, which could result in compliance failure under the CCPA.

Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have access to your data, including any third party that might be forced to provide access to your data encryption keys.

Compliance

"According to research done by Lookout in 2018, for over 67 percent of the hundreds of firms surveyed, the number one reason for choosing a CASB solution was to implement one or more compliance use cases.

Compliance controls must enable you to monitor and enforce interaction with unsanctioned clouds, sanctioned clouds, and any of your custom applications that are hosted in Amazon AWS, Microsoft Azure, Google Cloud Services, or any of the other public or private cloud services platforms."

Mahesh Rachakonda
Vice President Product & Solution Engineering
Lookout

In February 2016, the Top Threats Working Group of the Cloud Security Alliance® published the first edition of a comprehensive report on the Cloud Computing Top Threats. This seminal document clearly identified the most up-to-date, expert-ranked understanding of cloud security risks. The goal of this document is to assist stakeholders in making educated risk management decisions regarding cloud adoption strategies. Lookout's CASB architecture was designed to directly address all cloud threats identified by the Cloud Security Alliance including the API-based attacks that can foil and bypass at rest (in the database) encryption.

Looikout protects your sensitive data in the cloud from data breaches, insecure API interfaces, system vulnerabilities, account hijacking, malicious insiders, malware, advanced persistent threats, and more. Lookout's CASB enables you to meet the challenges of the California Consumer Privacy Act of 2018 successfully for all of your enterprise clouds.

Compliance

Use Case #9 : Implement policies for Sarbanes Oxley Act compliance

Problem Statement. The Sarbanes-Oxley Act (SOX) was passed in 2002 to protect shareholders and the general public from accounting errors and fraud, and to improve the accuracy of corporate filings and disclosures. The act defines strict deadlines for compliance and publishes rules and requirements which include the need for a thorough SOX audit. A SOX audit includes a comprehensive review of a company's internal controls to IT assets, including any computers, network hardware, and other electronic equipment that financial data passes through. Data security, threat protection, and visibility are key components of meeting SOX audit requirements.

Problem Statement Example. Sarbanes-Oxley compliance is mandatory. This compliance has become more difficult with the rapid evolution of cyber threats, particularly as applications have migrated to the cloud. It has become more difficult to protect cloud-based data against threats posed by malicious insiders, configuration errors, errors in administration, and the evolution of advanced cyber threats.

Cost Impact if Unresolved. A corporate officer who does not comply with Sarbanes-Oxley or submits an inaccurate certification is subject to a fine up to $1 million and 10 years in prison, even if the error in certification is done by mistake. If done on purpose, the fine can be up to $5 million and the sentence up to 20 years in prison.

"In a well-architected system, the cloud service provider does not have direct access to the keys. If a request a request is made for access to the data, the enterprise must be involved."

Gartner Group

Compliance

Current Solution. Public institutions have put a plan in place, but they do not have comprehensive security sufficient to safeguard cloud-based applications.

CASB+ Solution and Benefits. Lookout CASB brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support for all of your clouds. Lookout CASB brings powerful end-to-end Zero Trust encryption. This capability allows you to encrypt all of your sensitive data at the cloud "edge" so that at any time, and at any stage in the lifecycle of the data, it is encrypted and protected. This includes encryption at rest (in the database), in use, and in transit (middleware, API, network, etc.). Edge encryption is the only way to protect against API-based attacks.

Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have access to your data, including any third party that might be forced to provide access to your data encryption keys.

In February 2016, the Top Threats Working Group of the Cloud Security Alliance® published the first edition of a comprehensive report on the Cloud Computing Top Threats. This seminal document clearly identified the most up-to-date, expert ranked understanding of cloud security risks. The goal of this document is to assist stakeholders in making educated risk management decisions regarding cloud adoption strategies. Lookout's CASB architecture was designed to directly address all cloud threats identified by the Cloud Security Alliance including the API-based attacks that can foil and bypass at rest (in the database) encryption.

Lookout protects your sensitive data in the cloud from data breaches, insecure API interfaces, system vulnerabilities, account hijacking, malicious insiders, malware, advanced persistent threats, and more. Lookout's CASB enables you to meet the challenges of Sarbanes-Oxley as you continue your move to cloud-based applications.

Compliance

Use Case #10 : Implement policies for FISMA compliance

Problem Statement. The Federal Information Security Management Act (FISMA) is a United States federal law passed in 2002. FISMA requires federal agencies develop and implement a comprehensive information security and protection program. FISMA requires that agencies meet the key standards and guidelines defined by FIPS 199, FIPS 200, and NIST 800 series of documents. FISMA requires that federal agencies and regulated contractors maintain an information system inventory, risk categorization of systems and data, system security plan, and security controls per NIST SP 800-53, risk assessments, and necessary certification and accreditation.

Problem Statement Example. You are a major defense contractor that supplies the U.S. Department of the Navy. You need to ensure that you provide adequate and compliant security for your cloud application deployment.

Cost Impact if Unresolved. Government agencies and regulated contractors that fail to comply with FISMA can face a range of potential penalties. These can include potential censure by Congress, a reduction in federal funding, and reputational damage. The obvious ramifications for affected contractors include a loss or severe reduction in access to federal programs and contracts.

Current Solution. Cloud requirements for security are inadequately addressed. The use of the cloud has been difficult for regulated agencies. Security plans have, in general, been insufficient to prevent the breach of information stored in the cloud.

CASB Solution and Benefits. Lookout CASB brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support for all of your clouds. Lookout CASB brings powerful end-to-end Zero Trust encryption. This allows you to encrypt all of your sensitive data at the cloud "edge" so that at any time, and at any stage in the lifecycle of the data, it is encrypted and protected. This includes encryption at rest (in the database), in use, and in transit (middleware, API, network, etc.). Edge encryption is the best way to protect against API-based attacks.

Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have any access to your data, including any third party that might be forced to provide access to your data encryption keys.

In February 2016, the Top Threats Working Group of the Cloud Security Alliance® published the first edition of a comprehensive report on the Cloud Computing Top Threats. This seminal document clearly identified the most

Compliance

up-to-date, expert ranked understanding of cloud security risks. The goal of this document is to assist stakeholders in making educated risk management decisions regarding cloud adoption strategies. Lookout's CASB architecture was designed to directly address all cloud threats identified by the Cloud Security Alliance including the API-based attacks that can foil and bypass at rest (in the database) encryption.

Lookout protects your sensitive agency data in the cloud from data breaches, insecure API interfaces, system vulnerabilities, account hijacking, malicious insiders, malware, advanced persistent threats, and more. Lookout's CASB+ enables you to meet the challenges of FISMA successfully for all of your cloud-based deployments.

"In October of 2017, Gartner Group evaluated the 11 leading CASB vendor solutions across a mix of features including architecture, data security, threat protection, UEBA, compliance/risk, and enterprise integration.

The Lookout CASB platform received a perfect score of 100 percent in all areas evaluated. We are uniquely positioned to bring the strongest data security, powerful end-to-end encryption, and comprehensive threat protection to cloud users for any other mix of cloud applications within the enterprise."

Pravin Kothari

Lookout EVP, Product and Strategy, SASE

Compliance

Use Case #11 : Implement policies for ITAR compliance

Problem Statement. The International Traffic in Arms Regulations (ITAR), is a set of government rules that control the export and import of defense-related articles, services, and technology on the U.S. Munitions List (USML). ITAR is administered by the U.S. State Department Directorate of Defense Trade Controls. ITAR requires that defense-related technical data listed on the United States Munitions List USML be shared only with U.S. citizens absent special authorization or exemption. You must be able to track digital information which is regulated under ITAR and be prepared to demonstrate that you have met the requirements of the regulation.

Problem Statement Example. You are a major defense contractor that supplies the U.S. Department of the Navy. You are working with other contractors overseas. Information regulated by ITAR that you must protect may include computer files, blueprints, photographs, training material, planning documents, certain kinds of instructions, and more.

Cost Impact if Unresolved. Violating ITAR brings a high risk for both civil penalties, criminal penalties, being barred from future exports, and in some cases imprisonment. ITAR civil fines can go as high as $500,000 for a single violation. ITAR criminal penalties can be up to $1 million and up to 10 years imprisonment. Criminal penalties are generally associated with only willful noncompliance.

Current Solution. DOD contractors usually have written policies, but many have no specific software controls that track or protect technical data that is governed by ITAR.

CASB Solution and Benefits. The Lookout CASB brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support to meet ITAR compliance. We provide the controls to set policy and monitor activity related to ITAR data that is uploaded to the cloud, downloaded, or shared.

Lookout CASB brings end-to-end Zero Trust encryption which can ensure that your data is encrypted and protected at all time. Under ITAR, this technology is essential if you intend to store any material on public clouds. Lookout CASB allows you to encrypt all of your sensitive data at the cloud “edge” so that at any time, and at any stage in the lifecycle of the data, it is encrypted and protected. This includes encryption at rest (in the database), in use, and in transit

Compliance

(middleware, API, network, etc.). Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have any access to your data, including any third party that might be forced to provide access to your data encryption keys. CASB also provides tokenization, which may also be used to protect ITAR data stored in the cloud.

Lookout CASB can help ensure that only authorized individuals can access controlled ITAR data. In the case of audit or concern, you can also access logs showing all cloud data access to ITAR data by individual, time, date, and details on the data objects accessed.

"by 2022, 60% of large enterprises will use a CASB to govern some cloud services, up from less than 20% today."

Gartner Group

Compliance

Use Case #12 : Implement policies for NERC CIP Compliance

Problem Statement. The North American Electric Reliability Corporation (NERC) created in 1968, was a voluntary member organization. In 2006 the Federal Energy Regulatory Commission certified NERC as the electric reliability organization for the United States. FERC regulates the interstate transmission of electricity, natural gas and oil and oversees NERC in the United States. The NERC CIP (North American Electric Reliability Corporation critical infrastructure protection) plan is a set of requirements designed to secure the North American bulk electric system. NERC CIP defines Security Management Controls that must be documented as policies and reviewed on a regular basis. Each revision of the NERC CIP requirements expands the definition of critical assets and the technical requirements to secure them compliantly. The level of controls and audit reporting is also substantial for entities that are regulated under NERC CIP.

Problem Statement Example. You are a bulk power system owner or operator and you must comply with NERC-approved standards. You must comply with the information protection portion of NERC CIP-003-3. This requires that you have security management controls in place to protect critical cyber assets. If you have accidental data exposure, it could be used to compromise sensitive systems and infrastructure, either now, or during some future nation state or terrorist attack. You must have complete visibility into access and use of your data. You do not have sufficient protections for your cloud based assets and this is evident within your risk assessment.

Cost Impact if Unresolved. NERC CIP fines can range from hundreds of thousands of dollars to many millions of dollars. Regulated entities must have the necessary

Current Solution. The U.S. electric grid inclusive of all nuclear power plants now has resilient cybersecurity defenses. In sharp contrast, the typical cybersecurity posture for industrial systems is low. The current cyber defenses, especially as extended to cloud infrastructure, are woefully inadequate.

CASB Solution and Benefits. Lookout CASB brings a single unified platform to provide the necessary visibility, data protection, threat protection, and compliance support to meet NERC CIP compliance. We provide the controls to set policy and monitor activity related to NERC CIP that is uploaded to the cloud, downloaded, or shared.

Compliance

Lookout CASB brings end-to-end Zero Trust encryption which can ensure that your data is always encrypted and protected. Under NERC CIP, this technology is essential if you intend to store any material on the cloud. Lookout CASB allows you to encrypt all of your sensitive data at the cloud "edge" so that at any time, and at any stage in the lifecycle of the data, it is encrypted and protected. This includes encryption at rest (in the database), in use, and in transit (middleware, API, network, etc.). Lookout CASB allows you, and only you, to manage the data encryption keys that protect your data in the cloud. No one else will have access to your data, including any third party that might be forced to provide access to your data encryption keys. CASB also provides tokenization, which may also be used to protect NERC CIP data stored in the cloud.

Lookout CASB can help ensure that only authorized individuals can access controlled NERC CIP data. In the case of audit or concern, you also can access logs showing all cloud data access to regulated NERC CIP data by individual, time, date, and the details about specific data objects accessed.

CASB Brings Fast Time to Value

CASB Support For All of Your Clouds

CASB supports many popular SaaS-based business applications, including SAP SuccessFactors, ServiceNow, SForce, Office365®, Adobe®, Box®, Dropbox®, SAP S/4HANA, SAP Hybrid Cloud, and many others. CASB+ provides data protection to application content while preserving application functions and ensuring compliance beyond the SaaS application provider's offering. The PaaS ecosystem applications offered in each provider's marketplace are also protected by the CASB platform, providing customers with greater control and visibility over which data is shared with these third-party PaaS providers. This suite of capabilities gives you one consistent approach and front-end interface to protect your data and help enforce compliance across all of your cloud environments. CASB extends our security to the enterprise edge, so there is never any data within your clouds that is not protected, either by encryption or tokenization.

CASB delivers fast time to value by supporting major enterprise integrations. Your team can integrate CASB smoothly with enterprise solutions such as SIEM, SSO, EMM, DRM, MDM, and more.

CASB Supports Your Custom Applications

Our Lookout CASB AnyApp™ connector allows customers to integrate these powerful data protection capabilities for their own custom cloud-based applications. This allows enterprises to ensure that customer applications will be able to protect data regardless of their chosen cloud platform. AnyApp allows customers to bring their custom cloud-based applications the benefits of encryption, tokenization, dynamic access control, DRM, UEBA, threat prevention, and many other security features.

CASB Delivery Models Speed Deployment

You can deploy in a matter of hours by using our hosted delivery. Administration and setup are simplified and fast, so you can set up our powerful CASB protection to secure, for example, your ServiceNow instance in hours, ensuring that all protection is applied beyond data encryption. We also support on-premise deployment in your data centers, fully hosted in the cloud, as well as hybrid (combining on-premise and hosted) options as necessary to support your compliance and operations strategy. Our cloud-native CASB platform simplifies deployment substantially and extends the definition of CASB to add end-to-end data protection with major enterprise SaaS, PaaS, and IaaS applications.

The Lookout platform architecture supports flexible and fast deployment. Our Cloud Security Broker (CSB) provides API-connected integration to allow CASB capabilities to be embedded and used by SaaS vendor-provided applications. CSB uses the APIs published and supported by the cloud providers. The CSB integration model allows a deeper inspection of all the users, content, and collaboration aspects of select clouds to achieve higher levels of monitoring, control, and protection (encryption).

Cloud Security Gateway (CSG) is an inline proxy to enforce the strongest security policies and achieve data protection. Our inline support for applications provides the deepest and completely transparent field-level data protection for vendor-provided SaaS programs, such as SForce, SAP SuccessFactors, ServiceNow, and many others, as well as for your custom applications.

The Largest Multinational Companies in the World Use Lookout

5 of the Top 10 U.S. Banks

6 of the Top Banks Worldwide

3 of the Top 10 Insurance Firms

3 of the Top 10 U.S. Health Care Firms

3 of the Top 10 Pharmaceutical Firms

2 of the Largest Telecommunications Firms

Government agencies in the United States,

United Kingdom, Canada, Australia, and beyond

"A truly innovative product, enabling cloud adoption by even the most risk-averse organization."

SC Magazine Judge, UK

"Lookout is helping businesses that could not otherwise adopt the cloud because of compliance and security concerns."

SC Magazine Judge, US

"Lookout ensures that customers are the only ones that can access data in the cloud while preserving the native user experience."

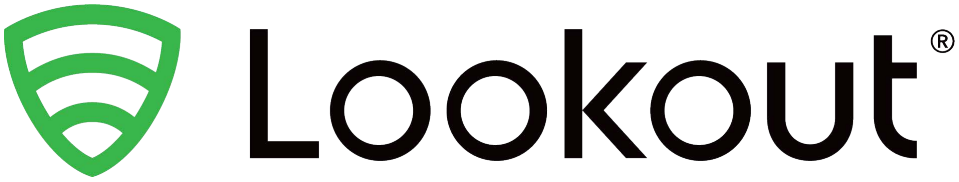
SC Magazine Judge, UK

"Cloud is here to stay and this (Lookout) lets it work in a safe manner."

SC Magazine Judge, UK

"This (Lookout) software meets a very real need for most companies moving forward."

SC magazine Judge, UK



About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

and Office 365® are registered trademarks of Microsoft®. SAP® SuccessFactors® are registered trademarks of SAP. ServiceNow®