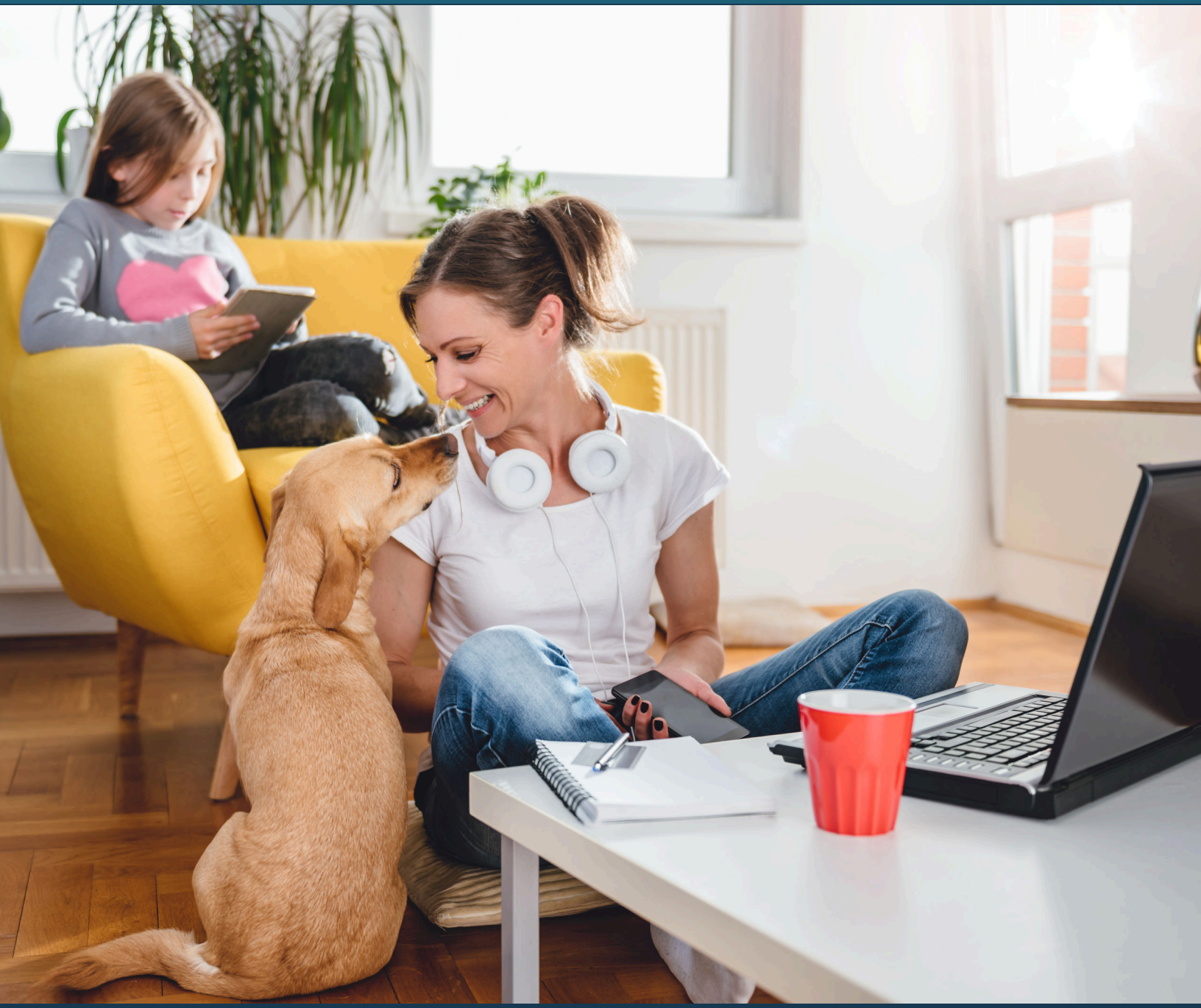
Lookout®

CISO's Guide for Securing the Remote Workforce

10 Use Cases for enabling Data Visibility, Protection and Compliance in the SaaS-Mobile Environment



White Paper

Content

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.

The world is witnessing an unseen trend in the past few weeks - industries across all sectors are rolling out remote workforce policies for their global staff as they brace for the new norm while maintaining business continuity. The sudden influx of employees connecting remotely has definitely put a strain on existing legacy network infrastructures, leaving many with sub-par connectivity and security. Organizations are scrambling to maintain data protection and compliance in this new remote workforce environment, prompting them to adopt a cloud-first strategy to ensure business continuity and high availability of servers and applications. Yet remote workers connecting direct-to-net using unmanaged devices and collaborating with SaaS applications to continue their day-to-day operations has in turn significantly increased the risk of data breaches, compliance failure, and loss of confidential information.

"IT teams need to get visibility into the data and user activity of remote workers to ensure sensitive data and PII is protected."

Salah Nassar,

Vice President of Marketing,
Lookout

Meeting these unique digital transformations and work-from-home challenges require a uniquely future-proof technology with comprehensive security capabilities that follow the data from device to the cloud, and vice-versa. Cloud Access Security Brokers (CASB) have emerged with the sole purpose of protecting corporations' data in a cloud-mobile environment, allowing them to seamlessly embrace cloud applications and services. CASB 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 human-centric and data-centric policy enforcement controls that are placed securely between the cloud providers and the customers that use them. CASB acts as the security gatekeeper to protect data and to insulate and isolate users from cloud threats and the inherent risks they bring to corporate networks.

"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 protect-ing users, devices, and data in any cloud. We believe Lookout's position as Visionaly 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

This white paper will share insight into the key CASB use cases to secure the remote working environment, enabling business continuity and 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 many more. All of these well-defined threats are directly addressed within the CASB use cases and blocked by Lookout CASB deployment.

USE CASE 1

Achieve full visibility of cloud apps being utilized in the organization

Pain Point

The average enterprise may use hundreds of cloud applications of varying sizes, but, in our estimate, the typical IT team has limited insights into all the applications in use. Complete knowledge of all cloud usage is required to meet corporate governance, stay compliant with the data privacy laws, efficiently utilize information technology and legal resources, and ensure there are no overlooked open shares and blind spots that might compromise enterprise security.

Pain Point Example

A healthcare institute has adopted work-from-home policy but its IT team is challenged with keeping track of all the users connecting directly to the cloud and sharing sensitive PHI data over SaaS apps. Lack of data visibility over the sanctioned and unsanctioned cloud usage might lead to data leaks, resulting in HIPAA violation for the institute.

Cost Impact if Unresolved

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

CASB Solution and Benefits

CASB Shadow IT Discovery streams logs from any network device and enables the automat-ed discovery of all of the clouds in use. Shadow IT Discovery provides a clear picture of the enterprises' risk exposure by scanning over 20,000 cloud applications and analyzing over 60 attributes to identify and classify the riskiest cloud apps that can lead to sensitive data loss.

CASB also performs Deep Application Intelligence to secure all major application activities, and not just data upload and downloads. CASB discovers and differentiates between different application instances in use to manage external collaboration and prevent open shares to secure files and folders in real-time.

"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, Looukout

USE CASE 2

Visibility into historical cloud data

Pain Point

With enterprises deploying additional SaaS and IaaS clouds to meet their business needs, the sensitive data today may reside across multiple apps, databases and personal devices. Without proper visibility, enterprises run the risk of compliance failure, security vulnerabilities and data breaches. It is of paramount importance that the enterprises first take a step back and get an assessment of archived or historical data that has been residing in their cloud for years.

Pain Point Example

An organization doing business in the State of California wants to ensure its business opera-tions are compliant with the CCPA regulations. It upgraded the security posture of its cloud application by deploying a cloud data protection solution to encrypt all customers records in real-time, but it failed to audit the historical data hosted in the cloud for years. A quick scan of that data revealed multiple compliance and data privacy failures.

Cost Impact if Unresolved

The cost of not identifying all the sensitive content in the clouds in use is potentially very high. A violation of GDPR or CCPA can have massive financial impact on the organization. Moreover, 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.

CASB+ Solution and Benefits

CASB+ Cloud Data Discovery (CDD) allows organizations to discover and classify data already stored in leading SaaS applications. While the first versions of CASBs focused on the data going into the cloud, they lacked the visibility into the data that was already stored in the cloud. With Cloud Data Discovery, organizations can scan historical data across multiple cloud apps, right from field-level information in structured clouds, such as ServiceNow and Salesforce, and unstructured data, files in collaboration apps, such as Office 365, Slack and Box.

USE CASE 3

Automatically detect and remediate malicious user behavior

Pain Point

It is important to monitor the user activity in the cloud-mobile environment, and detect and respond to unusual employee activity which might be suggestive of malicious behavior or of compromised credentials and an ongoing cyberattack.

Pain Point Example

An employee tries to log in to their account at 3 am from a personal device. They have worked for the enterprise for three years and have never logged in during this time period, even while working from home. Or, an employee based out of Chicago, Illinois attempts a valid log-in from Beijing only two hours after logging in from home.

Cost Impact if Unresolved

In the event of an external threat or malicious employee behavior, there may be considerable financial loss, loss of reputation, damage to the brand, and fines applicable due to compliance failure.

CASB Solution and Benefits

Lookout CASB includes advanced user behavior analytics and threat protection capabilities to keep your sanctioned clouds and custom-developed cloud-based applications secure and protected from unidentified and malicious users.

CASB User Entity and Behaviour Analytics (UEBA) capability uses machine learning to monitor user activity, including the 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. CASB UEBA collects 60+ attributes for every user activity and generates detailed audit logs to help in forensic analysis.

CASB Incident Insights points and clicks every device, user and application activity in the cloud, with drill-down reports to the last detail and relationships.

USE CASE 4

Identify and protect from unauthorized account access

Pain Point

As cloud-based collaboration and file sharing rapidly grow, you need assurance that users accessing SaaS applications, where sensitive or critical data are being stored, are who they say they are.

Pain Point Example

A cloud account getting compromised because of stolen user credentials or a verified user becomes a malicious insider and steals sensitive corporate data.

Cost Impact if Unresolved

If user credential is the key, your data is the crown jewel. If either is compromised, the conse-quences are severe and can lead to lawsuits, revenue loss, severe regulation fines, and the loss of a company's reputation.

CASB Solution and Benefits

Lookout CASB delivers end-to-end user and data security from any device, any location, to all trusted cloud applications, providing organizations the first step towards achieving Zero Trust Cloud Security.

CASB integrates with IDaaS solutions, such as Okta, to verify the user-integrity and control access at the door with Single Sign-On (SSO) and Multi-Factor Authentication (MFA).

Lookout CASB Adaptive Access Control complements the integration with IDaaS and performs a continuous risk assessment of verified users connecting from any location or device to cloud applications, enabling contextual access and protecting the end-to-end user journey with a zero-trust data security approach. CASB monitors the user behavior with User and Entity Behavior Analytics (UEBA) and can terminate the access privileges or prompt for reconnection with step-up authentication based on the user behavior risk, securing every user action from login to logout.

USE CASE 5

Identify and secure communication at rest and in motion

"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

Pain Point

There are many types of sensitive and restricted data within the enterprise, including intellectual property, financial data, sensitive data as stipulated by compliance regula-tions, and more. If there are not enough security controls around the data then the organization runs the risk of data leaks, theft of intellectual property and compliance failure. Organizations must enable full visibility and control over sensitive data in motion, in use or at rest, especially when hosting employee and customer records in CRM, HRM and ITES clouds such as Salesforce and ServiceNow, or collaborating over cloud-based email services and sharing information across multiple SaaS applications such as Office 365, Box, Google Drive, and Slack.

Pain Point Example

Sensitive content should be secured with data protection controls (encryption, masking, classification) before uploading to the cloud. A remote worker has logged in to corporate Box account from home and accidentally uploaded several documents with exposed social security numbers. Employees can download sensitive content from the cloud and share it with external agents over emails. This creates additional compliance failure as this data should not have been uploaded to the cloud without being protected by pseudonymization.

Cost Impact if Unresolved

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

CASB Solution and Benefits

Lookout CASB Data Loss Prevention (DLPs) includes granular policy controls to identify restricted and sensitive content in real-time. CASB DLP enables multi-cloud protection with a consistent DLP interface to secure data across the widest range of SaaS and IaaS clouds and even custom applications. You can also integrate CASB with your existing enterprise DLP products so that policies can be applied consistently across your enterprise, further preserving your security investments.

For Email data protection, Lookout offers the industry's first secure email gateway solution integrated within CASB, which allows emails from any client device (desktop, mobile, browser) to be routed through a secure dedicated gateway and enforcing DLP policies on the emails before they get delivered to the recipients. Email data protection includes sensitive content masking from subject and body, data rights management, and encrypting attachments.

USE CASE 6

Secure offline collaboration

Pain Point

Enterprises want their sensitive content to retain data protection capabilities when it gets downloaded from the cloud. Information Rights Management (DRM), originally designed for protecting copyrighted material in licensed distribution, allows enterprise and government to control access to digital documents that may contain copyright material, intellectual property, trade secrets, and other sensitive and confidential data. The purpose of enterprise IRM is to prevent unauthorized access, resharing, and redistribution of this digital data.

Pain Point Example

A remote employee downloads a sensitive document from one of your clouds to his mobile device and emails it to an external collaborator. Without proper data protection tools in the cloud, you have no way to restrict your remote workforce from downloading intellectual property and sharing it offline.

Cost Impact if Unresolved

In the event of data disclosure to an unauthorized party, this may cause financial loss, reputational and brand damage, compliance penalties, and more.

CASB Solution and Benefits

Lookout's comprehensive data security portfolio includes native IRM which secures offline data access. CASB IRM defines policies to apply centralized data protection and encryption controls on the data that gets downloaded from the cloud applications to users' devices, including defining what devices should be allowed to access the data (for example, users cannot use personal devices to access sensitive data). In the event that downloaded data needs to be protected from the misuse (from, for example, a former employee taking customer data to their new employer), administrators have the ability to retract access to the data, even if it was downloaded and copied to another device. Real-time key revocation can protect data on even lost and stolen devices. Lookout CASB is also integrated with major third-party IRM packages such as Microsoft's.

USE CASE 7

Ensure data protection in case of a breach

Pain Point

Many cloud service providers support basic data protection capabilities, limited to the application level, and fail to control and encrypt sensitive data at a granular level. Moreover, these cloud providers require copies of your data encryption keys. Unfortunately, these security limitations open 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.

Pain Point Example

Many data privacy laws require that your business must protect and pseudonymize data to be compliant. When you scanned your clouds as a compliance check, you realized that most of the content is in plain-text form. The few cloud services that do encrypt data only encrypt it at rest in the database. On top of that, a malicious insider releases copies of the cloud data encryption keys hosted on one of your SaaS clouds to a third party for financial gain.

Cost Impact if Unresolved

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

CASB Solution and Benefits. Lookout provides Zero Trust encryption that protects data no matter where it is – "at rest," in network transit, in the cloud application layers (API, middleware, memory), and in use. Lookout FIPS 140-2 certified data protection capabilities meets all global compliance regulations and provides the highest levels of cyber threat protection, preventing the most complex threats and attacks such as API-based attacks which target encrypted data. Furthermore, the data encryption keys are retained only by you, and are never shared with the cloud provider.

Lookout Tokenization solution caters to countries or regions with strict data residency laws specifying that certain types of sensitive data cannot leave national boundaries, even if encrypt-ed. Lookoput's cloud tokenization replaces sensitive fields with randomly generated tokens that are structurally similar but have no mathematical correlation to the original data, allowing organizations to seamlessly use cloud applications while retaining the data sensitivity on-premise.

"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. CipherCloud CASB+ Zero Trust encryption ensures you never have to do this."

Pravin Kothari,
Co-Founder and CEO, Lookout

USE CASE 8

Real-time management of mobile devices with endpoint security controls

Pain Point

Mobile devices may be stolen, "jailbroken," or in some other way deemed non-compliant. Jail-breaking 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.

Pain Point 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

In the event of data disclosure to an unauthorized party, this may cause financial loss, reputa-tional and brand damage, compliance penalties, and more.

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.

USE CASE 9

Maintain configuration integrity of IaaS and SaaS clouds

Pain Point

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. This needs to be secured to meet security and compliance requirements.

Pain Point Example

With remote working being the new norm, the security and operations team need to turn on multiple security controls to have 360-degree control and visibility over data and remote users. A slight human error or security oversight might result in a massive data breach for the organiza-tion. There are many examples of misconfigurations resulting in data exposure and unauthorized access to cloud data. 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.

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.

CASB Solution and Benefits

ookout's Cloud Security Posture Management (CSPM) performs an automated assess-ment of your cloud landscape against well-defined security and compliance guidelines, and provides a comprehensive view of your cloud risk posture through intuitive and drill-down dashboards. Lookout CSPM brings continuous oversight and real-time guardrails to protect critical administrative and configuration controls in your SaaS and IaaS clouds, such as, Office 365, Amazon AWS, Microsoft Azure and Google Cloud Platform. CSPM reduces the operational complexity through a centralized security solution for all cloud services and infrastructure, prevents data loss due to misconfigurations, and ensures the latest compliance guidelines – GDPR, CCPA, HIPAA, PCI, are adhered to in a multi-cloud infrastructure.

USE CASE 10

Integration with existing enterprise security infrastructure

Pain Point

Many organizations have made large investments in deploying enterprise security solutions, such as, Enterprise DLPs, SIEMs, SSOs, AVAMs, etc. Organizations would want to protect these investments not only from an ROI perspective, but also because of the time invested in training their workforce to learn the craft, build the security infrastructure and create policies and remediation workflows to meet the business needs.

Pain Point Example

An organization has invested heavily in an on-premise DLP solution, which offers comprehensive security capabilities to inspect and act upon endpoint traffic. While they adopted a cloud security solution to protect their assets in the cloud, they wouldn't want to lose out on the features offered by their existing DLP solution, even though the cloud security solution also offers a built-in DLP support.

Cost Impact if Unresolved

Lack of integration with on-premise enterprise security solutions may lead to multiple siloed deployments to protect enterprise assets, complicating the network infrastructure and management. This may also increase the chances of security oversight and data breaches.

CASB+ Solution and Benefits

The Lookout CASB platform allows you to integrate with existing enterprise security solutions to optimize existing investments including EDLP, SSO, and Antivirus/Antimalware solutions, to name a few. Customers can also integrate with existing SIEM solutions as well as consume data from enterprise firewalls and proxies to provide additional visibility on all clouds in use, including non-approved SaaS applications (Shadow IT).

CASB integrates with External DLP solutions such as Symantec DLP, enabling organizations to maintain existing enterprise-specific DLP policies, extending them to data being uploaded to SaaS and cloud services. With this solution, organizations can maintain policy details specific to their environments while benefiting from the encryption and policy enforcement offered by Lookout.

CASB integration with Single Sign-On (SSO) services such as Okta, provides the ability to create and apply access policies to login actions. This ability enables more fine-grained access control over login activities over SaaS and IaaS applications.

CASB Antivirus/Antimalware (AVAM) includes Bitdefender antivirus support to enhance the detection of many types of malware such as zero-day threats, viruses, spyware, ransomware, worms, and bots.

CASB 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. CASB leverages Azure Information Protection (AIP) for DRM, document classification, extending AIP to any document in any cloud, including exported reports containing sensitive information.

CASB+ Brings Fast Time to Value

Agentless Architecture for Faster Deployments

CASB supports reverse-proxy based deployment (CASB Mobile Connect), providing secure agentless connectivity for mobile and unmanaged devices. This ensures quick, frictionless deployment, delivering full CASB functionality without any resource inten-sive installation of agents and expensive upkeep.

Support For All of Your Clouds

CASB supports many popular SaaS-based business applications, including Office 365, Slack, Salesforce, Amazon Web Services, SAP SuccessFactors, ServiceNow, Adobe, Box, Dropbox, and many others. CASB provides data protection to application content while preserving application functions and ensuring compliance beyond the SaaS and IaaS application provider's offering. This gives you one consistent approach and front-end interface to protect your data and help enforce compliance across all of your cloud environments.

Support For Custom Applications

Lookout CASB AnyApp connector allows customers to integrate the powerful data protection capabilities for their own custom cloud-based applications. With AnyApp, customers can bring the benefits of encryption, tokenization, dynamic access control, DRM, UEBA, threat prevention, and many other security features to their custom cloud-based applications. This ensures protection of custom enterprise applications, regardless of the chosen cloud platform.

The Largest Multinationals in the World Use Lookout CASB

- 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

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.