

WHITEPAPER

Lookout CASB

Platform Overview

Table of Contents

Remote workforce driving cloud adoption	3
Challenges introduced by the growing cloud footprint	3
Why is CASB essential for cloud and enterprise security?	5
Lookout CASB Overview	6
CASB Deployment Modes	
Lookout Policy Engine	
CASB Continuous Protection Model	8
Deep Visibility & Intelligence	8
Threat Prevention	10
Data Protection	13
Governance and Compliance	16
Lookout Integration Ecosystem	18
Secure Access Service Edge (SASE)	18
Zero Trust Network Access (ZTNA)	19
Intelligence-led Threat Protection	19
Identity and Access Management	20
External DLP Integration	20
Data Classification Integration	20
SIEM Integration	20
MDM Integration	20
Lookout Differentiation	21
Rich legacy in cloud data protection	21
Support for the widest range of clouds (SaaS, PaaS, IaaS)	21
Agentless CASB solution, accelerating deployments	21
Single vendor for SaaS governance and email security	21
Unified Policy Enforcement for all Clouds	21
Advanced DLP Engine	21
Advanced UEBA with detailed entity and incident analysis	22
Endpoint security controls to manage BYO devices	22
DRM built for remote collaboration	22
End-to-end data protection: field-level encryption and file-level DRM	23
Deep Application Intelligence	23
About Lookout	23



Section 1. Introduction

Remote workforce growth is increasing cloud adoption

Given the unique backdrop of the global pandemic, the pace of cloud applications adoption has accelerated significantly, driven in large part by unprecedented expansion of the remote workforce. While researchers with Chubb estimate that the number of people working remotely has grown by nearly 400% over the last decade, the COVID-19 outbreak has pushed unprecedented numbers of workers outside the confines of the traditional office. For example, pollsters Gallup have reported that as many as 70% of North American office workers have shifted to some measure of remote working in 2020 to account for the ongoing pandemic.

As a result, popular cloud apps including Office 365, G Suite, Slack, Box, and Salesforce, among others, have established an even greater presence as enablers of critical communications and collaboration to support business continuity. This development has amplified an already tectonic shift in the manner that sensitive data is being stored, accessed and handled as organizations dramatically increase their dependence on the cloud.

Security challenges introduced by the growing cloud footprint

The tremendous benefits generated by the widespread adoption of cloud applications have arrived with their own set of unique security and data protection implications. While cloud apps offer unprecedented flexibility and availability to support changing business requirements, the distributed nature of cloud infrastructure, and in particular the elimination of traditional IT network and security perimeters have created a wide range of challenges.

With the surge in active users converging from distributed and unsupervised work environments, exchanging huge volumes of data with both internal employees and external partners through cloud apps, it has therefore become hugely important to strengthen related defenses. From monitoring capabilities that serve to identify and protect sensitive information as it is transmitted across multiple cloud apps, to enforcement functions that prevent data from falling into the wrong hands, along with necessary compliance controls, today's practitioners require advanced cloud and data security protection in the form of dedicated software solutions.

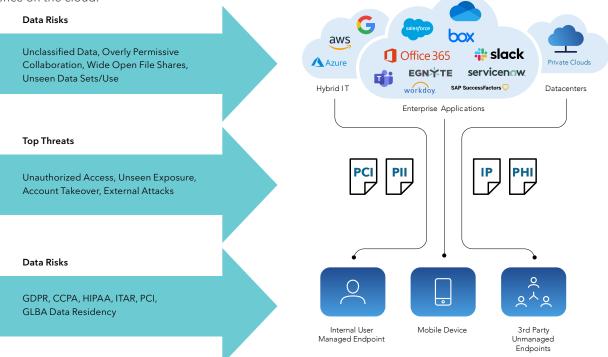


Fig. Challenges introduced by the cloud environment



The "Top Threats to Cloud Computing: The Egregious Eleven" report issued by the Cloud Security Alliance (CSA) further details this growing requirement for staunch cloud security protections. While basic cloud security requirements are now being aptly addressed, the report cites that organizations continue to grapple with "emerging issues that are harder to address as infrastructure becomes more secure and attackers more sophisticated."

The report further contends that organizations should increase their focus on issues of insider threats, identity and data security, along with cloud misconfigurations, to protect their 'crown jewels' in the cloud.

To that end, many of today's organizations seek to emulate industry best practices by applying a so-called "zero trust" approach to securing cloud information, services and access – invoking layered defenses to prevent against potential threats and data exposure. Key to achieving this approach centered on the belief that organizations should not automatically trust anything inside or outside their perimeters, specifically as related to the cloud, practitioners must prepare to answer pertinent questions including.

- How do I gain 360-degree visibility into cloud user activity, including file uploads and information sharing?
- How do I detect suspicious user behavior and prevent data loss due to compromised accounts or insider threats?
- How do I detect and protect sensitive information such as PII, PCI, and PHI data as it travels across cloud apps?
- How do I differentiate managed and unmanaged devices to enable secure data access and collaboration?
- How do I ensure compliance with the latest data protection laws such as GDPR, CCPA, and HIPPA?

CSA Top Threats Report: The Egregious Eleven ranked in order of significance

- 1. Data breaches
- 2. Misconfiguration and inadequate change control
- 3. Lack of cloud security architecture and strategy
- Insufficient identity, credential, access and key management
- 5. Account hijacking
- 6. Insider threat
- 7. Insecure interfaces and APIs
- 8. Weak control plane
- 9. Metastructure and applistructure failures
- 10. Limited could usage visibility
- 11. Abuse and nefarious use of cloud services

¹ Source: The CSA "Egregious Eleven" cloud security risks



Why is CASB essential for cloud and enterprise security?

The broad scope of cloud and data security challenges driven by increased cloud adoption and rapid expansion of the worldwide remote workforce demand an inclusive approach to security - one that incorporates foundational requirements and offers fine-grain visibility and control, all while paving a path toward long term maturity. From baseline identification and awareness of cloud usage, to integrated data protection and rights management, to threat prevention and protection against misconfiguration errors, practitioners need a solution that addresses the widest array of capabilities in a centralized and integrated fashion.

Cloud Access Security Broker (CASB) solutions represent this specific manner of platform, sitting between enterprise networks and the cloud to offer complete visibility and control over cloud applications utilization. By directly addressing core requirements related to protection of data in the cloud – both at rest or in motion – while enabling enforcement of contextual, data protection policies to secure sensitive information from external or internal threats, CASBs have become established as state of the art in acquitting the needs of today's organizations.

Unlike Secure Web Gateways (SWG), Web Application Firewalls (WAF), Virtual Private Networks (VPNs) and Enterprise Firewalls – tools that focus on securing the individual elements of the internal perimeter – CASBs offer highly differentiated, cloud-specific security capabilities designed to protect sensitive data as it moves outside the enterprise premises and into SaaS, laaS and PaaS environments. Embracing the CASB approach allows organizations to seamlessly scale their cloud operations to thousands of remote users, while enforcing strong policies to protect data, maintain data privacy and regulatory compliance requirements.

Unique benefits offered by CASB solutions include:

- **Detailed Visibility:** Granular visibility and control across cloud apps, users, data, devices and user activity to identify cloud usage, cloud data repositories, risky clouds and users and unsanctioned cloud utilization.
- Advanced Data Protection: Powerful data protection controls to identify, classify and secure sensitive cloud data, along with integrated data encryption, masking, redaction, removal, and prevention of external users or domains from accessing shared folders.
- Integrated Threat Protection: Antivirus & anti-malware integration for deep scanning of all incoming and outgoing traffic for malicious content or infected files, along with User and Entity Behavior Analytics (UEBA) to identify anomalous user behavior in real-time and prevents potential data breaches related to bad actors and internal threats.
- Validated Compliance: Centralized compliance with data protection laws (GDPR, HIPAA, CCPA, GLBA, SOX and more) with data privacy and localization requirements.
- Posture Management: Cloud Security Posture
 Management (CSPM) and SaaS Security Posture
 Management (SSPM) automates identification and
 remediation of cloud implementation to prevent breaches
 due to misconfiguration and user errors.



Section 2. Lookout CASB

Overview

Lookout CASB is a cloud native CASB platform that provides the deepest levels of integrated cloud security and data protection available, offering an immediate solution to organizations' most challenging security and compliance requirements. Lookout recognized data security expertise forms the foundation for the industry's leading Zero-Trust CASB solution, providing seamless security across all clouds and applications with unified policies, trusted data security, and validated standards compliance.

While many CASB solutions only address data as it is being shared to the cloud – with limited visibility into information already resident in cloud applications – Lookout CASB offers deep visibility, powerful end-to-end data protection, adaptive access control, advanced threat protection, automated posture management, and centralized compliance and governance for enterprises embracing cloud applications. CASB empowers organizations to address the full breadth of their cloud security challenges through a single platform while ensuring that confidential data is always protected.

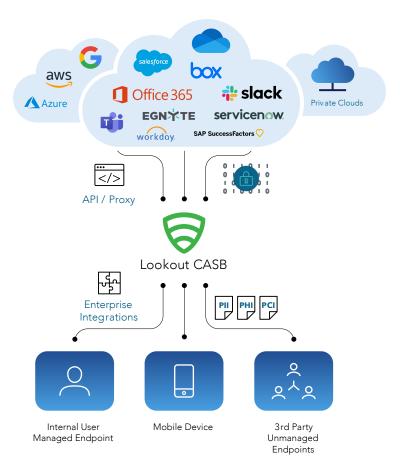


Fig. Lookout CASB Overview

The centralized data protection policies executed through Lookout CASB further monitor, detect, classify and remediate sensitive data exposures across cloud apps, collaboration platforms and emails and enforce automated remediation actions including data masking, redaction and deletion, along with quarantine and privilege limitation. This allows organizations to keep pace with the evolving scope of their unique requirements and securely collaborate in a multi-cloud environment, without the operational complexity of managing security policies across individual SaaS, PaaS and laaS accounts.



CASB Deployment Modes

CASBs can be deployed in multiple modes – inline and API. While most of the CASB solutions support one of the deployment modes, Lookout CASB works in all the modes, offering maximum use case coverage, and visibility and control over all users, all devices, and all cloud services. The primary deployment modes of CASB include:

API-based: In API mode, CASB acts as an out-of-band solution without sitting in the direct path between the enterprise users and cloud applications. CASB in API mode provides deep data visibility and enforces data protection policies via an API trigger "after" the data gets uploaded to the cloud. Since the operation is asynchronous, there is no performance impact or any latency in user experience. API mode provides coverage across both managed and unmanaged devices, with data protection using DLP, data discovery, classification, posture management, audit trails, user activity monitoring, content inspection, scanning user privileges, sharing permission on files, folders, and app security settings.

Proxy-based: In proxy mode, CASB sits between the enterprises and cloud applications, controlling data flow through a single gateway in "real-time". This ensures the data always goes to the cloud in a protected form. Proxy-based deployments can be enabled via models including:

- Forward proxy: CASB in forward proxy mode routes all traffic from endpoint to the CASB instance. CASB can either work with existing proxy services that can forward traffic to CASB proxy, or an agent software needs to be installed on managed devices to forward traffic to CASB.
- Reverse proxy: CASB in reverse proxy mode provides secure agentless connectivity for all devices, including mobile and unmanaged devices. It works by simply redirecting all traffic through the CASB to the service provider. This can be done by integrating either with existing IDaaS solutions such as Azure AD, Okta, Ping etc. SSO or with the Lookout Secure Cloud Workspace to securely redirect traffic through CASB.

Lookout Policy Engine

The Lookout CASB Policy Engine allows administrators to enforce centralized data protection policies while enabling a consistent approach towards securing assets in a multi-cloud environment. The flexible Policy Engine supports definition of highly customized policies to support the widest range of scenarios using an array of options across multiple attributes, including:

- **Subject:** user, user group, domain, device status, operating system, user risk, etc.
- **Object:** DLP, data classification, OCR, malware, watermark, structured or unstructured data, etc.
- Environment: location, IP address, IP risk score, sharing type, browser type, etc.
- Function: upload, download, share, delete, edit, update, export, import, etc.
- Decision/Action: allow & log, notify, deny, user coaching, step-up auth, redact, watermark, permanent delete, remove collaboration etc.

For example, this might involve defining a policy to scan and classify files with sensitive content, uploaded by a particular user, and watermarking those assets before they are finally uploaded into the cloud.

New enhancements to the CASB Policy Engine include:

- Content Rule Template(CRT): Unifying content scanning, identification and classification within a single policy framework. This includes DLP rule templates, document rule templates, predefined and custom DLP libraries, applying file metadata, classification and watermark rules on top of DLP rules.
- Content Digital Rights (CDR): Unifying all content actions within a single policy framework. This includes watermark, classification, token obscurity, encryption.



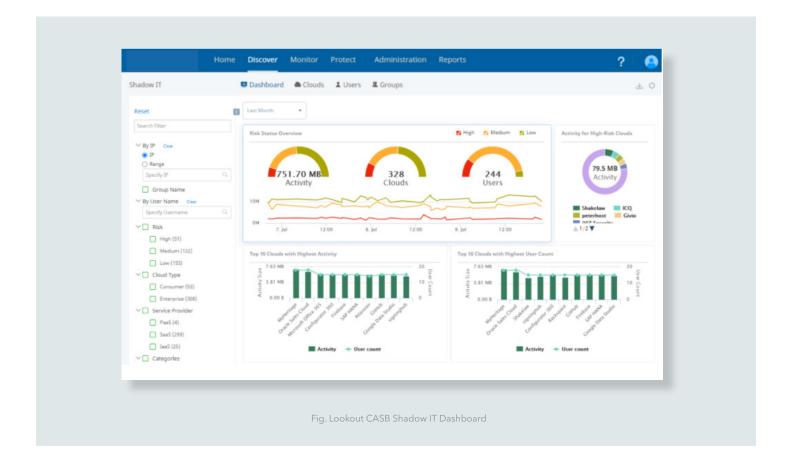
Section 3. Lookout CASB Continuous Protection Model

Deep Visibility and Intelligence

Cloud Monitoring

Getting full visibility of all cloud applications running in your organization is the first step in improving overall cloud security standing. Lookout CASB integrates with existing security logs from network devices, firewalls, proxy services, and delivers complete visibility into your organization's cloud usage by discovering shadow IT resources, along with enabling deep intelligence into user behavior and applications usage.

With over 20,000 clouds profiled in its onboard knowledge base, CASB provides an assessment on the risk of each cloud service being used, based on over 60 attributes per cloud. The deep visibility captured in activity logs and detailed CIO/CISO reports help support data protection and compliance reporting, auditing, and forensic investigation, while enabling IT and Security Operations teams to take immediate steps to reduce data loss and exposure from risky clouds.





Insights Investigate

With the increasing adoption of cloud, in particular to enable the remote workforce, InfoSec and SOC teams demand deeper intelligence into their sanctioned cloud environments to analyze use and abuse, run forensics, and respond to potential threats.

Lookout's Insights Investigate feature provides a rich set of tools for incident management, enabling administrators to analyze all activities occurring in the cloud, view incidents that involve policy violations, assign a level of severity to each incident, and specify necessary remediation. This feature also allows admins to capture crucial details on each incident source.

Insights Investigate consists of the following components:

 Incident Management: lists all the policy violated incidents occurring in the organization, enabling the administrator to filter each list based on time period (day, date, hour), cloud (managed or unmanaged), severity (low, medium, high) or status (open, under investigation, resolved).

- Incident Insights: presents a graphical view of different types of incidents along with count of incidents occurred for each incident type. Violation types include login, DLP, DRM, and external sharing violations, malware, geo anomalies, and location anomalies. With Incident Insights admins can drill down to the bottom of an incident by defining queries based on time intervals and entity type (user, device, location, application). For example, generating the list of incidents arising from an employee John Doe's account on Office 365 cloud in the past one month.
- Entity Insights: presents a graphical organization-level view of the count of incidents by their source, including user, device, location, application, content, and external user. For example, generating the list of users, devices, applications, content and external users accessed from New York in the last month.

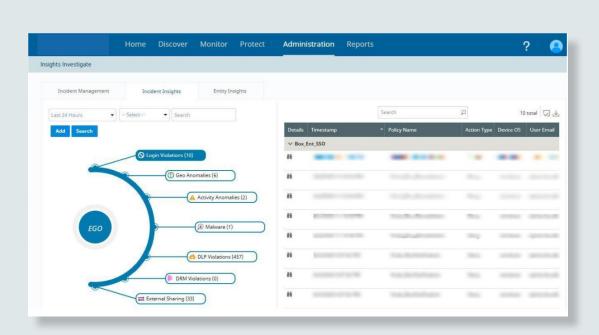


Fig. Incidents Response and Insights



Threat Prevention

Zero Day virus/malware protection, Sandboxing

The cloud introduces many new threat and malware prevention challenges, including attacks that are shared between clouds and often bypass conventional network antivirus systems. Viruses, shared by users as attachments or links, can propagate rapidly through the clouds and cause damage on a large scale. As enterprises expand their cloud use, they must ensure that this platform does not become a channel for malware delivery to their users or internal networks.

Lookout uniquely addresses the growing wave of threats facing today's cloud-based remote workforce by aggregating and correlating threats from the enterprise network, cloud, SaaS and mobile environments, and offering complete visibility into these risks in SaaS environments. Lookout's zero-day threat protection provides integrated malware detection designed for the cloud with industry-leading detection rates. Lookout CASB antivirus anti-malware (AVAM) solution defines policies to scan all inbound and outbound cloud content for malicious code and cleans or quarantines infected content on the fly, without adding any noticeable latency. Sandbox integration allows CASB to create an isolated test environment for executing suspicious files or URLs and discover zero day threats.

Lookout CASB can also be integrated with the FireEye Detection On Demand and Juniper ATP platforms to extend enterprise threat detection to the cloud and gain full visibility into alerts, activities and threats in the cloud, enterprise and remote workforce environments

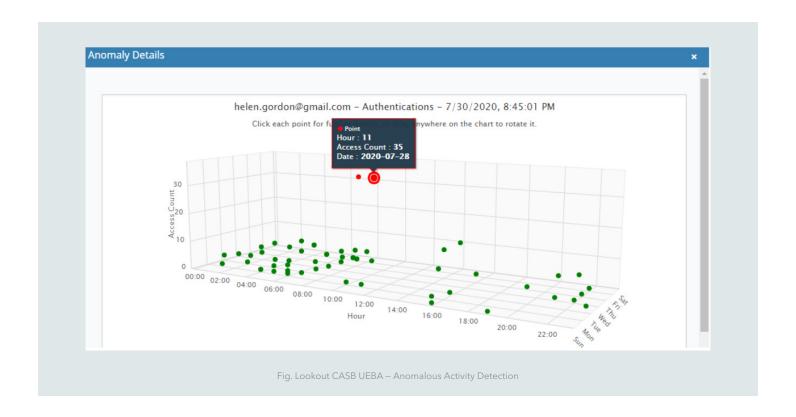
User Anomaly Detection with UEBA

Data leaks and losses from compromised accounts and insider threats is one of the biggest pain points facing today's organizations. Lookout's User and Entity Behavior Analytics (UEBA) engine performs continuous monitoring of users, devices and application activities, to detect anomalous behavior across multiple sanctioned cloud apps and prevent accounts from getting compromised by malicious insiders and external threats.

Lookout UEBA utilizes machine learning algorithms to model the behavior of users and devices on cloud apps, detects deviations from normal behavior patterns, and highlights anomalies that could be the sign of a cyberattack. Examples of anomalies might be an abnormally large number of downloads from an individual user, a higher than normal number of logins from the same user, or persistent login attempts by an unauthorized user. CASB UEBA monitors user and entity activities on real-time dashboards for point and click incident analysis. Monitoring includes the locations from where logins take place (geo-logins), source IP addresses, and devices used. User behavior includes activities such as content uploads and downloads, edits, deletes, logins, and logouts.

UEBA profiles a rich set of attributes for every activity to detect user anomaly and generate detailed reports. The attributes include user ids, emails, groups, location, device information, activity, content ids, names, folders, objects, data destination location, app context, sharing types, sharing targets, email recipients, collaborators, etc.





Zero-Trust Adaptive Access Control, with step-up authentication

As cloud-based collaboration and file sharing rapidly grow, you need assurance that access to critical information across multiple SaaS applications is allowed to users with valid and proven identities. Lookout Adaptive Access Control performs a continuous risk assessment of users, devices, apps and locations, delivering zero-trust user access security from any device or location, to all trusted cloud applications, and protecting against data loss and threats in SaaS apps and emails from unauthorized users or devices.

Lookout AAC defines policies to allow cloud and data access based upon the user context – location, user group, IP Address, device type, etc., with automated remediation on detection of policy violation. Remediation may include user blocking, user coaching.

Lookout Adaptive Access Control policies allow classification of endpoint devices into managed and unmanaged, enabling selective access to cloud resources from personal, BYO devices, for example browser-based read-only access. Security at the gate can be increased for unmanaged devices through a step up authentication process.



Securing access from personal, BYOD device

There has been a recent surge in the usage of personal devices in the workplace. These devices lack the security settings on company-issued hardware, and employees more often ignore the security best practices while connecting to the sanctioned cloud apps for collaboration. The lack of visibility and control over personal device activity can lead to unauthorized cloud access, data leaks, and accidental disclosure of sensitive information.

Lookout CASB enables context-aware management of devices connecting to the cloud from any remote location and triggers corrective actions, such as blocking the access, on detection of a policy violation. Lookout's endpoint security controls include:

- Device classification into managed or unmanaged through the installation of digital certificates on the connecting devices.
- Zero Trust access through integration with SSO solutions to authenticate user identity during login.
- Integration with MDM/EMM solutions to fetch the endpoint device status and use that intelligence to define security policies and enforce corrective actions.
- Limit the cloud data access based on device type (managed/unmanaged) through Adaptive Access Controls.

Zero Trust access with IDaaS integration

Authenticating the user identities who are accessing the most sensitive data and applying strong data controls to prevent data loss are the two most important aspects of cybersecurity. A Zero Trust security solution must satisfy the following criteria:

- Trust but verify the user identity and monitor their behavior throughout the journey
- Provide a highly secured but low friction user experience
- Deliver advanced security controls to user identity, gain full visibility of cloud app usage, apply granular policy controls, and automatically remediate risks.

Lookout CASB in reverse-proxy mode combines with IDaaS solutions, such as Okta, Ping and Thales, to deliver end-to-end user and data security from any device, any location, to all trusted cloud applications, providing organizations a first step to achieve Zero Trust Cloud Security. This allows organizations to define and enforce device and context-aware access policies, provide a safe and convenient single sign-on solution to reduce user friction, and enable fine-grained access control over login activities over SaaS and laaS applications.

Lookout in conjunction with IDaaS solutions protects against unauthorized access and continuously monitors user activity in the cloud apps to identify and mitigate threats, as detailed below:

Step 1: Verify the user - Control Access at the door with SSO and MFA.

Step 2: Apply context-based policy to enable access to cloud resources. Context may include user type, location, time of the day.

Step 3: Continuous user behavior monitoring with remediation such as step-up authentication, risk mitigation, or session termination based on user risk level.



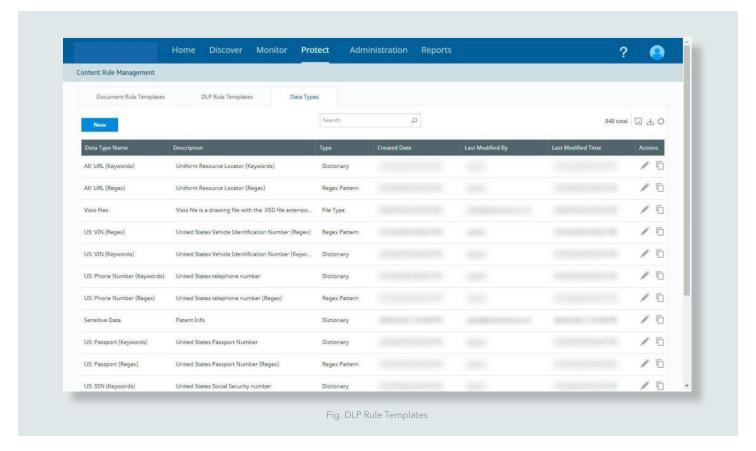
Data Protection

DLP and Classification

Lookout CASB delivers integrated Data Loss Prevention (DLP) that extends the enterprise data security controls to the cloud and defines centralized policies to monitor, classify and protect sensitive data across cloud apps and emails - while in motion or at rest. CASB DLP brings consistency in managing data across multiple SaaS apps, emails and custom cloud deployments, and ensures the security of sensitive information through extensive data protection options that go beyond basic allow/deny capabilities. These options include controlling real-time collaboration, allow & log, notify, deny, removing public links and external collaborators, enabling step-up authentication, applying data classification labels, encrypting files to protect data during downloads, setting up user coaching, document highlighting, redacting, watermarking, permanent delete, user remediation.

Key Lookout CASB DLP Differentiators include:

- Multi-mode data inspection API, Proxy and Email modes, for securing historical data and real-time cloud collaboration
- Context-aware policy enforcement: upload, download, share, collaborate
- Predefined and customized policy templates to address multiple global regulations - PCI, HIPAA, GDPR, GLBA, CCPA etc.
- Advanced file and image scanning OCR, Fingerprinting, EDM
- Integration with enterprise DLP systems to extend corporate policies to cloud apps



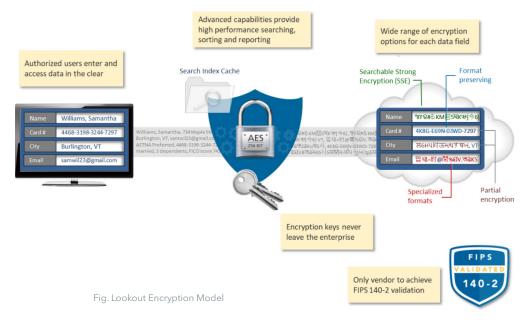


End-to-end Encryption

First-generation CASB solutions offering basic data protection with no or "at rest" encryption capability are no longer enough to protect your assets hosted in the cloud, beyond the enterprise perimeter and out of direct control. Attackers have successfully breached the cloud APIs that have enabled them to compromise even encrypted cloud data.

CASB brings a comprehensive FIPS 140-2 validated encryption solution that applies a Zero Trust approach to cloud security and protects data no matter where it is – "at

rest," in network transit, in the cloud application layers (API, middleware, memory), and in use. Lookout's central premise is that data protection should be granular and policy-based to cover every scenario. This means that security policies must travel with the data and maintain exclusive control over access and handling, regardless of where it resides in the cloud. This enables enterprises to safely adopt a multi cloud strategy, ensuring that confidential and sensitive data is protected across all locations – in the cloud, on managed user devices, and unmanaged remote endpoints.



Lookout Key Management allows customers to either use the cloud provider keys or bring their own keys to encrypt the data. The data encryption keys are retained by the customers, and are never shared with the cloud service providers, ensuring the cloud providers retain no control over the protected data.

Lookout's end-to-end data encryption solution includes:

- Granular policy controls to selectively encrypt any type of data
- Field and file level encryption for SaaS and IaaS applications
 - Field-level support for Salesforce, ServiceNow, SAP SuccessFactors

- FIPS 140-2 validated Searchable Strong Encryption (SSE) solution - first in the cloud visibility and data protection industry
- Encryption at rest, in-flight, and in-use while still preserving the cloud functionality (searching, sorting, reporting)
- Secure offline data access with native rights management solution
- Email data protection that includes sensitive content masking from subject and body, data rights management, and attachments encryption
- 100% user key control for total security



End-to-end Encryption

Lookout's native Data Rights Management (DRM) enforces data protection controls on sensitive data in the cloud, enabling secure collaboration and offline data sharing with automatic encryption of sensitive data, reports, and emails during downloads. Sensitive data downloads is permissible only on managed devices, and only the authorized users would be able to decrypt the downloaded files using Lookout's lightweight DRM client.

Lookout DRM provides full visibility into the data accessed and downloaded by internal and external users, including customers, vendors, and partners, allowing admins to remotely shred the content on detection of policy violation.

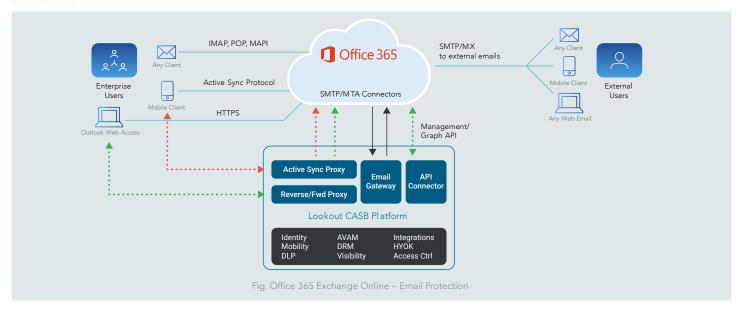
Admins can also revoke the keys in real-time to protect data on lost or stolen devices. This allows organizations full ownership and control over data, regardless of where it is being shared.

Apart from providing full-blown native DRM capabilities, CASB also integrates with major third-party DRM packages such as Microsoft's

Secure Email Gateway

Lookout offers the industry's first Secure Email Gateway in a CASB, enabling deep visibility into corporate email usage with unprecedented audit capabilities, and acting as a single CASB solution for SaaS governance and email security. This unique functionality allows customers to extend existing DLP policies to Office 365 and G Suite email services (Microsoft Outlook, Exchange Online and Gmail), without adding another product, management console, or new policies, preventing data loss from cloud-based corporate emails.

Lookout CASB routes all emails from any client device, managed or unmanaged, through a 'Secure Email Gateway' for advanced DLP scanning of email subject line, body and attachments and protects sensitive content in the email before it gets delivered to the recipients. The Secure Email Gateway is platform agnostic and integrates directly with your preferred email solution across access points – web app, thick apps or email clients.



Following are the feature highlights of Lookout's Secure Email Gateway:

- Centralized view for emails, collaboration apps, and infrastructure
- Prebuilt DLP templates to ensure compliance of sensitive data on email
- Automated policy enforcement to mask sensitive content in email subject line and body, and encrypt sensitive file attachments
- Removal of external recipients on-the-fly from the mailing list before sending out emails



Advanced capabilities - OCR

CASB DLP Optical Character Recognition (OCR) enables the detection of sensitive content in image files uploaded across emails and collaboration apps, preventing screen capture sharing and other unsanctioned handling and delivering the industry's most inclusive approach to cloud DLP enforcement. For example, applying data protection controls on a photo, a screen shot, or other image file (.png, .jpg, .gif, and so on) that shows a credit card number, social security number, employee ID, or other sensitive information. OCR protection can also be applied to policies for files that include images; for example, a PDF or a Microsoft Word file that includes one or more images within the file.

Governance & Compliance

Support for global data protection laws

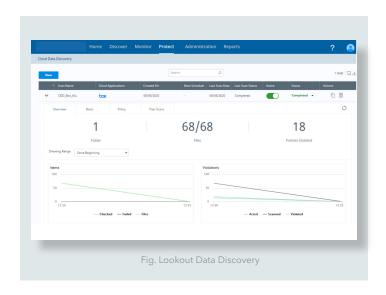
Lookout CASB enables zero-trust protection across all your SaaS and IaaS apps and provides comprehensive compliance capabilities that go beyond a regular cloud service provider offering. The predefined DLP templates defined by CASB allows organizations to migrate to the cloud in alignment with complex data privacy and protection regulations across the globe such as GDPR, CCPA, HIPAA, PCI, GLBA, SOX, and many more.

The Lookout encryption and key management architecture allows cloud applications to selectively encrypt the data for each required country and thus meet local data privacy requirements. As the encryption keys are exclusively retained by the customers and not shared externally with cloud service providers, Lookout CASB not only secures the sensitive data in case of a breach, but also provides "Safe Harbor" exemptions to the breach notification laws, which recognize that if your data is adequately encrypted or "rendered unintelligible" and no third-party has access to the encryption keys then there are Safe Harbor exemptions from notification, and legal liability.

Cloud Data Discovery

Lookout Data Discovery performs historical scanning of existing data across multiple popular SaaS clouds through an API integration and provides deep insights into data resident in multiple cloud applications for years. With Data Discovery, organizations can perform a comprehensive audit of the data resident in the cloud to identify and classify sensitive information related to PII, PHI, PCI, HIPAA and many more, and enforce remediation to preserve data integrity and compliance.

Lookout performs a deep assessment of data in the clouds with out-of-the-box DLP templates to identify security blind spots, detect open shares and address many global regulations – PCI, HIPAA, GDPR, GLBA, etc.



The data scanning can be periodic or ad-hoc, and encompass field-level information in structured clouds, such as ServiceNow and Salesforce, and unstructured data, files in collaboration apps, such as Office 365, Google Drive, Slack and Box.

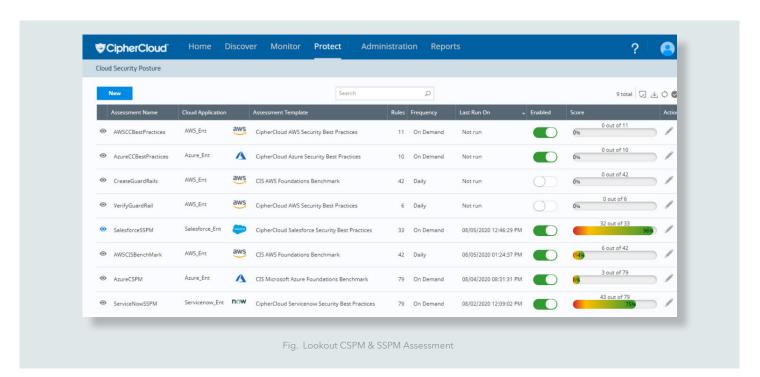
Intuitive Cloud Data Discovery dashboards provide drill-down details on the historical file scans, along with the number of existing violations. Post this discovery, the admin can take action to remove the files or limit their exposure.



CSPM & SSPM

With the growing cloud popularity and adoption, organizations migrating their business critical applications to the cloud are overlooking a simple cloud security question – how do I automate the security posture across multiple SaaS and IaaS clouds such as Office 365, Box, Salesforce, AWS, and Azure and drastically reduces the risk of data loss due to configuration error or human oversight?

Lookout Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) perform an automated assessment of your cloud landscape against well-defined security and compliance guidelines, and provide a comprehensive view of your cloud risk posture through intuitive and drill-down dashboards. CSPM and SSPM provide a centralized dashboard to reduce your operational complexity in managing multiple cloud applications, prevent data loss due to misconfigurations, and the latest compliance guidelines – GDPR, CCPA, HIPAA, PCI, are adhered to in a multi-cloud infrastructure.



Lookout CSPM benefits include:

- Discovering cloud assets in laaS clouds
- Gaining deep visibility into usage and security events
- Getting alerts and notification to stay on top of events
- Securing Open Buckets (S3), laaS, SaaS configurations
- 30+ page detailed CIO/CISO report for audits



Section 4. Lookout Integration Ecosystem

Secure Access Service Edge (SASE)

In today's 'new norm' of remote working and the continued adoption of SaaS apps, large volumes of sensitive data is moving across datacenters, cloud services and end user devices. Organizations demand immediate, uninterrupted, yet secure access to the data for business continuity. Traditional security solutions such as on-prem firewalls, SWG, WAFs, etc., fail to solve these emerging business challenges as they lead to the creation of siloed environments that are complicated to deploy and manage. Moreover, they don't focus on the biggest challenge – secure access to data from any user, using any device, from any location.

Lookout Secure Access Service Edge (SASE) is the future of cloud access architecture that focuses on solving the complexity of siloed security measures through the convergence of network and security point solutions into a unified, global cloud-native service. SASE is identity and context driven, relying on the identity of the entity at the source of the connection (user, device, branch office, IoT device, edge computing location) to provide access to cloud services, irrespective of the user location. The consolidation of networking, network security, and cloud security enables a 360-degree security solution that goes till the edge and follows the data back to the cloud.

Lookout industry-leading CASB and ZTNA capabilities integrated with Identity & Access Management (IAM), Enterprise Mobility Management (EMM), and Endpoint Detection and Response (EDR) – provide an extremely strong foundation for Secure Access Service Edge (SASE).

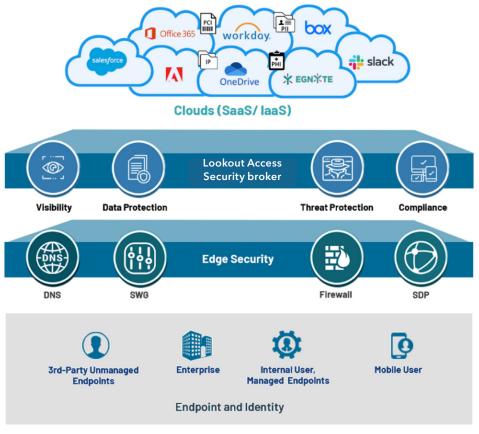


Fig. Lookout SASE Architecture



Zero Trust Network Access (ZTNA)

Lookout is partnering with the security industry's leading network security, identity, and threat protection providers to enable best-of-breed integrations and offer out-of-the-box Zero Trust Network Access (ZTNA) solutions.

Delivered by the Lookout CASB solution, our approach to ZTNA fully embraces the principle of "least privilege" to offer adaptive, identity-aware access to nearly any application hosted on-premises or in the cloud. This integrated strategy, combining the strengths of CASB and proven ZTNA solutions enables practitioners to dictate Zero Trust access across enterprise applications and data from any device and location – facilitating secure, flexible, and scalable remote workforce deployments.

Key elements of the Lookout ZTNA approach include:

- End-to-end Zero Trust security delivered via extension of CASB controls to private applications
- User identity-based access to specific applications, addressing overly permissive network access for authenticated users
- Full application cloaking, preventing exposure of internal applications to the Internet and reducing the risk of data exposure
- Agentless access to specific services (HTTP/S, SSH)

Intelligence-led Threat Protection

Lookout CASB is integrated with FireEye Detection On Demand and Helix platforms to deliver the industry's first real-time protection of zero-day threats across the enterprise, cloud, SaaS and mobile environments. The solution offers 360-degree visibility by aggregating and correlating threats from the enterprise networks, cloud and end user devices to uniquely address the new wave of cybersecurity threats facing today's remote workforce.

By combining FireEye Detection on Demand and Lookout CASB, this joint solution analyzes content in real-time across SaaS applications and cloud repositories. The combination is designed to deliver high fidelity results as to whether an object shared via SaaS and Cloud applications is malicious or not. Should evil be detected, the content is blocked by Lookout in real-time helping to protect employees, partners and customers.

Below is how the integration works:

- Lookout CASB enables visibility and protection of regulated data created or shared outside the enterprise perimeter
- Lookout CASB SaaS security for dozens of applications extended to FireEye Detection on Demand for intelligence-driven threat protection
- User activity, anomalies and malware events are normalized and sent to FireEye Helix advanced SEIM solution

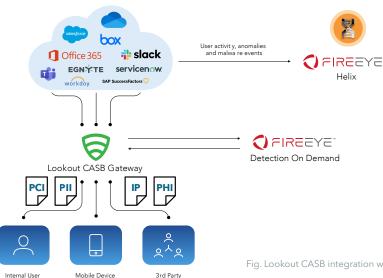


Fig. Lookout CASB integration with FireEye Detection On Demand



Identity and Access Management

Data breaches, insider threats, account hijacking – these are the most critical cloud security threats in the past few years. In today's remote workforce environment, protecting the user identity has never been more important. As users connect from any remote location and endpoint device to multiple cloud applications, how do you ensure continuous protection of your data, both from internal and external threats?

Lookout CASB integrates with IAM solutions – Okta, Ping and Thales, to create and apply access policies to login actions and enable Zero Trust access to cloud services. The strong identity controls of IAM solutions combine with the strong cloud security controls of Lookout CASB to provide more finegrained access control over login activities over SaaS and IaaS applications, and enable a 360-degree protection around your data and access, from user log in to log out.

External DLP Integration

Lookout CASB seamlessly integrates with external DLP engines, such as Symantec, to extend data protection capabilities and enable consistent policy enforcement from enterprise premises to the cloud. CASB offers organizations the flexibility to scan data through native DLP, external DLP, or augment data protection using a multi-level scan, where the data is pre scanned through native DLP and a final scan is performed by external DLP engine.

Data Classification Integration

Lookout CASB DLP extends data classification and governance to any document in any cloud, integrating with Microsoft's Azure Information Protection (AIP) and TITUS Classification. The CASB+ policy engine identifies and protects sensitive information to control user-cloud interactions, and can also apply enterprise standard classification on unclassified data. CASB+ provides full visibility into and protection across multiple apps, users and devices - securing intellectual property and other protected information from unintended data exposure.

SIEM Integration

SIEM tools allow the security teams in organizations to aggregate data from various sources (network devices, servers, firewalls) and analyze the data to detect threats and prevent potential breaches.

Lookout CASB integrates with multiple SIEM solutions including, HP ArcSight, IBM QRadar, Intel Security, LogRhythm and Splunk, extending the log collection from on-prem devices to the cloud to provide an in-depth analysis and control over the activities across the enterprise, cloud, SaaS and mobile environments. Through the integration, CASB pushes the logs to the SIEM system for centralized analysis and reporting of organization's security events.

MDM Integration

Lookout CASB integrates with MDM solutions, such as VMware Airwatch, via APIs. Installation of digital certificates on the end-user devices allows classifying them as managed or unmanaged while connecting to the cloud and use that intelligence in defining policies to access the cloud resources and enforce actions. For example, allowing read-only access via web browsers or stepping up the authentication for access through unmanaged devices.

For Office 365 users, the existing integration with Active Sync proxy can be leveraged to further enforce control based on the set access rights for the connecting device.



Section 5. Lookout Differentiation

Rich legacy in cloud data protection

Lookout has 10+ years of industry presence, securing the cloud information of the world's largest global enterprises in over 25 countries. Lookout has been recognized as a 'Visionary' in Gartner Magic Quadrant for CASB in 2018 and 2019, and our CASB platform has been rated highest for product capabilities in Gartner's Critical Capabilities report, 2019.

Support for the widest range of clouds (SaaS, PaaS, IaaS)

Lookout CASB delivers full CASB functionality - visibility, compliance, data protection, threat prevention, offering the greatest depth and breadth of product capabilities across the widest range of cloud apps. CASB offers centralized, granular controls with an extensive list of security controls to meet any mix of security, governance and compliance requirements across multiple clouds through a single pane of glass. Popular clouds supported include:

- Collaboration & Email: Office 365, G Suite, Slack, Box, Dropbox
- Enterprise apps: Salesforce, ServiceNow, SAP SuccessFactors, SAP C4C, Workday, Adobe Marketing Cloud
- laaS clouds: Amazon Web Services, Microsoft Azure, Google Cloud Platform
- AnyApp support: For custom/private cloud apps support

Agentless CASB solution, accelerating deployments

Lookout's flexible and agentless architecture allows frictionless deployment without any additional software installation on the end-user devices. Agentless support enforces data security controls on mobile devices (personal, BYO device), enabling seamless and secure access to any cloud, from any location and any device – managed or unmanaged.

Single vendor for SaaS governance and email security

Lookout CASB extends its CASB functionality to email in Office 365 and G Suite, allowing organizations to apply existing DLP policies to emails, and enable consistent CASB controls across apps, emails and devices. This ensures full visibility into every applicable data set and secures collaboration across OneDrive, Teams, Outlook, Sharepoint, Gmail, G Drive and other apps.

Unified Policy Enforcement for all Clouds

Lookout's centralized policy enforcement enables unified and consistent cloud security approach in a multi-cloud environment, and helps govern the full life cycle of data through discovery, classification, access control, encryption, masking, DRM and threat protection using a single pane of glass. Lookout's attribute-based policy engine is highly flexible and configurable, inspecting data in any mode – API, proxy and email, providing extensive coverage across multiple cloud collaboration scenarios.

Advanced DLP Engine

Lookout CASB integrated and centralized DLP engine is purpose-built to detect both historical information and real-time data in motion, inspecting data in any mode – API, proxy or Email – and enforcing advanced policies as the data moves across workflows, applications, and even unmanaged devices. Our latest DLP features include:

 More than 1,000 data types and ready-made compliance templates for HIPAA, PCI, GDPR, CCPA, Data Residency, organized by country and compliance class for ready use in policies.



- DLP rule templates for both structured and unstructured data.
- Advanced workflows for scanning and protecting data with a new document rule template that allows simultaneous inspection of content and metadata in policies.
- For content, rule templates can specify watermark text as well as file names, sizes, and types.
- For metadata, rule templates can specify data classification types and labels.
- Optimized Optical Character Recognition (OCR) engine, allowing low-latency examination of images and scanned documents
- Tighter integrations with document classification workflows by Titus and Microsoft MIP. Policy workflows support recognition of documents with multiple classification labels by multiple engines, and can help in contextual reclassification.

Advanced UEBA with detailed entity and incident analysis

Lookout CASB UEBA is backed by deep machine learning capability and 3D visuals, with drill-down capabilities to every last detail and relationship to pinpoint variations from normal patterns and detect anomalous user activity. 60+ attributes are analyzed from every user activity to calculate the risk posture and generate detailed logs to aid in forensics.

Lookout UEBA also supports creation of custom anomalous behavior profiles for focused monitoring of anomalous events. For example, enterprises have the provision to create profiles to track user activities such as content sharing, uploading, or updating.

Endpoint security controls to manage BYO devices

Lookout's native rights management and integration with ActiveSync proxy allows organizations to manage any enduser device, including BYOD. Lookout enables tighter security controls, allowing you to apply contextual, adaptive security policies on the devices and not just limit the functionality to device block or data wipe. For example, preventing access from risky networks during travels or block sensitive content sync if an user turns highly risky.

DRM built for remote collaboration

Lookout has enhanced its innovative DRM platform by introducing the first-to-market collaboration framework that enables simultaneous use of multiple master keys to encrypt documents on any cloud application or repository. With this functionality, enterprises can secure external partner or vendor data with their own master key, even when the data resides within the same cloud app. Additionally, DRM allows admins to have complete visibility into the externals users and the data they possess. In case an user turns risky, admins can revoke the keys anytime to prevent accessing sensitive data in downloaded files.



End-to-end data protection: field-level encryption and file-level DRM

Lookout offers best-in-class cloud security and data protection capabilities, securing data at rest, in transit or in use, across multiple clouds – structured and unstructured, and also extends CASB security controls on the data downloaded on devices. Customers have exclusive control over the keys for both DRM and cloud data protection, preventing the risk of data exposure or leaks due to breaches. Additional data protection capabilities include:

- Field-level data protection for structured cloud apps
- 40+ algorithms to support function and format preservation in the cloud
- Email data protection that includes sensitive content masking from subject and body, data rights management, and attachments encryption
- FIPS 140-2 validated Searchable Strong Encryption (SSE) solution - first in the cloud visibility and data protection industry
- Granular policy controls to selectively encrypt or tokenize any type of data

Deep Application Intelligence

Lookout CASB secures all major application activities, not just uploads and downloads and prevents collaboration invites to secured data by folder/site/channel in real-time. CASB can differentiate between personal and corporate instances of apps (example OneDrive, Slack) and enables differentiated policies in inline mode between apps of the same suite. For example, allowing uploads of sensitive content to OneDrive but denying uploads to SharePoint sites.

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.

To learn more about Lookout CASB, visit

lookout.com/products/cloud-access-security-broker

lookout.com