Lookout®

Unlock the Power of CASB

5 Key Advantages of Lookout Secure Cloud Access

Table of contents

Introducing Lookout Secure Cloud Access

In today's cloud-based digital landscape, data is more valuable than ever. And the ever-expanding attack surface makes discovering, classifying, and protecting data an ongoing challenge.

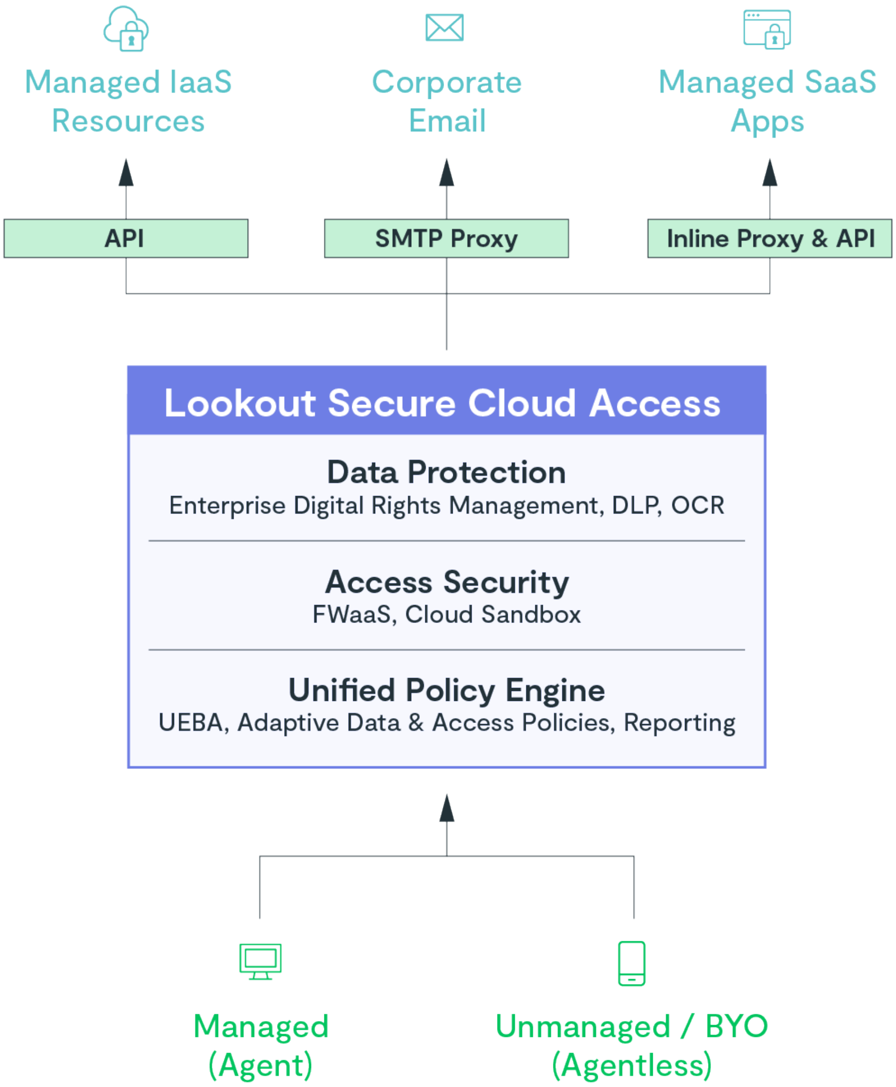
The numbers illustrate the risk. Just 54% of companies know where their sensitive data is stored.[1] A stunning 65% collect so much data that they're unable to categorize or analyze it.[2] With employees and contractors accessing data from a variety of locations and devices, this lack of visibility presents a major security risk, particularly when users engage in high-risk behavior.

To effectively protect data, organizations need visibility into where data resides, how it is being shared, and who has access.

Lookout Secure Cloud Access is a cloud access security broker (CASB) built on the foundation of zero trust. A growing number of organizations rely on it to help them discover, assess, and protect data across all cloud and SaaS applications.

Unlike the static data security policies of traditional vendor solutions, Lookout Secure Cloud Access's adaptive policies give you the context of each request to access data or apps. This reduces false positives for data sharing and support tickets for IT while improving worker productivity.

Lookout Secure Cloud Access puts you in control of your data as it moves, wherever it moves. Its centralized policy engine provides granular and adaptive data loss prevention (DLP) capabilities, simplifying the definition and enforcement of security policies across all cloud and Saas apps.



This white paper provides an overview of Lookout's innovative approach to delivering CASB capabilities on our unified security platform. It focuses on our core design principles, which deliver critical strategic value to organizations seeking to protect their most important asset — their data.

[1] https://www.spirion.com/data-classification/
[2] https://www.thalesgroup.com/en/markets/digital-identity-and-security/press-release/businesses-collect-more-data-than-they-can-handle-reveals-gemalto

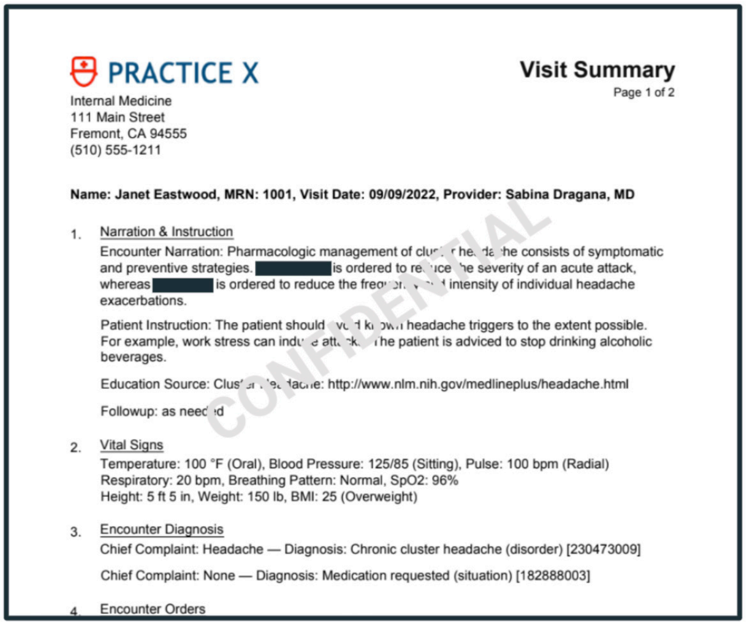
Get granular control over your data

Your organization relies on a variety of stakeholders using multiple collaboration tools. Not all of them reside within your organization. This presents quite the challenge. You must keep data secure as it's shared between external contractors and partners. Then, when projects are completed, you must protect the data that was shared.

Lookout Secure Cloud Access natively built digital rights management (DRM) capabilities provide complete control over sensitive data regardless of who shares it and how it's shared. Your data is safe, whether your employees, contractors, and partners collaborate via email or tools such as Slack, Microsoft Teams, Box, Dropbox, Google Drive, and Microsoft OneDrive.

Unlike other data protection solutions that simply enforce policies for allowing or denying access to data, Lookout enables flexible policies that put security guardrails around that access.

Lookout's exact data matching (EDM) and optical character recognition (OCR) technologies identify and protect sensitive data in a variety of formats, including text, images, and other scanned documents. Lookout scans files and folders as they're shared, and identifies and protects confidential information based on predefined policies with several enforcement options.



PRACTICE X

Internal Medicine
111 Main Street
Fremont, CA 94555
(510) 555-1211

Visit Summary

Page 1 of 2

Name: Janet Eastwood, MRN: 1001, Visit Date: 09/09/2022, Provider: Sabina Dragana, MD

1. Narration & Instruction

   Encounter Narration: Pharmacologic management of cluster headache consists of symptomatic and preventive strategies. [redacted] is ordered to reduce the severity of an acute attack, whereas [redacted] is ordered to reduce the frequency and intensity of individual headache exacerbations.

   Patient Instruction: The patient should avoid known headache triggers to the extent possible. For example, work stress can induce attack. The patient is adviced to stop drinking alcoholic beverages.

   Education Source: Cluster headache: http://www.nlm.nih.gov/medlineplus/headache.html

   Followup: as needed

2. Vital Signs

   Temperature: 100 °F (Oral), Blood Pressure: 125/85 (Sitting), Pulse: 100 bpm (Radial)
   Respiratory: 20 bpm, Breathing Pattern: Normal, SpO2: 96%
   Height: 5 ft 5 in, Weight: 150 lb, BMI: 25 (Overweight)

3. Encounter Diagnosis

   Chief Complaint: Headache — Diagnosis: Chronic cluster headache (disorder) [230473009]

   Chief Complaint: None — Diagnosis: Medication requested (situation) [182888003]

4. Encounter Orders

Lookout DRM policies redact all confidential information related to healthcare privacy regulations and incorporate a watermark to prevent sharing sensitive data with unauthorized users and to remain compliant.

> Lookout provides powerful native DRM functionality that allows organizations to control access to data and content, even after it has been shared with others. Organizations maintain control over their data even when it is stored on unmanaged devices.

- **Mask or redact:** Lookout identifies sensitive data such as social security numbers and credit card numbers, and also data that is specific to regions and industries. This allows admins to apply policies that enable data sharing while masking or redacting the sensitive information. Tools that lack DRM functionality can identify sensitive documents but they can't mask or redact information, so IT is forced to block data sharing, which hampers worker activity.
- **Watermark:** To maintain data security, Lookout can automatically apply watermarks to alert users of confidential content in sensitive files. Watermarks discourage employees from taking screenshots or sharing the documents.
- **Encrypt:** Lookout can encrypt files to ensure only authorized users have access. That access can expire after a defined amount of time. Encryption can also be combined with other DLP rules. For example, confidential information can remain masked within a decrypted file. This prevents an employee or a contractor from accessing sensitive documents once they leave an organization.

You can take data protection a step further by defining dynamic digital rights management policies to restrict who can decrypt content. This can involve a combination of configurable options such as user credentials, user risk levels, and geo-location.

The benefits of native DRM capabilities are clear: they facilitate secure collaboration and boost productivity while providing robust protection for sensitive data.

Identify anomalies, stop threats sooner

Lookout Secure Cloud Access applies user and entity behavior analytics (UEBA) to continuously monitor and assess users, devices, and activities. This enables your team to identify deviations from normal behavior, so you can quickly remediate a wide range of potential threats, including: malicious insiders, compromised accounts, and advanced persistent threats (APTs).

60%

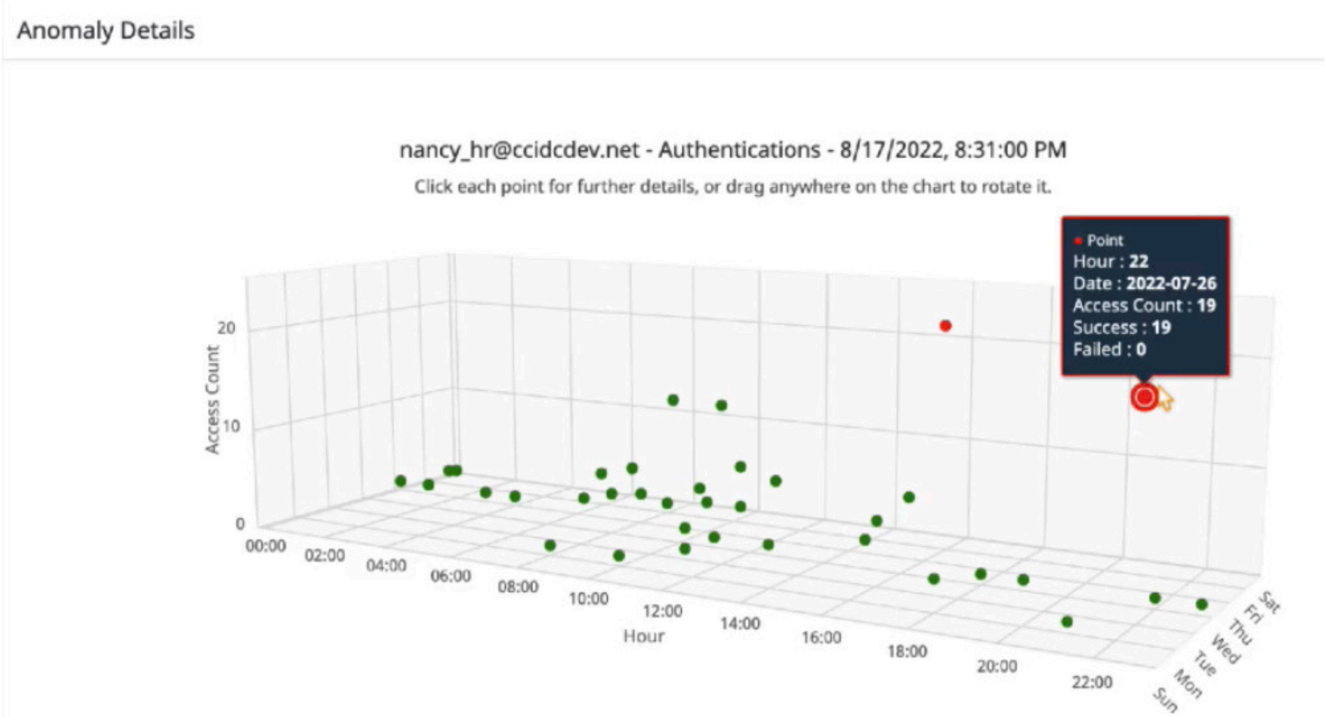
60% of data breaches are caused by authenticated users. By monitoring user behavior and identifying large data downloads and similar anomalies, UEBA technology can detect malicious activity such as data exfiltration or fraud.

UEBA not only monitors geo-location anomalies, it also identifies risky activity such as mass downloads from individual users, the use of unmanaged devices that might be infected with malware, persistent log-in attempts, modifications to data, or users accessing many files that they have not accessed before.

Monitor risk with adaptive access

Through real-time analysis of user, device, and location patterns, Lookout generates precise user risk scores that can be customized to your policies. Our adaptive access feature uses machine learning to analyze user behavior, device health, and location. Lookout assigns a risk score to each user that can increase based on user, IP, app activity and device posture then determines whether to grant or deny access to specific data based on that score.

An elevated risk score can trigger alerts for admin follow up, or automatically provide additional actions based on pre-set security policies such as requiring user re-authentication, masking or redacting data, or blocking user access completely.



Anomaly Details

nancy_hr@ccidcdev.net - Authentications - 8/17/2022, 8:31:00 PM

Click each point for further details, or drag anywhere on the chart to rotate it.

● Point
Hour : 22
Date : 2022-07-26
Access Count : 19
Success : 19
Failed : 0

Discrepancies in log-in activities trigger anomaly alerts.
This graph shows several log-ins outside of normal dates and times for a user.

Secure Cloud Access is built on the principles of zero trust. It validates a user's context before granting access to apps and data, and then continuously verifies access rights. Whether users are trying to access cloud and SaaS apps from managed or unmanaged devices, they're authenticated and authorized based on the security posture of their devices, as well as their risk profiles. Each user's level of access can dynamically change based on the risk indicators.

Reduce complexity and cost with a unified security platform

As networks and cyber threats have evolved and become increasingly complex, developers have created new products and solutions to meet the challenges they represent. This has resulted in a proliferation of point products, each designed to address a specific security threat.

As a result, some organizations now have as many as 76 security tools to manage. Teams are becoming overwhelmed. And the cost of doing business with so many vendors has become unsustainable.

These conditions have started to drive consolidation within the security market. But what security professionals need is visibility and management from a single location — a security platform that integrates a variety of security technologies into a single, unified architecture.

Traditional security stacks can be complex to manage and expensive to purchase and maintain. To make matters worse, each point product has its own console and administration interface. Packets must pass through multiple appliances before reaching their destination, which leads to latency and performance issues. And VPN-based access is slow and cumbersome. All add up to a poor user experience.

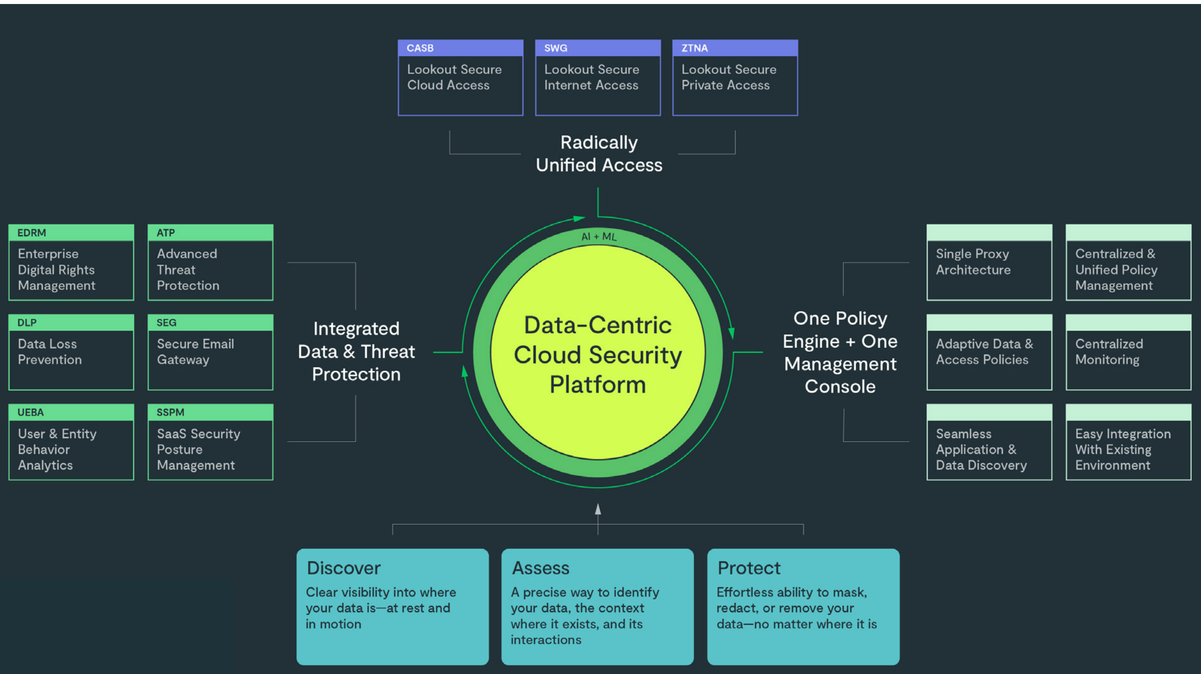
Lookout's unified security platform architecture reduces both the cost and complexity of security management. Its single console and administration interface mean you spend less managing policies and configurations across tools, integrating new services, and dealing with multiple vendors. By comparison, disparate point products don't always integrate well, if at all. They often require IT teams to pivot across platforms, administration screens, and tools.

Lookout Secure Cloud Access offers bundled pricing and lower overall costs for configuring, administering, and maintaining one unified platform, which can also reduce licensing costs.

One of the primary benefits of a unified security platform is it enables centralized administration policy enforcement, so you can apply consistent security policies, including those for DLP and data governance, across users, devices, and locations. This eliminates policy misalignment and misconfiguration errors.

Even as Lookout's centralized policy enforcement enables a unified and consistent cloud security approach, and provides extensive protection and governance within multi-cloud, multi-data center environments, it also offers a number of additional benefits:

- **Improved latency and performance.** Lookout's cloud security products use a single proxy architecture, which reduces the number of services that traffic must pass through for inspection and policy enforcement.
- **Real-time UEBA and advanced forensics.** Powered by a unified core data model, UEBA works in real-time to detect and respond to threats. This improves security and reduces the time it takes to investigate and resolve incidents.
- **Consistent threat tracking.** Lookout's unified security platform architecture gives your security team a clear understanding of the threats facing your organization, across all apps and data, so you can rapidly mitigate them.


CASB
Lookout Secure Cloud Access
SWG
Lookout Secure Internet Access
ZTNA
Lookout Secure Private Access
Radically Unified Access
EDRM
Enterprise Digital Rights Management
ATP
Advanced Threat Protection
DLP
Data Loss Prevention
SEG
Secure Email Gateway
UEBA
User & Entity Behavior Analytics
SSPM
SaaS Security Posture Management
Integrated Data & Threat Protection
AI + ML
Data-Centric Cloud Security Platform
One Policy Engine + One Management Console
Single Proxy Architecture
Centralized & Unified Policy Management
Adaptive Data & Access Policies
Centralized Monitoring
Seamless Application & Data Discovery
Easy Integration With Existing Environment
Discover
Clear visibility into where your data is—at rest and in motion
Assess
A precise way to identify your data, the context where it exists, and its interactions
Protect
Effortless ability to mask, redact, or remove your data—no matter where it is

Meet modern security needs with an application intelligent proxy

Proxies act as an intermediary between users and applications, and provide a valuable layer of security. However, not all proxies are built the same, and traditional proxies tend to only identify destinations as good or bad, without providing additional context.

Lookout's proxy provides context. For example, it identifies the security policy differences between personal and business usage of applications such as Google Workspace and Microsoft 365 and then adapts access based on those policies.

Since Lookout applies its purpose-built, intelligent proxy across a unified platform, it enables a consistent, comprehensive approach to securing all internet traffic, SaaS apps, and private enterprise apps. The single proxy architecture simplifies the management and deployment of security tools, ensuring consistent policy enforcement.

Lookout's intelligent proxy combines advanced security capabilities, unified policy enforcement, and comprehensive visibility to deliver robust protection for internet traffic and data.

By enabling capabilities such as user coaching, secure collaboration, and denied public sharing of sensitive data, the Lookout application intelligent proxy strikes the perfect balance between productivity and security.

Leverage the public cloud for a highly scalable architecture

Far too many security service edge (SSE) providers are encumbered by legacy proprietary cloud architectures for deployment of points of presence (POPs).

Lookout's AWS Global Accelerator includes a global network of 109 Points of Presence in 92 cities across 50 countries. This delivers a huge strategic advantage. It allows you to grow faster than your competitors. When you need a new POP location, Lookout can deploy it in just days, versus the months typically required by other providers.

Lookout enables customers to scale anywhere on demand with AWS. This gives you the advantages of cloud-first microservices, better tooling and feature velocity, and improved time-to-market.

Leverage the public cloud for speed, scalability, and highly competitive costs. **76% of the internet can be reached from cloud architecture. 50% of the top 1 million sites are in the cloud and 42% of the top 100,000 sites are on Amazon.** In contrast, private cloud architecture doesn't have the speed or agility to keep up with the need to rapidly and reliably scale your business.

Lookout Secure Cloud Access protects your data in the cloud

Every day, your employees upload, download, and share corporate data from your approved SaaS applications. While this is great for productivity, it increases the risk of data leakage, unauthorized sharing, regulatory violations, or malware incursions.

Lookout Secure Cloud Access protects your data in the cloud and gives you control over the usage of managed and unmanaged cloud apps. The benefits include:

- Acceleration of the speed and scale of deployment;
- The ability to identify and stop threats sooner, and;
- Reduced cost.

Take the next step. Get a SaaS Risk Assessment now.

We've described how Lookout Secure Cloud Access can help you protect your data, comply with regulations, and deliver return on investment. Now, learn more about how your current data security efforts are performing. Register for our free SaaS Risk Assessment. It:

- Pinpoints blind spots and areas that expose you to risk;
- Provides visibility into users, devices, and data associated with your SaaS apps, and;
- Offers actionable insights into how Lookout can help.

About Lookout

Lookout, Inc. is the data-centric cloud security company that delivers zero trust security by reducing risk and protecting data wherever it goes, without boundaries or limits. Our unified, cloud-native platform safeguards digital information across devices, apps, networks and clouds and is as fluid and flexible as the modern digital world. Lookout is trusted by enterprises and government agencies of all sizes to protect the sensitive data they care about most, enabling them to work and connect freely and safely. To learn more about the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and X (previously 'Twitter').

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo