Lookout®

Safeguarding Cloud Data With CASB:

4 Key Questions to Consider

lookout.com

Highlights

- Discover how CASBs serve as cloud-native DLP solutions for multi-cloud environments.
- Explore the importance of real-time visibility and consistent policy enforcement to cloud data protection.
- Understand why adaptive data protection that extends into unmanaged devices and applications is critical to securing hybrid work.

Protecting your cloud data requires the right solution

Cloud technologies have revolutionized the way users work, enabling them to collaborate from anywhere. Gone are the days when work was confined to specific locations or devices. Employees now access corporate resources directly through public networks and personal devices.

While this newfound freedom has boosted productivity, it does come with risks. Your data is now scattered across multiple cloud environments, each with its own security settings, and each shared with applications and endpoints you can't control.

To safeguard your cloud data effectively, you should consider a cloud access security broker (CASB). Just keep in mind that not all CASB products are created equal.

In this e-book, we'll explore four fundamental questions crucial to evaluating CASB products. By doing so, we'll empower you to make an informed decision, one that will ensure your cloud data remains secure while enabling seamless access for your hybrid workforce.

Why access controls and legacy solutions alone cannot protect cloud data

Existing security solutions simply aren't designed to protect sensitive data in the cloud. By understanding the challenges of securing cloud apps, organizations can mitigate the risks and protect their sensitive data.

Read Blog

Question 1: Will your data be secure across multi-cloud deployments?

Traditionally, CASBs only had to focus on a limited number of cloud apps. However, IT and security teams now face the daunting task of managing and securing dozens to hundreds of apps, each with its own settings and data handling methods. This complexity leads to potential security gaps and room for errors that could compromise your data.

To address these challenges effectively, your CASB must be able to enforce policies consistently from a centralized location across three major areas:

- **SaaS apps:** Statista revealed that enterprises deployed an average of 130 SaaS apps as of 2022. With such a vast app landscape, ensuring consistent data protection across all environments becomes paramount.
- **Data repositories:** To store data, enterprises rely on IaaS solutions such as Amazon Web Services, Google Cloud Platform, and Microsoft Azure. Your CASB must seamlessly extend its policies into these cloud repositories.
- **Configurations/settings:** With countless apps and data repositories, the risk of misconfigurations increases. Your CASB should be able to discover configurations across your entire organization and align them with industry standards for security and compliance.

Enterprise Strategy Group (ESG) survey: Reported data loss sources

26% from an IT-provisioned cloud service

25% from an unsanctioned cloud service

25% from misconfigured object storage accounts

Read Report

Lookout.

How Safe Is Your Data?

4 Must-Have Capabilities Your SaaS Security Needs to Protect Data in the Cloud

lookout.com

Question 2: Will you be able to enforce policies beyond SaaS apps?

It's no longer sufficient to merely protect against inbound threats to your SaaS apps and the data that resides within them. With remote and hybrid work models now common, your employees, partners, and contractors are using a variety of unmanaged devices and apps to access your cloud data. Often, many of them aren't controlled by your IT department, which makes the risk to your data high. According to an ESG survey, more than one-third (36%) indicated their organizations suffered data exposure due to remote users.

To protect your data, you need a CASB solution that goes beyond the traditional boundaries of IT control.

Security beyond traditional IT boundaries

- **Unsanctioned, personal, and third-party clouds (shadow IT):** It's not just the cloud apps you deploy that need protection. Often, employees use personal accounts of enterprise apps or unsanctioned services. In addition, partners or contractors may use their own apps to access your corporate data.
- **Unmanaged devices:** With hybrid work, your data is now exposed at a wide variety of endpoints; many of them aren't managed by your IT teams. These endpoints can include personal or third-party devices.
- **Emails:** While some security vendors treat SaaS apps and email as separate entities, the reality is that data exfiltration and sharing regularly occur through emails. This could involve unintentionally sending sensitive information to the wrong recipients, either within the email's body or as an attachment.

Question 3: Will you have real-time visibility into what's happening to your data?

In today's hybrid work environment, you've lost the critical visibility you once had on premises.

With employees collaborating from diverse locations and devices, and data flowing through a complex web of cloud services and endpoints, it's essential to have a robust CASB solution that enables continuous monitoring.

Device health

With the use of personal devices and unsecured networks surging, it's vital that you gain visibility into the risk level of every endpoint. Your CASB should know the answers to the following questions:

- Is it managed?
- Which version of the operating system is it using?
- Is it jailbroken?
- Does it have antivirus and antimalware installed?

User risk posture

Data risk extends beyond conventional malware, encompassing accidental data sharing, malicious insider threats, or compromised accounts. Even users with legitimate credentials can pose a threat. Make sure your solution answer these questions:

- Does it offer insights into past and current behavior, so you can identify anomalies?
- Does it know when users are copying, sharing, or modifying data?
- Does it know user location and network health?

Data sensitivity

Ultimately, seamless access requires decisions that align with the value of the data. Your CASB should answer:

- What types of data are in image files, folders, or zipped files?
- What data do you own in both structured and unstructured formats?
- How is data leaving your cloud apps?
- Do you have open shares and exposed data governed by regulations such as PCI, HIPAA, or GDPR?

> Ultimately, data protection should align with the way people work today.

Jon Oltsik, Senior Principal Analyst & ESG Fellow

ESG Report, Modern Cybersecurity Solutions Must Include Data Protection

Lookout.

How Safe Is Your Data?

4 Must-Have Capabilities Your SaaS Security Needs to Protect Data in the Cloud

lookout.com

Read Report

Question 4: Will you be limited to just allow/deny access?

To succeed in today's work world, you need to protect both your data and your productivity. That's why you must be intentional about access management. Leverage the increased visibility you get with your CASB to make the informed decisions that fit your data's value and that are sensitive to the fluctuating risk levels surrounding it. Here are some of the must-have capabilities you need to do so:

- **Adaptive zero-trust access:** Simply allowing or denying access can impede your hybrid workforce's efficiency and collaboration. Embrace adaptive access by considering factors like device health, user behavior, and location to determine acceptable risk levels for different types of data on an ongoing basis.
- **Precise data protection:** Instead of complete access denial, you should enforce data-centric policies. This includes disabling downloads and watermarking documents. Additionally, use redaction or masking to restrict access to sensitive information within data files.
- **Proactive encryption:** Beyond safeguarding data within cloud apps, your CASB should proactively enforce policies when data moves into unmanaged apps and devices. This entails encrypting data and setting time restrictions as it leaves your apps. With this capability, you can mandate step-up authentication or other requirements for data access from any location.

Rethinking CASB with a focus on data security

As the threat landscape evolves, you can't base your security solely on allow-denial access.

Instead, view CASB products as cloud-native data loss prevention (DLP) solutions and evaluate them accordingly. For effective cloud security, real-time visibility into all data activities and surrounding contexts is crucial. You must also maintain the ability to enforce policies consistently across diverse environments while adjusting based on risk levels and data sensitivity.

By embracing a data-centric mindset and selecting a robust CASB solution, you'll fortify your organization's cloud security, ensuring the safe and seamless handling of sensitive information in the dynamic world of hybrid work.

Cloud DLP Secures Data Shared With Thousands of Contractors

Discover why a leading construction firm chose the Lookout's CASB solution, seamlessly protecting sensitive data with native-DLP capabilities as it collaborated with its third-party partners.

Read Case Study

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 moreabout the Lookout Cloud Security Platform, visit www.lookout.com and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

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