Lookout

How Safe Is Your Data?

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

Highlights

- Learn why existing solutions struggle to protect cloud data
- Understand the major data protection challenges and how to overcome them
- Uncover the essential capabilities for safeguarding data in the cloud

The pros and cons of cloud adoption

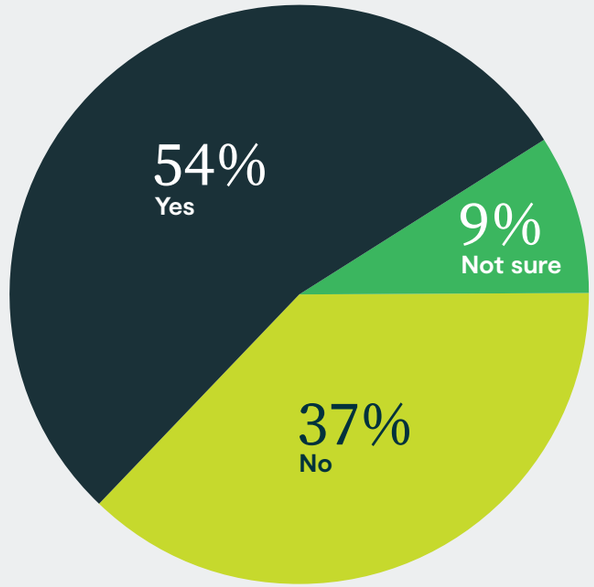
Cloud adoption has enabled your organization to enhance access to corporate resources, boost operational efficiency, and lower costs. It also has introduced a new set of cybersecurity challenges, particularly when it comes to safeguarding data in the cloud, whether it's sensitive corporate information or data that are protected by regulations.

To fulfill IT, security, and compliance requirements while supporting your hybrid workforce, you need to protect sensitive data without hindering access demands. Unfortunately, the cloud's unique characteristics have made data protection complex. Based on a survey by the Gartner Peer Community, a staggering 54% of organizations experienced a breach between 2020 and 2022. Furthermore, the costs of such breaches have soared, reaching $5.02 million in 2022, according to IBM's Cost of a Data Breach report.

By understanding how to secure data in SaaS apps, you'll be equipped to choose cybersecurity products that offer the protection you need.

Gartner®
Peer Community™

Has your organization suffered a data breach in the past 2-3 years?



Read Survey

n=542
Note: May not add up to 100% due to rounding

The limitations of access controls and legacy solutions

The 2020 pandemic fueled widespread adoption of cloud technology. To protect their valuable cloud data, organizations turned to identity and access management (IAM) with single sign-on (SSO) to govern access. Many also sought to extend their on-premises data loss prevention (DLP) and secure web gateways (SWG) capabilities.

However, as hybrid work has become increasingly prevalent — by 2022, 74% of employers were offered such arrangements, according to IFEBP — these approaches have become insufficient for effectively safeguarding cloud data.

Inefficiencies, vulnerabilities, and lack of visibility

- **IAMs and SSOs focus on access:** These solutions simplify app access management and rely on step-up authentication for security. As a result, they lack visibility into data access activities. So, once a user is authenticated, they're unable to control how data is accessed or shared.
- **Enterprise DLP can't reach cloud data:** Organizations previously invested heavily into on-premises DLP solutions. But with data now in the cloud, these tools don't provide the necessary visibility. Some organizations attempt to extend them into the cloud, but that requires backhauling traffic. This restricts productivity and creates operational inefficiencies.
- **Standalone SWGs don't care about data movements:** Whether on-premises or in the cloud, traditional SWGs protect cloud assets accessed via the internet. While these products excel at blocking incoming threats, they fall short when it comes to preventing outbound data movement. As a result, they can't effectively mitigate the risk of accidental or malicious data loss. This leaves your organization vulnerable to breaches.

Gartner
Peer Community™

What are the top 3 challenges that make you feel the most vulnerable?

Read Survey

n=542
Note: May not add up to 100% due to rounding

60%

of all corporate data is now stored in the cloud as of 2022.

2023 Lookout State of Hybrid Work Report

Read Report

Security challenges in the cloud

Users now rely on a variety of networks and devices to connect to your apps and data, which all reside in the cloud. The days of fencing off data within managed environments are over. Clearly, it's time for a new approach to data protection, one that takes on the challenges you face, including:

- **Lack of visibility and control over sensitive and compliant data:** According to the Gartner Peer Community, 61% of organizations cite this as their top security challenge. It's easy to see why. Your data is scattered across different apps. Users can access information from anywhere and share it with anyone, including third parties that are using apps and devices beyond your control. As a result, you have no idea what data you own, where it resides, or how it's being used.
- **Everchanging risk postures:** Your users now sit outside corporate perimeters. Their risk levels are constantly changing, depending on the location, network, and device they choose. In this hybrid work environment, where everything's decentralized, it's difficult to keep track of the changing risk postures and enforce policies against them.
- **Keeping up with the configurations of your apps:** One of the great things about cloud services is that cloud providers take on a lot of tasks you used to handle, such as patching. But configurations and access settings still fall on you. With the countless SaaS apps you now need to manage, it's increasingly difficult to grasp the controls and settings across multiple environments.

CASB: Why cloud-native DLP is key

According to the Lookout State of Hybrid Work Report, 60% of all corporate data is now stored in the cloud (as of 2022). Analysts consider a cloud access security broker (CASB) as the go-to solution for safeguarding cloud access. But access isn't the problem; data security is. To protect the data in your SaaS apps and cloud repositories, you need a CASB solution that includes cloud-native DLP that can protect your data no matter where it flows to or how it's handled.

43%

of hybrid workers use bring-your-own devices (BYOD)

32%

of hybrid workers use unapproved apps

2023 Lookout State of Hybrid Work Report

Read Report

4 MUST-HAVE CAPABILITIES TO PROTECT YOUR CLOUD DATA

1. Adaptive zero trust with precision

Seamless cloud access is essential. To protect data without hindering access, you must move beyond binary allow-deny controls. While enforcing zero trust is now standard practice, do it in a way that's precise and adaptive. This requires real-time visibility into the risk postures of users and devices, as well as into the sensitivity of the data they're trying to access.

2. Always-on data protection

According to the Lookout State of Hybrid Work Report, 43% of hybrid workers use bring-your-own devices (BYOD) and 32% of them use unapproved apps.

To protect data no matter where it flows, you need two critical capabilities. First, you must be able to discover and classify all the data you own, whether it's intellectual property, sensitive financial information, or compliance information. Then, you must be able to enforce policies consistently across all apps and endpoints. Be prepared to take action on individual pieces of data, including watermarking, reacting or masking sensitive information, and encrypting files so that only authorized users have access.

3. Protect email like any other app

We tend to think of SaaS apps as just cloud services like Salesforce, ServiceNow, or Slack. That's how many companies build their CASB solutions. And that's why many end up purchasing a separate product to protect emails. Your cloud DLP solution should treat email like any other app. When you create and enforce policies, they should extend into emails, where accidental information sharing happens frequently.

4. Identify and remediate misconfigurations

Given the countless apps you need to manage, policy enforcement and configurations should go hand-in-hand. If you misconfigure an app, it could lead to a data breach. Make sure you can match all your SaaS apps to industry-standard security and compliance settings and that you have visibility when something is misconfigured.

Why it's time to embrace a CASB with cloud-native DLP

Existing cybersecurity solutions fall short of effectively protecting data in the cloud, and a siloed security approach adds complexity and risk.

As you consider CASB solutions, remember that access isn't really the issue in today's work-from-anywhere environment, data protection is. You need a CASB solution with a cloud-native DLP that works no matter where your data resides.

How does your data security stack up? Take the quiz.

In an era of digital transformation, it can be difficult to know if your IT and security team are equipped to protect your data. Take our Data Risk Assessment to see how your data protection ranks, and learn what you can do to improve security in a few short minutes.

Start Assessment Now

Lookout

About Lookout

Lookout, Inc. is the endpoint-to-cloud cybersecurity 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