



# Minimize Risk To Your Corporate Data With End-to-End Visibility and Intelligent Security Controls



## Highlights

- With hybrid work, your data is now flowing freely between cloud apps, private apps, and endpoint devices, which means it's exposed to countless new risks.
- To minimize risk to your data as it's being accessed from anywhere, you need visibility from endpoint to cloud, including continuous assessment of device and user risk levels as well as an understanding of data sensitivity levels.
- Alongside end-to-end insights, you also need the ability to enforce consistent policies regardless of where your organization's data resides or how it's accessed.

Equipped with personal tablets and smartphones, workers can now connect directly to your corporate resources from their home and unsecured networks. While this has streamlined business operations and boosted productivity, it has also exposed your valuable data to new risks.

Currently, many organizations rely on traditional security tools that focus on static, point-in-time authentication that is ideal for data access within a defined perimeter. The philosophy is that if a user's identity is proven with a password and a second factor of authentication, then they are safe to access data.

The problem is that users are not always using corporate devices, may have malicious intent or accidentally share sensitive information with an unauthorized user. If you are using a virtual private network (VPN) or single sign-on (SSO), you can authenticate and authorize users at the time of access, but these tools will not protect from any malicious or accidental exfiltration of corporate data.

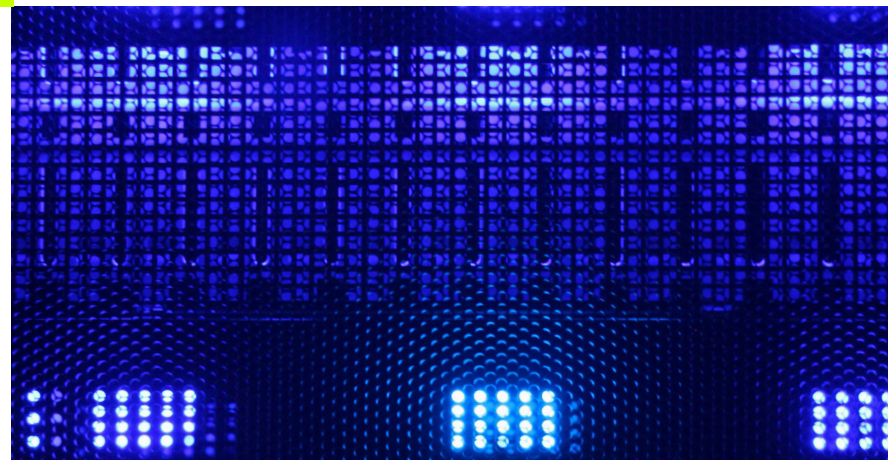
With the countless apps, users, and endpoints to keep tabs on, the traditional, appliance-based approach to security is no longer enough. Point products create silos, which in turn create management burdens on your already stretched IT and security teams. They also give you limited insights and control over what's happening to your data.

To ensure that your data is protected in this complex environment, you need to pivot into a platform approach. This requires finding a solution that combines continuous end-to-end monitoring alongside a unified policy framework.

In this e-book, we will discuss how to minimize the risk to your data and how the Lookout Cloud Security Platform, which delivers a security service edge (SSE) solution that includes native endpoint and data protection, is able to effectively minimize risk regardless of where your data resides.

“36% of IT and security professionals cite remote users as the top contributor to public-cloud related data loss”

- Enterprise Strategy Group



## Mitigating risk starts with getting complete visibility of the land

The cloud has made it simpler to streamline and scale operations. It also gives your users easy access to apps and data so they can stay productive from anywhere and any device. But this way of working also introduces a host of new threats like phishing attacks, cloud misconfigurations, and corporate data exfiltration from these apps.

It's no longer reasonable to assume that your on-premises tools have insights into the activities within your infrastructure and the entities seeking to access your resources. Instead, you need continuous insights into the various environments where your data is flowing.

**Lookout's unified cloud security platform provides end-to-end insights into these three major areas:**



### Cloud apps

Thanks to cloud apps, you no longer have to worry about running your own data centers, but there are still a lot of responsibilities that fall onto your IT and security teams. Ultimately, it's up to you to secure your environment, configure them, and understand what data resides within the apps and how it can be shared across users, devices and networks. Lookout grants robust insights into what's happening in your cloud apps.



### Private apps

As organizations go through digital transformation, resources in private clouds or on premises are sometimes forgotten. This could make them targets for malicious users that want to move laterally around your infrastructure. Lookout continuously monitors and protects data residing in your private apps. It provides users' access to these apps based on the risk posture of their devices and only gives users access to the apps they are authorized to access.



### The web and shadow IT

With hybrid work, the internet has become your default corporate network. Therefore, it's critical that you have visibility into internet usage, not just to intercept malware but also to prevent data leakage and enforce acceptable use policy. And the unmanaged cloud apps your employees are using are part of this picture. Lookout inspects both inbound and outbound internet traffic for any sensitive or malicious content that may affect integrity of your corporate data or compromise your underlying infrastructure.



## Contextual insights to precisely protect data

It's not just about the breadth of insights. You also need to understand the context and fluctuating risk levels affecting the integrity of your data.

It's this continuous insight into users, device posture, and consistent policy enforcement that separates some SSE solutions from others. With a focus on protecting data, the Lookout platform ensures that policies are enforced even when data is being suspiciously modified or it flows to unmanaged devices, including mobile devices.

**Below are the three major capabilities that the Lookout platform provides:**



### Endpoint security

Personal devices including mobile devices are used to access corporate resources. And due to the different apps they can have installed and the networks they can connect to, these endpoints' risk levels are constantly fluctuating. With continuous monitoring of endpoint device health, you can protect your data from insecure networks and outdated operating systems as well as app vulnerabilities, malware, and phishing attacks.



### User and entity behavior analytics (UEBA)

With people working from anywhere, you no longer have the control you used to have within corporate perimeters. Therefore, it's critical that you constantly monitor the behavior of your users. Whether it's the apps that they connect to or how they access and modify data, identifying anomalous behavior is critical to prevent a malicious insider or a compromised account from stealing your data.



### Data loss prevention (DLP) and digital rights management (DRM)

To protect data effectively, access security is not enough. You need controls to protect and reduce risk to your corporate data. With native data protection capabilities as part of a cloud security platform, you can identify data sensitivity and enforce the right policy to limit access like masking and redacting sensitive information, or encrypting and sharing sensitive documents, instead of denying access to information outright.

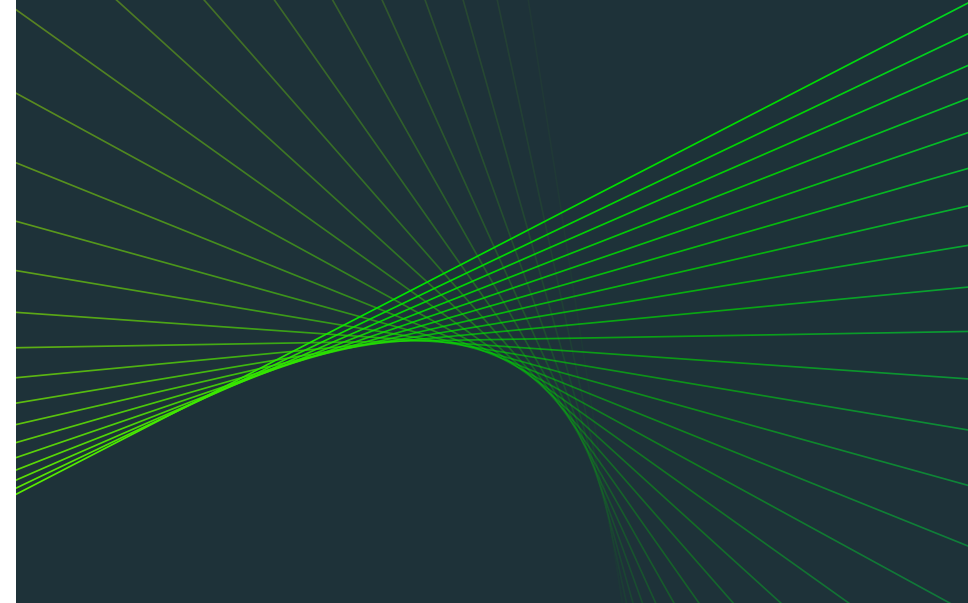
“29% of IT and security professionals cite persona devices as the top contributor to public-cloud related data loss”

- Enterprise Strategy Group

## Unified insights and dynamic policy enforcement

With thousands of activities and entities and hundreds of apps to keep tabs of, figuring out how to protect your data can be overwhelming. By combining endpoint-to-cloud visibility with advanced data protection capabilities, Lookout automates the process of minimizing data risk.

**By leveraging deep insights alongside a unified policy engine, Lookout enables organizations to protect their data efficiently and stay compliant. Here are some common use cases:**



### Accidental data exfiltration

Cloud apps have made collaboration and data access very simple. But that also means it's easy to accidentally share content to the wrong person. By monitoring network traffic, Lookout can detect whether sensitive data is being leaked out. With native data protection, the platform can enforce various data protection measures including watermarking and keyword redaction.



### Malicious insider threats or account takeover

Whether it's a legitimate user gone rogue or an employee's account that's been taken over, it's difficult to detect whether a user is putting your data at risk. Using user behavior analysis in our analytical engine, Lookout benchmarks what's normal so that when anomalies are detected, such as excessive downloading or data modification, the platform can block or caution the users, based on the policies set by an administrator.



### Mobile phishing attacks

Mobile devices have become one of the most lucrative targets for attackers, as they are the devices that people use the most. When a phishing link attempts to deliver malware or steal credentials, it's crucial that you have the ability to detect and mitigate against these attacks. The Lookout platform uses machine intelligence to quickly identify and block any malicious threats, whether it's coming from SMS text messages, email, or mobile apps.

## Minimizing data risk requires a holistic approach

The digital landscape has become much more complex because of cloud adoption and hybrid work. With data no longer residing in one place, organizations need security that can handle that complexity.

This requires a fundamental shift in how you approach, plan, and deploy your security strategy. Rather than rely on appliance-based tools that forces teams to be divided into silos, you need to look at a platform approach.

The Lookout Cloud Security Platform provides insights into users, endpoints, apps, and data, ensuring that data is protected regardless of whether it's in cloud apps, private apps, endpoint devices, or flowing through the internet.





## About Lookout

Lookout, Inc. is the endpoint to cloud security company purpose-built for the intersection of enterprise and personal data. We safeguard data across devices, apps, networks and clouds through our unified, cloud-native security platform — a solution that’s as fluid and flexible as the modern digital world. By giving organizations and individuals greater control over their data, we enable them to unleash its value and thrive. Lookout is trusted by enterprises of all sizes, government agencies and millions of consumers to protect sensitive data, enabling them to live, work and connect — freely and safely. To learn more about the Lookout Cloud Security Platform, visit [www.lookout.com](http://www.lookout.com) and follow Lookout on our [blog](#), [LinkedIn](#), and [Twitter](#).

For more information visit  
[lookout.com](http://lookout.com)

Request a demo at  
[lookout.com/request-a-demo](http://lookout.com/request-a-demo)

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.