Lookout

Consolidating Your IT Security?

Here's why you need a data-centric platform

Highlights

- With employees using a diverse mix of cloud apps, private apps, personal networks, and unmanaged endpoints, IT and security teams are now asked to secure an extremely complex environment.
- Point solutions may have worked before, but they won't give you the visibility, scalability and control required to tackle new challenges introduced by cloud and hybrid work.
- Security service edge (SSE) platforms that include data and endpoint protection, help organizations take an agile approach to security that's efficient and scalable.

It's no secret that the environment that IT and security teams are tasked with protecting has become considerably more complex. Even just a few years ago, most users were still going into offices, which meant that they were connected to a secure network and protected by perimeter-based security tools. Now, organizations operate a much more decentralized infrastructure.

Most have dozens or hundreds of cloud and SaaS apps, each with their own security settings and configurations. In addition to those apps, some IT teams still have software and repositories in private clouds and on-premises infrastructure that require manual patching. And since hybrid work has become the default method of work, all organizations have had to accept the fact that the public internet has become the de facto corporate network and that using personal unmanaged devices has become acceptable.

Organizations are realizing that evolving their security approach is key to adopting and securing their cloud-first operations. At first, using solutions built for specific use cases worked. But now, given how complex environments have become, point solutions no longer get the job done. With multiple consoles to manage, operational costs become high and there's increased potential for security gaps and human error.

Here at Lookout, we cut through that complexity by developing a cloud-native and a data-centric security service edge (SSE) solution that provides you with a unified insight into activities across SaaS, private clouds, on premises, and endpoints. With a simplified management console that includes a unified policy framework, the Lookout Cloud Security Platform empowers organizations with consistent and adaptive data policy enforcement no matter where the data flows to.

There are dozens of vendors in the market that sell cloud access security brokers (CASB), zero trust network access (ZTNA) and secure web gateway (SWG) products. The issue is that they often function in isolation, are not built for the cloud, and don't have built-in endpoint security and data protection, which means you have to spend time and money evaluating and deploying additional products to get complete protection.

In this e-book, we will break down what you should look for in a cloud security platform, and why Lookout's endpoint-to-cloud approach is uniquely positioned to reduce the complexity of your IT security regardless of how you operate.

"69% of respondents say that fragmented IT and security infrastructure is a top reason why their cyber resiliency hasn't improved."

– IBM Security

Consistency across your environments

Your valuable data is now sprawled across different locations and devices that your perimeter-based tools cannot reach. And as you adopt more cloud apps, or if you're engaged in mergers and acquisitions, this environment will get even more complex. It's therefore critical that security operations be moved to the cloud.

What you need to keep in mind is that this transformation cannot simply be about capabilities. If you try to switch out on-premises tools with cloud-delivered ones on a one-to-one basis, you will end up with a complicated product set that will be a burden for your IT and security teams to manage.

So whether you're looking to speed up cloud adoption of the cloud or you have to incorporate another organization's infrastructure after an acquisition, you need the ability to consistently monitor and respond to threats.

"Security teams spend 54% of their time manually producing reports."

- Panaseer

Here are some of the major benefits of having a unified endpoint-to-cloud platform:

Full visibility

Hybrid work has accelerated interconnectivity. A mobile phishing attack can now result in the exfiltration of sensitive data from a SaaS app via a Windows or a Macbook device. Instead of attempting to analyze security events via multiple different consoles, Lookout provides a simplified management system within the same platform.

Unified insights and automated protection

With continuous visibility into all activities, you have the insights needed to set up automated protection that doesn't strain your IT resources.

Consistent policy enforcement

A significant amount of resources are often poured into configuring each of your security tools correctly. With Lookout's simplified management console, you only have to write a policy once and it can be enforced across all apps, devices, and users.

Native data and endpoint protection

As cloud adoption and hybrid work continues, it's not just your infrastructure that gets more complex. So are the types of risks your data is exposed to. The ways that users, endpoints, and apps are interconnected makes the threat landscape much more complex, especially since risk in one area can easily affect another.

This is why a cloud security platform delivering an SSE stack shouldn't just be about securing SaaS apps, private apps, and internet access. The Lookout Cloud Security Platform provides native data protection capabilities, including data and endpoint protection capabilities. By consolidating these capabilities, it streamlines management so your IT and security team can focus on strategic initiatives.

The benefits of an endpoint-to-cloud platform:

Simplified management console

Rather than purchasing individual tools for the different environments where your data resides, monitor and enforce policies within the same platform.

Continuous monitoring

With how quickly events can occur in a cloud-driven world, it's no longer enough to have static checks on users or assume trust. By continuously assessing how your user is handling sensitive data and the health of the device they're using, you can make real-time decisions about access without creating additional work for your team.

Adaptive data protection across all apps and mobile endpoints

To protect your cloud operations you need security that's agile and intelligent, but siloed security strategy makes this impossible. By using a platform that understands the data you own, as well as the fluctuating risk levels of users and user devices, you can enforce data protection policies without sacrificing user productivity.

Future-proof expansion with agile security

Organizational needs are constantly changing. In addition to protecting what you already own, you also need to think about how security can support any future business requirements. Here are two of the common scenarios where a unified platform would be able to expand protection without adding additional strains on security resources:

Adopt the cloud faster while improving productivity and security

While cloud adoption has created efficiencies and empowers users to work from anywhere, it has also created additional complexity. Each app and environment you onboard come with their own settings, which means management becomes a burden that would lead to misconfigurations or human error. Cloud adoption also means that many of your on-premises investments become ineffective or obsolete.

Consolidating your IT security into a single platform that includes data protection means you can cut through this complexity with consistent policy enforcement. So whether it's discovering and remediating various misconfigurations or enforcing consistent data security policies as users request access, the Lookout Cloud Security Platform enables you to freely onboard new cloud investments.

Accelerate mergers and acquisitions and keep the company running smoothly

Mergers and acquisitions are key avenues to business growth. But this also comes with a set of security challenges. Unifying disparate security policies and tools is a time consuming and costly process. And in that time, your organization may leave gaps in your security posture and unknowingly create misconfigurations.

With a unified platform like Lookout's, you can reduce friction when onboarding new systems. Because the platform has a simplified management console and a unified policy engine, any new app that's incorporated would automatically have your existing policies applied.

Not all platforms are created equal

It's encouraging that security professionals recognize new cloud-based challenges, but solving those challenges with point solutions is a piecemeal approach.

The security landscape has become considerably more complex. Streamlining security operations is critical to your ability to tackle this new environment. As you evolve your strategy and onboard new products, ensure that you are investing in platforms that have a holistic understanding of risks in cloud apps, private clouds, on-premises environments, as well as endpoint devices, including mobile endpoints.

The cybersecurity industry is telling organizations to enforce zero trust as a way to provide secure access to resources, but how do you go about doing that across all these different environments without inflating your security stack?

Lookout has a cloud-native platform that is built with data and endpoints in mind to take the complexity out of your IT security. Rather than pouring resources into new point solutions that don't talk to each other, you can focus on protecting data and empowering your hybrid workforce.

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 organizationsand 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 and follow Lookout on our blog, LinkedIn, and Twitter.

For more information visit
lookout.com

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