Lookout

# Standalone Tools Create Complexity:

## Why you need to consolidate your IT security

## Highlights

- With cloud apps and hybrid work, specialized tools create a management burden for IT and security teams and costly inefficiencies.
- Standalone products hinder IT teams' ability to analyze and stay ahead of evolving risks.
- To efficiently protect a fragmented infrastructure, organizations need to converge their security capabilities.

IT security used to be more structured. Users, devices, applications, and data resided within a controlled perimeter, where security hardware had full visibility and control over how that data flowed in and out.

But this defined environment has been replaced by a much more complicated landscape as organizations adopt cloud services, bring your own device (BYOD) programs, and hybrid work. Data is now scattered across countless locations, including SaaS apps, private enterprise apps, unmanaged devices, and cloud and on-premises repositories. At the same time, people are working from anywhere and using public networks to connect directly to corporate resources.

In an attempt to regain some of the controls they had, organizations have pieced together complex ecosystems of cloud-delivered products as they move down the checklist of modernizing their infrastructure. But this approach is neither scalable nor cost effective. Deploying specialized products, even if they are cloud-delivered, still requires additional resources to manage. Asking your IT and security teams to juggle more administrative consoles adds complexity to the environment, creating security gaps, poor end user experience, and room for human error.

> "89% of organizations aren't confident of their ability to protect sensitive data in the cloud."

– Source: Cloud Security Alliance

As you look to tackle these new security requirements, it's not enough to simply replace on-premises tools with cloud-delivered ones. At a time when your infrastructure is getting increasingly complex, it's critical that your security operation is streamlined. To get to that point, you must fundamentally shift away from the legacy mindset of deploying standalone products toward an integrated, platform-centric approach.

## Buying point solutions used to work, but not anymore

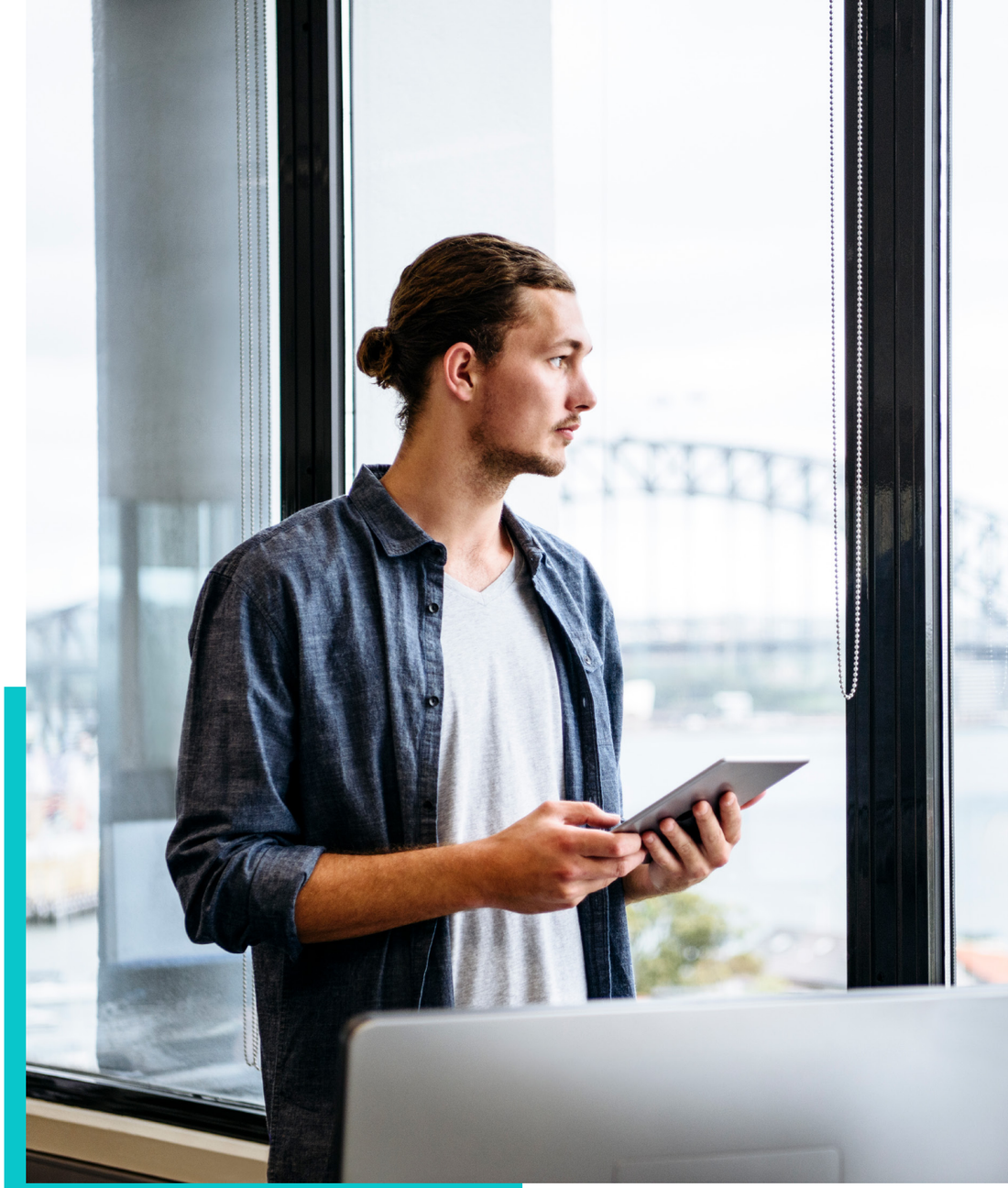
When all activities happened on a corporate network, you had most elements under your control and by extension had a better grasp of the risks you were faced with. As a result, security happened in a “defense in depth” approach where capabilities were layered on top of each other.

To reduce risks from endpoint devices, you handed out corporate-owned laptops that had rigid usage policies. Secure web gateways (SWGs) were deployed as pieces of hardware to inspect internet traffic to help block malware and malicious websites. Virtual private networks (VPNs) were used to provide remote access to a small percentage of the workforce. And data loss prevention (DLP) appliances, which looked at the traffic flowing out of the perimeter to ensure that your data didn’t get exfiltrated, were also common.

This was a costly endeavor, as each additional tool required resources from your IT and security team. But it worked for the relatively controlled environment you needed to protect.

The world isn’t so simple anymore. Organizations now rely heavily on the cloud, and workers are connecting from anywhere. And yet, the strategy of purchasing standalone products and running specialized security teams has persisted.

The result is that large enterprises now have an average of 76 security products deployed — a number that’s up almost 20% from 2019.1 In this same time period, the frequency and magnitude of breaches continue to rise.



> “Organizations using more than 50 security tools ranked themselves lower in their ability to detect and respond to an attack.”
>
> – Panaseer

# A siloed security approach creates complexity

The environment you're tasked with protecting is already quite complicated. Your data now resides in apps, and users are connecting via different networks and devices. As a result, the way to protect data is now the ability to monitor and enforce consistent policies across all these different places.

Purchasing additional tools doesn't actually provide you with that solution. Instead, standalone tools add an additional management burden to your IT team, and could create gaps that expose you to additional risk. It also entrenches the idea of siloed operations within your organization that limits your ability to detect and mitigate threats across your infrastructure.

**The challenges a siloed IT security stack introduces:**

## Reduced visibility

Each tool will likely give you visibility into a specific area, but not the whole picture. Without a way to integrate these insights into a simplified view, you have no way of understanding the risks you're exposed to.

## Strained resources

There is a global shortage of cybersecurity talent, which means security teams are already stretched. When you have separate consoles and policy frameworks, it becomes nearly impossible for any organization to keep pace with the increasing number of threat vectors.

## Exposure to additional threats

From misconfigurations to insider threats and ransomware, organizations are more prone to attacks when their environment becomes overly complex. Without a unified view of your organization, it's difficult for your IT and security teams to detect and mitigate these threats.

# Tackle complexity with a consolidated approach

Even as new use cases arise every day, it's important to take a step back and think about how you can most efficiently solve multiple challenges at once in order to achieve your team's ultimate goal — protecting the data.

With data scattered everywhere and users connecting to your resources from public networks and unmanaged devices, you need visibility into all these different activities and the ability to take actions on them in one motion. To do so, you need to think about driving efficiency with a platform-based approach.

**Here are the major capabilities you need to look for to reduce the complexity of your IT security:**

## Consolidated traffic monitoring

Rather than having one product look at data loss and outbound traffic while another monitors inbound traffic for threats, streamline the two. This grants a more holistic view of everything, such as user activities, data movement, and malware uploads. It also enables you to be much more efficient in how you identify threats and enforce policies.

## Continuous endpoint assessment

With hybrid work, people are using more unmanaged endpoints, including mobile devices. Whether your users have managed or unmanaged devices, it's critical for you to continuously monitor the health of these endpoints, which are exposed to a wide range of threats, including malware and phishing, you need continuous visibility into their health.

## Unified policy framework

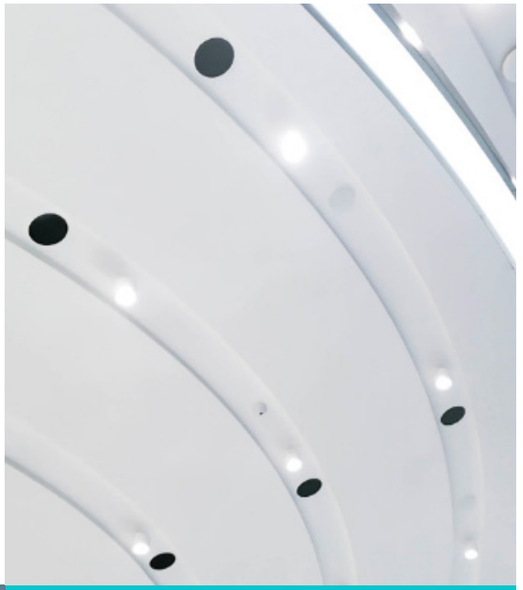
By integrating user, device, app, and data monitoring, you can more accurately enforce data protection policies. Being able to protect your data no matter where it resides will cut through the complexity introduced by cloud apps and a hybrid workforce.

# Streamline your security with a platform

The infrastructure you're tasked to protect is much more complex than when everyone worked inside offices. Which means the old tools — along with the old strategy — no longer apply.

As you enjoy the business benefits of cloud apps and hybrid work, you also need to rethink how you can better streamline your IT security. This starts with full visibility into all activities across your organization, not just in cloud apps, but also in private clouds and on premises. It should also extend to the endpoint devices your users are using, which are often not managed by your IT teams.

Solutions like the Lookout Cloud Security Platform are built with this converged approach in mind. With insights into user behavior, device health, and data, you're able to focus on writing and enforcing policies rather than managing a pile of tools that don't talk well to each other.



## 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