Lookout™

The Hybrid Work Dilemma:

How to Securely Work From Anywhere

lookout.com

Highlights

- Hybrid work has changed the way organizations think about security.
- Legacy tools aren't able to handle the granularity, scalability, and sprawl required to work in the cloud.
- Moving outside of the perimeter means losing visibility into users, endpoints, networks, and data.
- With more ways to collaborate, there's greater risk of losing track of data.
- Learn why you don't have to choose between security and access.

Work is no longer tied to physical spaces or corporate devices. In many ways, this has been a fundamental change for organizations. Because users aren't constrained to one physical location, or particular networks or devices, they can be more productive and efficient however is best for them. And now that organizations and their employees have gotten a taste of hybrid work, for most of you, there's no going back to the way things used to be.

With this change in working style also comes a change in security strategies. More than 60% of corporate data is now located in cloud applications, which means your sensitive information is distributed across different clouds and locations. And with data in the cloud, your users are able to access and share corporate information directly, sidestepping the perimeter-based security tools you used to rely on for monitoring and policy enforcement.

As you add more apps and services, your security environment as it stands today with on-premises solutions will only get less managed and complex. Not only is your data scattered, users are also connecting directly from the internet and using personal devices, including smartphones and tablets without following the traditional security protocols.

When you're in that situation, you may think you need to make a trade-off between security and access — locking everything down by default could make your operations secure, but it doesn't guarantee that people will have access to what they need to do their jobs. If you're working with a combination of remote workers, hybrid workers, and third-party collaborators like partners and contractors, that's simply not a feasible long-term solution.

Instead, IT and security teams are now faced with a critical question: How can we protect the organization's valuable data without hindering the productivity gained through hybrid work?

"Statista found that in 2022, more than 60% of corporate data was stored in the cloud — and that figure is only expected to increase."

Existing tools make you choose: security or flexibility

Your existing IT and security tools — as well as the strategies behind them — are simply not built for this new style of work. Appliance-based tools like firewalls, enterprise data loss prevention (DLP), and on-premises secure web gateways (SWGs) were deployed at the edge of perimeters to monitor and protect against incoming threats, but they required your users to sit inside a corporate office. To further control the environment, this strategy also asks employees to use company-issued laptops.

In that spirit, managed endpoint devices are the norm, where organizations use unified endpoint management (UEM) and mobile device management (MDM) solutions to look after corporate-owned devices or ask users to enroll personal devices into these management solutions. And while these tools can restrict users from accessing risky apps and push updates to ensure that operation systems are up to date, it also requires them to adhere to an extremely rigid working style. In turn, this eliminates the productivity boost that organizations have come to expect from hybrid work, and they ignore the reality of how organizations operate and employees get their work done.

The reality is that enterprise resources are now sprawled across countless cloud apps, and users are using the public internet and personal devices, including mobile devices, to connect to them. This means there are now countless threat vectors you need to keep tabs on. But simply managing devices with an UEM or MDM won't provide you real visibility into risks like phishing attacks or apps with risky capabilities. Some organizations have turned to a virtual private network (VPN) in an attempt to extend perimeter-based security's capabilities. But, not only does this slow down connections and add an additional layer of requirement to accessing resources, you still won't have insight into everything that's happening to your data.

If you don't want to make the choice between security and access, you're going to have to leave perimeter security tools and strategies behind.

Secure access has gotten more complicated

With perimeter-based security, you could be relatively sure that everything inside that controlled environment was secure and that users were given access under the assumption that they were trustworthy.

But with hybrid work, that assumption is no longer valid. Apps and services are now in the cloud, and your users and endpoints are using networks you don't control. As a result, there are new factors that require continuous monitoring to determine trustworthiness. Instead of taking an allow-or-deny approach, your security solution needs to have a holistic understanding of your users, endpoints, network, and data to help you stay protected.

Does your security solution have you covered?

Users

If you aren't sitting inside your network, it's practically impossible to assume they are who they say they are. Phishing attacks are on the rise, which means that account takeovers are a risk you need to be conscious of.

Endpoints

Users aren't just using corporate-issued laptops. People are using their own laptops, Chromebooks, tablets, and smartphones. Tools like MDM or UEM put basic safeguards around endpoints, but only on corporate-issued devices or select personal devices that choose to enroll. And these software don't have the insight you need into risks like malware, phishing, risky apps, or device vulnerabilities.

Networks

The internet is now your corporate network, so whether you're facing inbound threats like phishing or outbound threats like data leakage, perimeter-based tools won't be sufficient to detect them.

Data

Since your data is now sprawled across countless apps rather than within a corporate perimeter, you'll lose sight of the data you own as well as how it's being handled if you're relying on legacy tools.

Don’t let data security concerns hinder collaboration

The way we collaborate has changed dramatically due to hybrid work. You can share data really quickly now, but it’s also becoming easier to lose track of that data.

To promote collaboration in a hybrid work environment, you need to understand how your data is being handled. When you have control over your data, you’ll be able to minimize risk while enabling your users to work the way they want to.

These are the elements that you need to be aware of in order to retain that control:

> “According to the Verizon 2022 Data Breach Investigations Report, 82% of breaches involved a human element like lost credentials, phishing, intentional misuse, and simple mistakes.”

SaaS apps

Organizations use SaaS apps to collaborate — but without an additional security stack layered on top of them, they don’t have the same entitlement controls or data classification standards of on premises tools.

Third-party collaboration

We’re now using the same tools to collaborate with partners and contractors as we use internally. With everyone using tools like Slack, Microsoft Teams, Google Workspace, and more, it can be easy to share data with users who aren’t actually authorized to access it. And it’s also becoming easier to accidentally share corporate data using personal instances of these apps.

Shadow IT

When users take advantage of bring-your-own-device (BYOD) policies or use personal versions of enterprise apps, they are introducing shadow IT. Because IT departments have very little visibility into what happens on those apps and devices, and it’s easy to lose track of what’s happening to data. This exposes your organization to considerable risk that can be easily exploited.

There has to be a better way

If you stick with existing siloed, on-premises security tools and strategies, you'll eventually have to choose: enable collaboration and improve employee productivity, or keep your data secure?

But if you leverage the cloud and converge your previously siloed security capabilities into a unified platform, you won't have to make that tough decision.

A cloud-native, unified solution like Lookout Cloud Security Platform gives you visibility and insight into all activities, including what's happening in cloud apps, private apps, on the web, and in endpoints. With advanced data protection capabilities, you can understand the context of how your data is being used, granting access and enabling collaboration — without putting data at risk.

A unified solution also means your security environment becomes less complicated, and you'll be able to dynamically enforce policies across the entire enterprise without putting undue strain on your IT department.

Lookout™

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