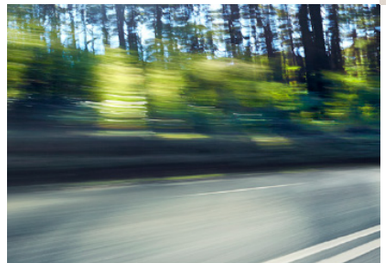
Lookout

Securing Hybrid Work Requires a Platform With Endpoint and Data Protection



Highlights

- In a hybrid work environment, you face a challenging trade-off between productivity and control when you use legacy tools.
- Regaining that control starts with regaining visibility into your apps, data, users, and devices.
- A unified, cloud-native SSE platform with built-in endpoint security and data protection enables you to protect data without sacrificing user experience.

Organizations now operate in a hybrid work environment, giving users the opportunity to work from wherever they feel the most productive. Using personal devices and public networks, employees are connecting to corporate resources, whether they're in the cloud or on premises. While the work-from-anywhere movement has been a business enabler for most organizations, there's a consequence that comes with this hybrid environment — you lose control over how your data is used and shared.

Legacy security solutions are designed for the hybrid work environment in such a way that they hinder productivity. If you're still relying on legacy tools, you may find yourself stuck with two bad options: keep the organization secure but hamper productivity or give your users free rein and open yourself up to threats.

Of course, neither of these options is a good solution. Instead, you need to find a security solution that can meet both workforce and IT requirements — empowering users to be productive in a hybrid environment without risking your data.

It’s all about data

Data is your organization’s most valuable asset, but in a hybrid work environment, it’s difficult to know how, exactly, that data is being used and where it’s being stored. Your legacy tools were great at providing insight into what was happening inside the perimeter, but between workers using personal devices to access corporate resources, the public internet being used as your primary network, and the proliferation of cloud apps, those same legacy tools leave you flying blind.

Instead of trying to manage a hybrid environment with legacy tools, you should turn to a security solution with advanced data security capabilities and adaptive controls that enable you to make intelligent access controls that don’t stand in the way of productivity.

Look for a solution that provides continuous and in-depth visibility into how your users are interacting with your data — especially when they’re doing so outside the perimeter and using devices you don’t manage. Your security solution should grant you insight into how your data is being shared across SaaS apps, private apps, and through the internet.

Secure unmanaged apps

Employees frequently sidestep your organization’s IT policies and use apps that haven’t been reviewed or allowed for use. This problem, known as shadow IT, is only a problem if you don’t have the right tools to detect when these apps are being used. Instead, you need a security solution that can discover unmanaged apps and bring them into the fold. This way, you get the best of both worlds: users are able to work productively with their preferred tools, and the organization can still keep close tabs on their data.

The dilemma of unmanaged devices

The challenge of visibility and shadow IT in hybrid work doesn't just apply to apps. In a way, bring-your-own device (BYOD) represents an evolution of Shadow IT that comes hand-in-hand with hybrid work. When employees are using their personal phones, tablets, and Chromebooks running modern operating systems to access corporate resources, it introduces more risk into your security posture.

Endpoints like mobile devices are appealing targets for bad actors and are frequently targeted by phishing attacks through emails or text messages. Unmanaged endpoints are also exposed to risks that are difficult to identify, including mobile apps that have vulnerabilities or risky permissions. And even though these devices are personal, they are still being used to access corporate data that you need to protect.

While the spectrum of mobile risk is expansive, there are some critical capabilities to cover when securing both managed and unmanaged devices in your fleet:

Detect and block connections to phishing sites

Analyze whether the network in use is secure

Detect out-of-date operating systems (OS) and app vulnerabilities

Assess the data risk posed by individual app behavior and permissions

Move to a unified, cloud-native security platform

To take full advantage of hybrid work, your organization should look for a security service edge (SSE) platform that includes these four solutions to provide visibility and security controls across cloud apps, private apps, internet access, and endpoints:

- Secure web gateway (SWG): A SWG prevents unsecured traffic from entering an organization's internal network. Traditional SWGs are an appliance that sit inside your perimeter, but a modern, cloud-delivered SWG can protect against threats even when users aren't on premises, while also blocking outbound data exfiltration.
- Cloud access security broker (CASB): This acts as an intermediary between users and cloud apps, giving organizations the ability to see what's happening in your SaaS apps and enforce corporate policies.
- Zero trust network access (ZTNA): A ZTNA can provide secure, remote access to your organization's private apps and data based on clearly defined access control policies.
- Endpoint security: As BYOD becomes commonplace, especially with mobile devices, robust endpoint protection that is part of a broader platform is essential to ensure that you take into account device health while making access decisions.

Advanced data protection capabilities

Ultimately, the platform you choose should secure your data and the way your employees access it. The following data protection capabilities should be integrated throughout the framework to keep data secure wherever it goes:

- User and entity behavior analytics (UEBA): This process monitors normal user behavior and flags unexpected changes from the usual pattern, helping detect insider threats and compromised accounts.
- Data loss prevention (DLP): When users seek access, modern DLP solutions can automatically identify and classify that data, keeping your organization's sensitive information secure.
- Enterprise digital rights management (EDRM): EDRM automatically encrypts data when it's downloaded, ensuring only authorized users can access it.

Choosing the right platform matters

There are several SSE platforms out there to choose from, but they aren't all created equally. Some lack the advanced data protection tools or don't have an endpoint security solution.

Lookout Cloud Security Platform is a fully integrated SSE solution that enables you to stay secure across cloud apps, private apps, internet traffic, and managed and unmanaged endpoints. Lookout Secure Internet Access, Lookout Secure Cloud Access, and Lookout Secure Private Access — combined with Lookout Mobile Endpoint Security — provide you full visibility and control over your data. Native advanced data protection capabilities ensure precise policy enforcement, which can dynamically evolve so they don't get in the way of productivity.

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