Lookout

# Why Hybrid Work Requires a Data-Conscious Security Strategy

## Highlights

- With work from anywhere, your data is more spread out than ever, across apps and endpoints you may not fully control.
- Cloud apps and remote users increase risk of intentional and accidental data leakage and exfiltration.
- It's difficult to know how your data is being used when users, endpoints, apps, and data all reside outside your security perimeter.
- To protect sensitive data while enabling hybrid work, you need to be able to automate policy enforcement with precision.

The days of work being tied to specific locations or devices are over. With the adoption of cloud technologies, users can now work and collaborate from anywhere. Using public networks, they connect directly to your corporate resources via personal devices.

This is a great leap forward for workplace productivity, but it's also introduced new threats that are vastly different from the ones from the past. Legacy security and data protection strategies were designed when there was a defined perimeter, which meant policies were much more rigid and typically only allowed or blocked an action with no in-between.

Now that there's no perimeter, many organizations continue to enforce these access-based policies. Not only is this contradictory to the nature of hybrid work, but focusing on access doesn't keep your data protected. To continue giving your employees the flexibility they prefer, you need a precise yet dynamic way to protect your data. This requires real-time insights into what's happening with your data and controls that provide both seamless and secure access.

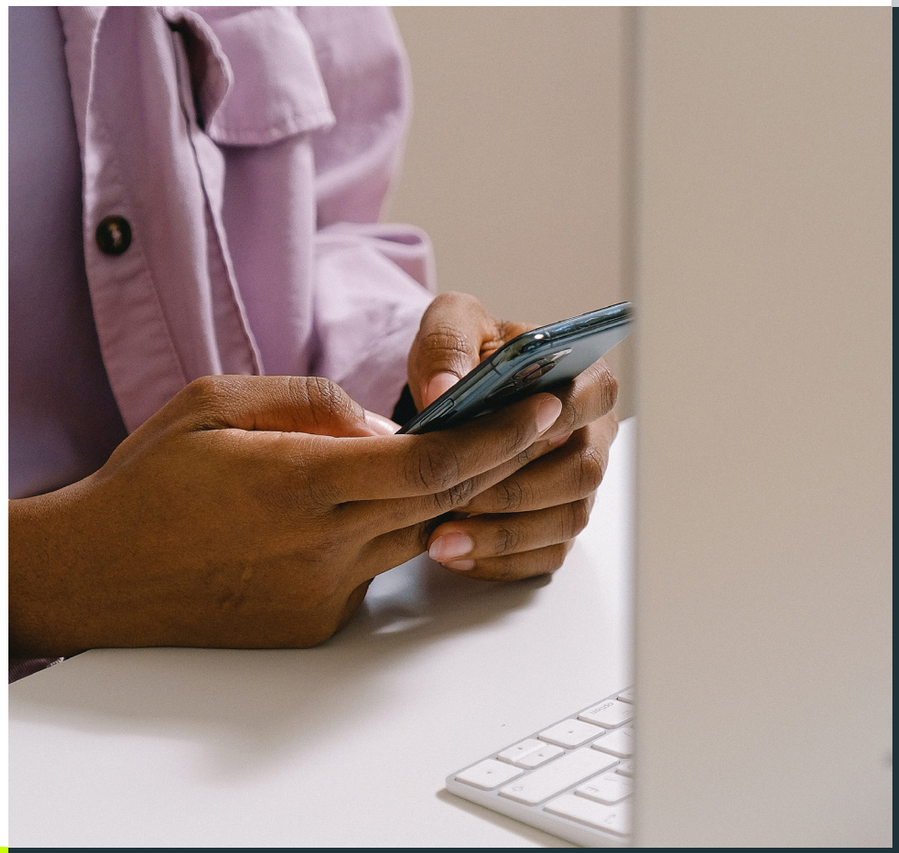
If you need to modernize your data protection strategy and aren't sure where to start, this e-book proposes a framework for protecting your data without hindering user productivity.

# Focus on the data

Before you can enable your workforce to securely work from anywhere, you need to have a plan. Hybrid workers require seamless access to what they need, but security has traditionally been a hindrance to access. Instead of trying to recreate your perimeter for a hybrid setting, keep users productive and secure by focusing on how data is accessed and handled.

You may have heard the security industry throwing around the term “zero trust” as a way to provide secure access for hybrid work. This is the idea of not giving any entity access to your corporate data until their risk level has been verified and accepted. But zero trust can be applied to anything in your security framework, which means it can get very complicated to enforce. To support work from anywhere, you should think about the end goal of securing your hybrid work force — and that’s protecting your data.

So how can you prevent your data from being accidentally leaked or being maliciously exfiltrated? The key is to follow it throughout its life cycle. If data is being stored across cloud apps or being shared with third parties, you need to maintain visibility and control over your data. At the end of the day, all of your policy enforcement should revolve around protecting data.



# Security everywhere starts with telemetry

Your data is no longer being handled within controlled environments, and legacy tools are woefully unprepared to tackle this level of data sprawl. Third-party partners and employees leaving the company can easily walk away with your data, and even corporate-issued devices are using networks that are outside your control.

Data management becomes even more elusive when you acknowledge that the SaaS apps you deploy each have their own controls in place, and BYOD policies can introduce new vulnerabilities and unsafe apps. With all these variables, it's incredibly difficult to get a holistic view of what's happening with your data.

**To enforce data protection policies across these complex environments, you need insight into all activities, including:**

## Device health

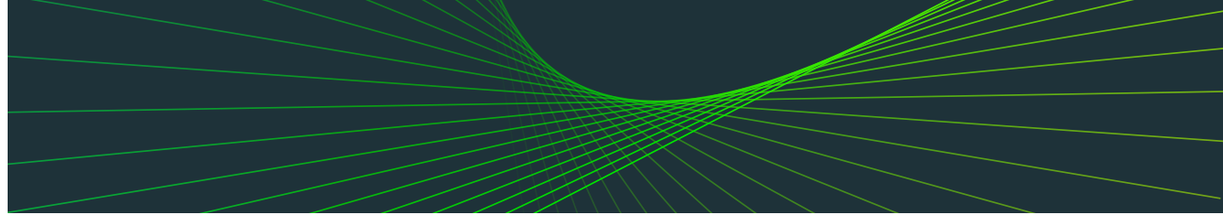
Mobile devices are a key part of hybrid work. This means your data is exposed to mobile threats including phishing, unsecured networks, malware, and risky apps. To protect your data, you need to provide access based on the health of the devices being used.

## User behavior

Users connecting from anywhere, which makes it difficult to know whether an account is being used by the actual authorized user. Data sharing is very easy when using the cloud, which means you'll only be able to detect insider threats — whether it's a case of accidental leakage or malicious exfiltration — if you have a good understanding of baseline user behavior.

## Data sensitivity

Awareness of data sensitivity is what will help you pull the data centric approach together. In order to efficiently provide access that's precise and doesn't over-entitle users to data they don't need, you need to understand the value of the data that's being requested so you can apply appropriate restrictions and map it to the risk levels you're seeing from the user and their device.



# An intentional approach to access

In order to protect data without hindering productivity, you need to be very intentional about how you give access and change that access based on context. And this will require you to continuously monitor things like device health, user behavior, and what kind of data they're interacting with.

**These are the controls you need to have in place in order to grant the right amount of access to your users:**

## Microsegmentation

Know what your users need access to and provide exactly that — no more and no less. There's no need to connect them to your entire infrastructure, which is what you used to do when everyone and their devices sat inside a perimeter or were using a virtual private network (VPN).

## Adaptive access

Don't take a binary allow-deny approach to access. Look at the health of the device alongside user behavior and location and map it to the acceptable level of risk for the different types of data you value. If a user wants access to a document that has no personally identifiable information (PII), you can take more risk with access than if a user was asking for access to a document with confidential financial information.

## Precise data controls

You should also be able to implement restrictions beyond denying access. These might include encrypting the data and requiring step-up authentication or disabling downloading privileges.

## Selective restriction

Rather than stopping someone from getting work done altogether, you should be able to automatically restrict portions of a data file based on sensitivity levels using features like redaction and masking.

# Cloud-based platforms are the path to securely enabling hybrid work

Static controls worked fine when everyone was working inside the perimeter, but that's not the case anymore. Appliance-based security is no longer enough to keep your organization and your corporate data secure. Cloud-based solutions provide flexibility and scalability that can stretch into your unmanaged devices and cloud apps, enabling you to stay laser focused with what's happening with your data.

However, keep in mind that you can't simply exchange those on-premises tools for cloud-delivered versions. If you keep your security stack fragmented, you will still have a hard time getting the insights to enforce smart zero trust access.

To stay both productive and secure in a hybrid environment, you need a comprehensive platform like the Lookout Cloud Security Platform. This approach enables you to enforce policies consistently across cloud apps, private apps, and internet activities, and advanced data protection capabilities ensure that your organization can keep data secure.

## 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