How to Build an **Effective Data Security Strategy**

Five steps towards full visibility
and control across your organization

Lookout®

It’s no longer business as usual for cybersecurity

Dramatically accelerated by the pandemic, your move to the cloud has fundamentally altered your organization’s relationship with users, apps, and data and how they interact with each other. In terms of productivity, this has unlocked unprecedented ways for anyone, regardless of their location or device, to stay productive and collaborate. But this also deconstructed the many assumptions that we had about cybersecurity. With very little residing exclusively within a defined perimeter, your sensitive corporate data is now exposed to new risks.

Operationally, this means your IT and security teams cannot rely on specialized appliance-based tools, as they have little insight into cloud activities. A recent survey showed that 66% of IT professionals have seen an increase in security incidents and requests due to remote work.[1] In a different 2021 report, 63% of respondents said their organization had sensitive data exposed in the cloud.[2]

1. Ivanti, “Remote Worker Survey Report,” June 2020
2. Ermetic, “State of Cloud Security 2021 Report Results,” June 2021

Table of contents

Lookout®

Why is protecting data in the cloud so hard?

Protecting data may sound simple, but it's not, especially when you're juggling multi-cloud environments and a dispersed workforce.

Your IT infrastructure has become very complicated, where there's a product for every use case. Some are used for fixed and mobile endpoints; some to provide access controls to apps, and to identify and authenticate users; and some to protect internet access. No wonder large enterprises have an average of 76 security products deployed in 2022 – a number that's up from an already astonishing 64 security products deployed in 2019.[3] Each product was likely purchased individually to solve a single problem, which means they operate in isolation and don't communicate with each other.

What this means is that silos emerge within your organization. Your IT and security teams have to divide and conquer to manage separate policy frameworks and learn how to use the different management interfaces or consoles. Not only does this make it very difficult to get a holistic picture of how your sensitive data is handled, it also makes it difficult to enforce consistent policies, which leaves gaps and potential for human error.

76: The average number of security products an enterprise has deployed

3. Panaseer, "Security Leaders Peer Report," November 2021

Maintaining the status quo does not protect your data

It's tempting to just let whatever you have deployed stick around – after all, you've already gone through the trouble of procuring a budget, allocating personnel and deploying them. The reality is that the current situation is likely more costly to you, both in terms of operating costs and security risk. With a patchwork of tools, your team spends most of their time maintaining your complex infrastructure rather than working on strategic issues and improving your security posture. They quickly burn out, leaving even fewer people to do an increasingly difficult job.

The status quo also means a poor end-user experience where your employees have to install multiple agents on their devices. They not only have to deal with a wave of notifications, but there are also complex restrictions and rigid policies that hinder their ability to work.

And like what's already mentioned above, siloed security tools provide very poor visibility and disparate controls. This makes it almost impossible for IT and security teams to determine if there is a major attack underway or any consistent way to enforce policies and ensure your data isn't compromised.

How to protect data in a cloud-centric environment

At the end of the day, your IT and security team's job is to ensure that your organization's sensitive data is secure. To do so as you embrace the cloud, there are three buckets of actions that you should be able to take:

- Consolidate and modernize your IT security infrastructure in a way that streamlines operations and reduces costs
- Provide dynamic access to your hybrid workforce, ensuring a better end-user experience while protecting your sensitive data
- Detect and mitigate cyber threats efficiently and proactively so that your organization is secure from emerging threats and data breaches

At a high level, the only way to fulfill these requirements is by deploying an integrated platform that can protect your users, endpoints, apps and data. But this might sound a little too abstract. To break it down, here are five steps you should take to ensure that your data is protected in the cloud:

Step 1: Secure your endpoints (both managed and unmanaged)

In the past, securing traditional corporate-owned endpoints such as laptops and desktops was enough, especially when you had a defined corporate perimeter. Not anymore. Personal and unmanaged devices like smartphones and tablets have just as much access to your sensitive data as those other endpoints and are increasingly being used by your employees to stay productive from anywhere.

How much risk do these unmanaged mobile devices introduce? The answer is a lot more than traditional endpoints. For starters, they sit squarely between a person's personal and professional lives, which means they are more trusted and therefore more prone to social engineering. In addition, there are countless mobile apps with messaging functions that can be used to deliver phishing attacks – and any of them could steal login credentials or deliver malware. And because a device could have countless apps installed and easily connect to any network, exposure to app and network threats is much higher.

To truly protect your sensitive data, you need the ability to protect against a wide spectrum of endpoint risks. Especially with mobile endpoints, you need a platform that leverages rich telemetry and machine intelligence. This will enable you to detect and respond to known and unknown threats without the need to conduct intrusive and resource-intensive scans.

66% of IT professionals saw an increase in security incidents and requests due to remote work

Step 2: Provide dynamic access based on continuous risk assessment

The reality is that risk levels, both of endpoints and users, are constantly changing. To protect sensitive data while enabling seamless access, you need both in-depth and real-time visibility as well as controls that can take advantage of that telemetry.

For endpoints, this assessment includes: is the device jailbroken or rooted; does it have any risky or malicious apps installed; and is it connected to a vulnerable network? User risk postures would include data points such as: are they trying to access corporate apps at an unusual time of day or from an unexpected location; and are they deviating from their usual pattern of behavior and putting data at risk?

It's only with this continuous assessment that you can protect data while empowering your work-from-anywhere initiatives. By having this integrated into a platform, you can build precise and dynamic policies that efficiently enforce zero trust across your organization, whether it's access to cloud apps, private apps or the internet. This is not just about binary, deny-or-accept access; it's ensuring that access is appropriate to the risk levels of the user and endpoint.

If a user is exfiltrating a large amount of sensitive data, this is obviously a malicious activity that indicates an insider threat or compromised account and access should be shut down. But what if a user is using an unmanaged device that's connected to an unsecured public Wi-Fi? You could decide that the user gets view-only access because the data has a medium sensitivity level. This way they can continue to stay productive, without the risk of data exfiltration or accidental data leakage.

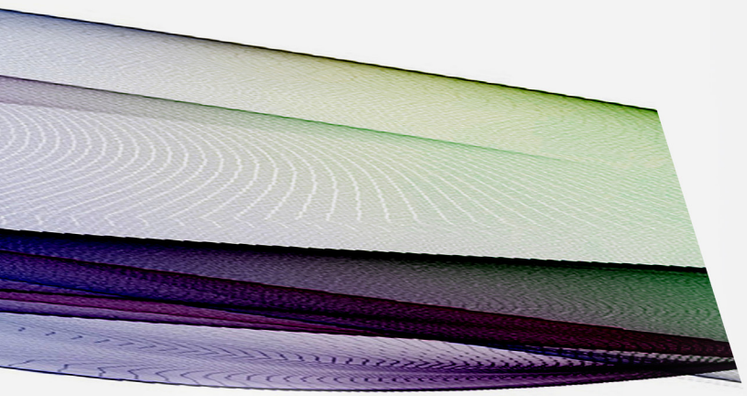
Step 3: Secure access to your private apps

While we tend to focus on software as a service (SaaS), apps that you have inside data centers or private cloud instances need to be part of your data security strategy. With work from anywhere, access to these apps is just as critical and requires the enforcement of zero-trust principles.

Just as you would enforce data protection policies in the cloud, private apps benefit greatly from a platform approach where risk levels of endpoints and users, as well as the sensitivity level of data, are considered. Traditionally, organizations relied on identity access management (IAM) and virtual private networks (VPNs) as gatekeepers to an organization's entire infrastructure. This can be quite dangerous. By only asking for a password and a second factor of authentication to enable network-wide access, you're giving compromised accounts or malicious insiders the ability to move freely within your organization. This is why you need the ability to enforce zero trust across your organization, including private apps.

With a platform that extends into private apps, you will be able to provide dynamic access that protects data because you have data points into everything from user behavior, endpoint risk postures to data sensitivity. And because the policy engine and monitoring is within a unified platform, your IT and security team doesn't need to spend any extra time rewriting policies and assessing security data on a separate console.

63% of organizations have sensitive data exposed in the cloud



Step 4: Protect users from hidden threats in internet traffic

The internet used to be an occasional destination for your users when everyone worked inside a perimeter. Now, it has become your default corporate network. To protect your workforce from internet-based threats, you need the ability to intercept and detect malicious content such as phishing or malware from all web traffic, something that your perimeter-based security can no longer do.

This requires an integrated platform with inline controls and a comprehensive threat intelligence engine, which will enable you to quickly detect the latest threats – whether it's zero-day attacks or ransomware being uploaded – and remove the content before it reaches your network or devices.

This web protection should also extend to phishing websites or destinations that go against compliance requirements or your corporate acceptable use policies. To be effective, the platform should have access to website blocklists that indicate suspected malicious IP addresses and URLs.

Step 5: Gain control over unsanctioned SaaS apps

So far we've talked about apps that your organization owns. But those aren't the only software interacting with your data. Your employees are likely using apps that you don't know about, including one-off SaaS apps or personal versions of enterprise apps, such as Google Workspace or Microsoft 365. You will likely also encounter partners' and contractors' own apps that end up with copies of sensitive data that you shared with them. With data moving freely in the cloud, it's very easy for information to leak out or have someone intentionally exfiltrate your data.

The reason these unsanctioned apps, also known as shadow IT, exist is due to the productivity and collaboration they enable. But you need the ability to identify and monitor their usage, and enforce security controls. Just as you have parity in visibility and control between your cloud apps and private apps, you should have the same for these unsanctioned apps. Ideally, that same inline proxy would stretch across your entire organization so you can centralize policies for all apps.

Cybersecurity shouldn't adhere to arbitrary boundaries

Cloud migration has ushered in massive changes to how we work and operate an organization. With the ability to access resources from anywhere, employees can now work and collaborate from anywhere and on any device. Your IT teams can also deploy software as needed without incurring any additional resources.

But these opportunities also come with security challenges. Your data is now sprawled across countless apps and being accessed by endpoints and networks you don't manage. Employees, contractors and partners are also bringing their own unsanctioned apps into the mix. On top of all this, traditional security tools have become obsolete as users, apps and data no longer reside exclusively within corporate perimeters.

We've introduced five major areas you need to address in order to protect your data in this environment. The key takeaway is that all of them require a unified platform approach. Many organizations have moved away from perimeter-based security and started deploying cloud-based tools. But often this is done with a siloed mindset, where products are purchased to solve a singular issue.

Your users and data do not adhere to arbitrary boundaries. Your security strategy shouldn't either. With a unified platform that's built on a single inline proxy, you should be able to have full visibility and control over all your cloud apps, private apps and web usage. This solution should also have continuous insights into your users, the endpoints and networks they use, as well as the sensitivity level of the data they seek to access. It's only with this rich telemetry that you can efficiently enforce zero trust in a way that protects your most valued assets while enabling work from anywhere.

If you'd like to get a free evaluation of your risk, we can help.

Lookout®

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit www.lookout.com and follow Lookout on its blog, LinkedIn, and Twitter.

Lookout