Don’t Leave Behind Cybersecurity **in Your Digital Transformation**

Is your organization equipped to handle cloud-based threats?

Lookout®

The cloud is a double-edged sword

Migrating to the cloud has become a no-brainer. By passing down the maintenance costs to the service providers and enabling users anywhere access to resources, you're able to streamline operations, reduce costs and boost productivity. It's no wonder that 96% of organizations have moved some of their assets to the cloud,[1] which now hosts more than 60% of all enterprise data.[2]

While the cloud provides clear benefits, it also creates unique challenges. In fact, almost 80% of organizations have experienced a cloud breach between 2020 and 2021.[3] With data sprawled across countless apps and your employees connecting from any network and on any device, you are now faced with vastly different challenges than when everything resided within a corporate perimeter. You now need to ensure that each of your apps is configured correctly while at the same time keeping tabs on users and endpoints operating outside your sphere of influence.

As your organization continues to go through a digital transformation, cybersecurity needs to keep pace. This will require your security operations to go through the same cloud transformation as well. To help you navigate this process, we've compiled the major steps you need to take.

96% of organizations have moved assets to the cloud

[1] Flexera, "Flexera 2022 State of the Cloud Report," March 2022

[2] Statista, "Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2022," March 2022

[3] Ermetic, "State of Cloud Security Maturity 2022," August 2022

Table of contents

Assess your current security posture

Thinking about cloud-delivered security solutions is a good start. But to fully understand whether your organization is equipped to tackle cloud threats, you need to think about your security capabilities from all angles. Below are questions you can ask yourself to understand your team's ability to protect assets and mitigate threats in a cloud-first environment.

How much visibility and control do you really have?

Many of your resources are now spread across infrastructure you don't own and outside the visibility and control of your perimeter-based tools. There are two major areas to consider as you assess your security posture: users and endpoints, and configurations and responsibilities.

Users and endpoints: The risk levels of these entities are constantly in flux, which makes them difficult to control, especially as they connect from environments you don't own. Does your organization have the ability to tell the difference between normal behavior and risky or malicious behavior? Would you know if an endpoint is attacked by a phishing message or when malware is delivered?

Configurations and responsibilities: While the move to cloud services means that many software management responsibilities now reside with the service provider, you need to understand where that boundary ends. At the end of the day, your IT and security teams are still in charge of protecting your identities, apps and data. Some 80% of organizations find that they need to add an average of 3.3 new roles and functions just to deal with the cloud.[4]

Do you know exactly how your data is being handled?

The cloud is designed to make data sharing easy – you can share information with a click of a button or a link. But this means that data can easily be leaked out or accessed by unauthorized users. So as users collaborate across your multi-cloud environments or share data with third parties using their own apps, do you have visibility into how your data is being handled and by whom?

Do you have a handle on access, configurations and patching?

Cloud-based threats are rapidly evolving, taking advantage of weak credentials or unprotected ports. With everything interconnected, an attack can easily start on premises and then move laterally throughout your network, including cloud services.

The reverse can also happen, with an attack compromising a cloud app and then breaching your corporate network.

Breaches can occur due to a number of issues. This could include misconfigurations, overly permissive identities, unpatched vulnerabilities, as well as human errors. An example is the SolarWinds attack in which the bad actors first gained access to on-premises data centers before pivoting to Microsoft 365 and Azure environments.[5]

Would you know if you're out of compliance?

With requirements such as GDPR, HIPAA, PCI-DSS and other mandates, data privacy and confidentiality are top of mind for many organizations. Equally important is the need for you to protect confidential corporate data, like intellectual property, that lets you maintain a competitive advantage.

With the dozens of cloud apps that your organization is likely using, as well as a large number of users and endpoints sitting outside corporate perimeters, it has become more difficult than ever to stay in compliance. You need to make sure that you have the ability to enforce compliance policies across your organization, including on unmanaged endpoints as well as apps that can be considered shadow IT.

Almost 80% of organizations experienced a cloud breach between 2020 and 2021

[4] Foundry, "Cloud Computing Study 2022," April 2022

[5] Pierluigi Paganini, Cybernews, "SolarWinds hack: the mystery of one of the biggest cyberattacks ever," September 2021

Modernize your IT and move to the cloud securely

Protecting your move to the cloud begins by moving away from legacy security strategies. Back when users, data and apps all resided within perimeters, organizations deployed specialized tools as new use cases arose. The result is that a typical organization now has an average of 76 security products.[6]

This siloed approach is not only costly to operate and a drain on your security team, but it is also ineffective when dealing with rapidly evolving threats. As data is sprawled across apps, and users and endpoints are connecting from anywhere, you need to converge your security capabilities to handle cloud-based risks.

By having a single platform in the cloud, you have a single place to monitor and enforce policies. This also provides you with the scalability and computing power to automate detection and response that protects data without hindering productivity.

To ensure your organization has the capabilities to securely move to the cloud, these are the three steps your security solutions should be able to take:

[6] Panaseer, "Security Leaders Peer Report," November 2021

Step 1: Ensure that only authorized users can access your apps and data

Today you deal with a broad universe of users, such as employees, contractors and partners. With cloud apps, any of these users could access your corporate assets from anywhere and any device. The positive is that this speeds up collaboration. But it also means that you need accurate controls to ensure that data leakage or malicious data exfiltration don't occur.

To precisely provide the access that's required, you need the ability to monitor all users' behavior, the risk levels on their endpoints and how they interact with your apps and data. This is where a cloud-delivered platform comes in, leveraging machine intelligence to efficiently analyze all these different data points to quickly mitigate any threats. With this rich telemetry, you're able to implement dynamic zero-trust access, whereby users are given seamless access to what they need while ensuring that sensitive data isn't at risk.

Step 2: Leverage automation to protect your cloud-based apps and data

In addition to securing data from the end-user side, you also need the ability to protect the data itself, regardless of where it goes. This involves classifying data by its sensitivity, encrypting it while at rest and in transit, and changing sharing settings on the fly. Your data protection should also expand beyond binary allow-and-deny decisions. The right platform should be able to redact keywords, apply watermarks, or encrypt data so that it is protected even when distributed offline.

This step also involves making sure that your cloud apps and infrastructure are properly configured. Misconfiguration is a leading cause of data breaches.[7] As Gartner has stated, "…at least 95% of cloud security failures will be the fault of the organization."[8] With the right platform, you should be able to efficiently assess and fix any misconfigurations of your apps and infrastructure. It also needs to coordinate and communicate with the various elements of security and compliance, including user access, data protection and application security.

80% of organizations said they need an average of 3.3 new roles and functions to deal with the cloud

Step 3: Protect against internet-based threats such as phishing and malware

In this cloud-first environment, your corporate network is replaced by the internet. And with the proliferation of bring-your-own-device (BYOD) programs and work from anywhere, you now have little visibility into the threats coming in from the web.

One of the most common internet-based threats is phishing, which uses social engineering to trick your users into giving up their login credentials. This is especially dangerous on mobile devices where there are countless avenues to deliver the attack, including messaging apps, social media platforms and SMS messages. Once an account is compromised, an attacker can quietly enter your infrastructure and move laterally. Another threat is malware, which is most commonly delivered by cloud apps.[9] Unmanaged endpoints can upload malware to the cloud where it can then lead to an infection across your enterprise. Malware can also move from apps to other endpoints or to another cloud service.

To combat both threats, you should implement a phishing and malware detection solution that makes use of big data and machine intelligence. This is something that requires a cloud-delivered platform with visibility into devices, apps, web domains as well as the latest threat intelligence.

[7] Identity Theft Resource Center, "2021 Annual Data Breach Report," January 2022

[8] Gartner, "Gartner Survey Says Cloud Computing Remains Top Emerging Business Risk," August 2018

[9] Jonathan Greig, ZDNET, "Even after Emotet takedown, Office docs deliver 43% of all malware downloads now," July 2021

The importance of a cloud-delivered platform approach

When you rely on a cloud-delivered platform, you reduce the complications associated with implementing, configuring, updating and managing multiple security tools across your infrastructure. A single unified management console removes the uncertainty posed by multiple disjointed alerts, each of which your team needs to manually investigate and resolve. In a platform, all this information converges, allowing you to keep full control over your data while providing intelligent enforcement of security policies to protect your data.

Security should be just as much about enabling productivity as about protecting your data. Modernizing your IT infrastructure with a platform that uses machine intelligence delivers a better user experience because it knows what users need to access, as well as what is normal behavior. It can spot suspicious activity and dynamically implement security enforcement controls when needed. This means dynamic and granular zero-trust access that protects data without creating friction for your legitimate users.

The steps we outlined in this paper all require this converged approach. With better visibility and context across your entire environment, you can efficiently protect your users, data and apps. You're also able to guard against emerging threats, limit exposure and improve detection and response. Ultimately, it provides comprehensive protection against the entire threat landscape through a streamlined, modernized infrastructure that makes life easier for your team and your users alike.

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

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®