Whitepaper

You Rushed to the Cloud

Now What? 5 Security Steps for Cloud Clarity

cbi
A CONVERGE COMPANY

CHECK POINT™

Countless companies made hasty cloud transitions to enable their remote workforce during the onset of COVID-19. Their stories are familiar—the pandemic hit, they didn't have enough VPN licenses to allow all the new remote users into their environment, so they migrated to the cloud in as little as a week. The cloud has enabled their business and operations ever since, but they have no idea how secure their environment actually is.

This predicament is completely understandable. With the rush to keep the business running in unprecedented circumstances, there was no time to plan, organize, or document assets, users and connections. But now, more than two years after the pandemic forced the remote workforce shift, many companies remain in a state of uncertainty about their cloud security status—unsure of who their users are, where their vulnerabilities are, or whether their data is exposed somewhere, just waiting to be uncovered.

Lacking clarity over your cloud infrastructure is a precarious state to be in. As the cybersecurity adage goes, if you don't know what you have, you can't secure it. It's no surprise that cloud incidents are increasing: According to Check Point's 2022 Cloud Security Report, **27%** of organizations have experienced a public cloud security incident, **up from 10%** the previous year.

This rise might be partly due to a common misconception about the cloud, which is that the cloud is inherently secure. In reality, "cloud" just means the data is stored on someone else's server. And while big cloud providers like AWS, Azure and Google Cloud have earned their reputation for secure infrastructure, the shared responsibility model means customers of those providers are held accountable for the security of the data in the cloud. That means controls like application management, encryption, and network configuration are the responsibility of the organization using the cloud—not the cloud provider.

If your organization finds itself uncertain about its cloud environment, the best thing you can do before signing on to the newest cloud security solution is to start where you are. That means assessing what you have in the cloud so you know your current status. Only with a complete understanding of where you are now can you develop an effective plan to get where you want to be.

With that in mind, here are our recommendations for organizations wondering how to start getting a handle on their cloud security.

1. Inventory Your Users

Security is all about users and where and how they're sharing data. Know who should be using your cloud, and revoke access for those who should no longer be. This means auditing your users and disabling accounts for former employees and contractors. Additionally, it's a good idea to inventory account access for each current user. This helps ensure that when an employee moves on, all of their accounts are disabled in addition to their main user account. This information should be logged to help ensure no accounts are left out in the open, waiting for discovery by threat actors.

2. Review Your Admins

Know who is administrating your cloud. Find out who your admin users are and assess whether those users truly need admin privileges to do their jobs. An excess number of administrator accounts violates the principle of least privilege, which states that a user should have no more permissions than needed to do their job.

On the other hand, to ensure separation of duties, you should always have more than one cloud administrator. If one admin account is lost or compromised, another admin user should be able to step in to perform tasks.

Once you have tightened up your admin users, enforce multifactor authentication [MFA] for those accounts. While MFA is a good idea for all users, it's a must for admin accounts.

3. Check Your Access Methods and Connections

One of the biggest questions companies ask when they move to the cloud is how to handle remote connections. Some companies choose to have users log into their environment with their Microsoft account, while other companies have users authenticate via an identity provider such as Okta or Duo. Companies going the more traditional route will use a VPN, through which users connect to the actual office branch, which then connects to the cloud. Whichever connection method is used, it must be secured and audited. Companies should determine which devices or people can connect to the cloud service provider and how and when they are allowed to connect.

Further factors to consider are access rules such as geolocation. For example, if you don't have Russia-based employees, you should be suspicious if a user is logging in from Moscow in the middle of the night. Be sure to establish rules around the types of connections allowed and set up logging and alerting to flag when these connections deviate from expectations.

4. Inventory Your Assets

Cloud assets are things like servers, virtual machines, containers, compute instances, and S3 buckets. A recent analysis found that 90% of all devices in organizations today are cloud-based, with physical devices accounting for less than 10% of total devices in the modern organization. When we ask companies how many assets they have in the cloud, we know that those who give us an approximate number have been doing their homework. But many companies don't know.

It's important to understand what types of assets your enterprise has in the cloud and how they are secured. Is data protected with proper configuration settings and encryption? Are data loss prevention policies in place, such as rules preventing users from downloading a sensitive file? Auditing your assets and their controls will go a long way towards gaining clarity in the cloud.

5. Consider Adopting a Zero-Trust Approach

Accounting for your users, assets and connections is an important prerequisite on the journey to a zero-trust security approach. Zero trust has become a popular buzzword, but at its core, it's a framework that enforces the "rules of the road" in the company environment for each user, device and connection.

If you imagine your environment is a system of roadways, a zero-trust framework checks whether each user meets the criteria to be on the road and for the routes they attempt to access. All drivers must have a valid license to be allowed on the road. If a driver tries to enter a tollway without payment or an HOV lane without a passenger, zero-trust controls stop them. Zero trust is the solution for today's complex, distributed environments, where devices and users no longer fit neatly inside a defense perimeter.

Before you can enforce the rules of the road, you must map out your system of roads, streets and highways, what resources they lead to, and who and what is using them. Once you've defined and cataloged the parts of this system, you can begin setting up policies and rules that determine who is allowed to access what and adopt the technologies that enforce these rules.

Start Where You Are

Every organization is at a different point in its cloud journey. When it comes to securing your cloud, there's no one-size-fits-all solution. With cloud expertise in short supply, reaching out to an experienced third party for help assessing your cloud state and risk landscape is always recommended. However you accomplish it, taking stock of your current cloud environment will lay the groundwork to create a roadmap to where you want to be in the future and help ensure you procure the appropriate tooling to get there.

About CBI, A Converge Company

Clients rely on CBI, A Converge Company, to meet their unique cybersecurity needs with industry-leading solutions and expertise. Our services-led team uses an advisory approach to help clients safeguard their traditional and cloud infrastructure, critical assets, users and brand. We combine over three decades of expertise with Converge's IT solution portfolio to deliver comprehensive services and solutions to elevate corporate security, advance business outcomes, and drive competitive innovation.

Learn more at cbisecure.com.

About the Author

Leon Malkowych | Director
CBI, A Converge Company

Leon brings more than 15 years of network and security expertise to his role as Director of Architecture, Implementation and Management Services with CBI.

He oversees the strategy, development, and delivery of services designed to help organizations align cybersecurity capabilities with desired business outcomes and strengthen defenses across people, process, and technology. He has extensive experience leading teams of highly experienced engineers, and helping clients build and mature their cybersecurity posture.

About Check Point Technologies Ltd.

Check Point Software Technologies Ltd. is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from 5th generation cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers multilevel security architecture, "Infinity" Total Protection with Gen V advanced threat prevention, which defends enterprises' cloud, network and mobile device held information. Check Point provides the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

Learn more at www.checkpoint.com.