Whitepaper

Your Data Is Not Innately Secure Or Insecure In The Cloud

cbi
A CONVERGE COMPANY

CHECK POINT™

Just five years ago, organizations were generally leery about the cloud.

Back then, the common perception was that moving to the cloud—entrusting another company to protect mission-critical data and development—was risky and perhaps even irresponsible. Cloud marketing teams were tasked with convincing organizations that their data would be secure on someone else's servers.

Times have changed. With the pandemic forcing organizations away from a traditional data center model to survive, stay agile and scale at pace, perceptions have shifted. A 2021 Google/IDG study found that **85%** of global IT leaders felt as secure or more secure with cloud than with on-premises infrastructure. Organizations are now much more likely to believe the cloud is safe for their data and applications.

Both viewpoints are misconceptions to some extent. The cloud is not fundamentally insecure, nor is it secure by default. The shared responsibility model for cloud security means that the cloud provider is responsible for the security of cloud infrastructure while the customer is responsible for the security of the apps and data they put there.

Security experts generally agree that the major cloud providers do a better job of securing cloud infrastructure than the typical organization can with an on-premises data center. After all, cloud providers pour billions of dollars into their core business of operating and securing their data centers. They constantly upgrade hardware and software, patch in minutes instead of days or weeks, and employ dedicated researchers who proactively find vulnerabilities and security issues in their infrastructure.

That's not to say these providers are bulletproof. Microsoft has fixed a handful of serious Azure flaws discovered by outside researchers over the past year. But to date, there are few known breaches of actual cloud infrastructure. Cloud breaches are overwhelmingly the result of misconfigurations, errors and oversights that fall in the realm of the customer's responsibility. Gartner estimates that through 2025, **99%** of cloud security failures will be the customer's fault.

Companies transitioning to the cloud should be less concerned about the security of the cloud itself and more concerned about whether they have the skills and know-how to use the cloud securely.

Cloud Security Challenges

So, what are the special security risks and challenges companies need to be sure they can address when moving to the cloud?

First, there are misconfigurations. The Check Point 2022 Cloud Security Report names misconfigurations as the number one cause of cloud security-related incidents. According to the 2022 Verizon DBIR, when taking into account breaches in general, **13%** are caused by errors—a figure heavily influenced by misconfigured cloud storage.

Misconfigurations can happen at any time, but they are even more common when organizations are forklifting over large amounts of data to the cloud. Staff members—who are likely unprepared for the complexity and scale of the transition—may neglect to change insecure default settings or make appropriate policies. The 2021 Ponemon Cost of a Data Breach Report cites extensive cloud migration as among the top factors contributing to higher-than-average data breach costs.

Then there is attacker detection, which is more difficult in the cloud than in on-premises systems. For example, in a conventional network, attackers commonly "live off the land" by running tools installed in the target systems like Mimikatz or PowerShell to help them accomplish their objectives. Defenders can watch for indicators that these tools are being run and flag these events. But in the cloud, attacker behavior primarily consists of using compromised credentials to gain access to legitimate accounts—a tactic much harder to distinguish from normal user behavior.

Moving to the cloud means some loss of visibility due to the lack of a centralized dashboard. Orgs lose some of the visibility they may have had with their previous on-premises data center because the responsibility for this has now shifted to the cloud provider. Visibility between cloud providers is also limited, as well as visibility between cloud and on-prem systems. These limitations all mean lost opportunities for detection—a troubling situation when attackers are known to compromise an organization's existing on-premises systems first and then pivot to the cloud environment.

Finally, there is shadow IT, which can be challenging to monitor in the cloud. As different people in different parts of the business spin up new cloud instances and new cloud accounts, the attack surface increases. Mergers and acquisitions further complicate this picture.

Keeping Up With The Cloud

The cloud offers unprecedented speed, flexibility, elasticity and efficiency—and yes, security at the infrastructure level. But given its unique considerations and challenges, organizations should be sure they have access to the expertise required to keep the customer area of responsibility secure—the applications and data.

That's because security in the cloud requires a specialized skill set. In addition to knowledge of network security fundamentals, Linux, and programming languages like Python, the cloud also requires expertise traditional network security doesn't. These can include command of identity and access management, CASB solutions, containerization, DevOps, cloud architecture, and familiarity with detecting anomalous behavior in the cloud.

The good news is that most cloud breaches stem from misconfigurations and design errors, which means these incidents are preventable. A comprehensive assessment of your environment by cloud-fluent experts is a great way to gain a clear view of your current cloud security risk landscape so you can get ahead of potential issues before they become incidents.

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.