Enterprise Spotlight: Securing the cloud

Credit: Rob Schulz / Shutterstock

This Special Report explores cloud security's unique challenges, the extent of the threats facing organizations today, and how the rapid adoption of AI is amplifying the problem. You'll learn where to look for hidden risks and essential strategies and best practices for securing your cloud environment.

CONTENTS

From the editors of Foundry's enterprise IT sites:

CIO CSO COMPUTERWORLD InfoWorld NETWORKWORLD

The state of cloud security

Attackers are increasingly turning their attention to cloud environments that enterprises aren't doing enough to secure

BY LUCIAN CONSTANTIN FOR CSO

Companies are having a hard time keeping their cloud infrastructure secure and the race to adopt and integrate AI services into their apps and workflows is making things worse.

Having analyzed billions of production assets on AWS, Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud this year, researchers from Orca Security warn that cloud assets have on average 115 vulnerabilities and over half of organizations have at least one such vulnerability that's over 20 years old. This is an alarming trend considering that attackers, including state-backed cyberespionage groups, have increasingly targeted cloud infrastructure in recent years.

A third of analyzed cloud assets fall into Orca's neglected-asset category — resources that use operating systems that are no longer supported and haven't been patched in over 180 days. Almost all companies have at least one neglected asset, usually virtual machines.

Organizations are also feeling the pressure to adopt AI so they don't get left behind, but this rushed approach often comes at the cost of security. According to Orca's findings, 62% of organizations have at least one vulnerable AI-related package in their cloud environments and many of these AI flaws are medium severity and above, allowing for attacks such as data leakage or remote code execution.

VULNERABILITY EXPLOITATION ON THE RISE

According to Verizon's 2025 Data Breach Investigation Report (DBIR), analysis of 22,000 security incidents, including 12,195 confirmed data breaches in 139 countries, found vulnerability exploitation to be the second-most prevalent initial access vector, overtaking phishing for the first time and after credential abuse.

Coupled with the fact that many organizations now employ hybrid environments that combine local and cloud assets, vulnerabilities in either setting are attractive targets for attackers.

Orca found that over two-thirds of organizations have at least one cloud

asset that is public-facing and enables lateral movement. Moreover, 55% of organizations have assets deployed across multiple cloud providers.

Web services are the most vulnerable assets, with 82% of organizations having at least one unpatched web service. And those vulnerabilities are not all new: 98% of organizations have at least one cloud asset vulnerability that's over 10 years old.

Log4Shell and Spring4Shell, highly publicized and widely exploited flaws reported in 2021 and 2022 respectively, are two prominent examples. Orca found that almost 60% of organizations still had assets affected by these vulnerabilities and a third had Internet-exposed assets that were vulnerable to Log4Shell, a flaw that leads to remote code execution.

"Clearly, these findings signal the critical need for better patch management, especially in the context of sophisticated threat groups targeting the least path of resistance to a compromise," the Orca team wrote in its report.

For example, APT29, a cyberespionage group attributed to the Russian Federation's Foreign Intelligence Service (SVR), is well known for exploiting vulnerabilities for initial access and for targeting cloud infrastructure. The group's targets include technology companies, the compromise of which can lead to supply chain attacks.

ISOLATED RISKS LEAD TO BIGGER ISSUES

Orca also warns that half of organizations have assets exposing attack paths that can lead to sensitive data exposure, as well as 23% with paths that lead to broad permission access and compromised hosts. Attack paths are the combination of risks that appear isolated but can be combined to lead to bigger compromises.

For example, Orca found that over a third of organizations had at least one asset that created more than 100 attack paths, with one in 10 having assets with more than 1,000 attack paths. The most toxic asset identified by Orca in its dataset was responsible for 165,142 attack paths.

Data exposure is a common issue with one in three organizations having publicly exposed storage buckets or databases with sensitive data in them.

"Threat actors prize sensitive data, especially at a time when the demand for data continues to increase amid AI innovation," the Orca team wrote. "It underscores a troubling trend that calls for more attention on data security."

IDENTITY THREATS

While vulnerabilities were the second most common initial access vector found in Verizon's DBIR, abused credentials once again took the top spot. Identities that can be abused for initial access

or lateral movement include not just end-user credentials but also API keys, access tokens, service accounts, cloud functions, and other non-human identities (NHIs) used by machines, services, and workloads.

"Our analysis finds that NHIs outnumber their human counterparts by an average of 50:1," the Orca team said. "Yet NHIs, when left unsecured, can dramatically increase cloud risks. This is especially true when users grant NHIs more permissions than they need."

Orca found that 77% of organizations that use AWS have at least one service account with permissions across two or more accounts and 12% of organizations have permissive roles attached to more than 50 instances. Some of these roles, once created, remain unused, with almost 90% of organizations having IAM credentials that were not used in over 90 days.

Many secrets that enable access to sensitive resources are exposed through source code repositories (85%) and over half of plaintext secrets remain embedded in Git history even if they are removed from the latest version of the code.

On top of exposed secrets, attackers can also take advantage of misconfigurations in infrastructure-as-code templates (20% of organizations), Lambda functions (77% of organizations), and source code management platforms such as GitHub and GitLab (57% of organizations).

"Cloud security has reached a critical turning point," the Orca team concluded. "As organizations increasingly rely on the cloud to accelerate innovation and growth, several converging trends are reshaping the challenges security teams face — and the strategies they need to stay ahead." ■

8 often-overlooked cloud security gotchas

With the typical enterprise today leveraging a dozen cloud vendors globally, there are plenty of ways for security nightmares to sneak in

BY EVAN SCHUMAN FOR CSO

As enterprise CISOs try and maintain security across their entire global threat landscape, they are finding themselves in a love/hate relationship with their various cloud environments. For many, though, it's more of a hate/despise relationship.

Clouds can appear to be a seamless extension of existing operations, but they are in reality controlled by various cloud teams that are spread across the enterprise — and that may be at odds with the cybersecurity team's directives and needs.

As such, the very nature of cloud use in the enterprise can deliver a wide range of insidious cybersecurity problems that can be difficult to detect. We spoke with a range of cloud security experts about under-the-radar cloud security issues most likely to surprise the enterprise SOC.

1. TEMPORARY RESOURCES ARE A HUGE THREAT

Few things in the cloud deliver as permanent a headache as temporary resources. That is mostly because they are difficult to scan — given that they are so short-lived — making them ideal places to hide malware.

These ephemeral resources, such as temporary storage instances or dynamic provisioning of resources that exist only to perform a specific function and then terminate, are becoming increasingly common in cloud environments.

"The temporary aspect of ephemeral resources might lead security teams to underestimate the potential security risks, assuming these resources pose less of a threat due to their short lifespan," says Cache Merrill, founder of software vendor Zibtek.

But once these resources are compromised, they can become the attacker's best friend by serving "as entry points or temporary havens for malicious activities without leaving much trace for forensic analysis," Merrill adds. "This can be particularly

challenging because traditional security tools and practices are often configured for long-standing infrastructure and might not automatically extend to these short-lived components."

According to Merrill, the chance of typical security scans missing ephemeral attacks is "super high. Worst case scenario? You leave read-write access open to the world."

2. IT INVENTORY EXCUSES DON'T CUT IT IN THE CLOUD

Security specialists often avoid dealing with performing inventory of IT assets on-prem. What many don't realize is that taking inventory in the cloud is far easier and there are no excuses for avoiding doing it anymore, argues Scott Piper, principal cloud security researcher at Wiz.

"A lot of folks have scars from dealing with inventory from before. Historically, doing IT inventories was very difficult in a world where you needed to physically trace wires and get eyes on devices. Then you needed to try to understand the software they ran and how they were configured, which required getting agents on them," says Piper.

"That's a difficult problem because you need an agent that works for the OS with testing and approvals for the potential performance and reliability risks, figure out how to authenticate to the device in order to install the agent, additional possible configuration changes for the network communications they need to perform, trouble-shoot any problems if the agent stops calling in, and more."

Conversely, the cloud sees everything as an API, which makes taking inventory much more straightforward. It may be far from fun, but security must overcome years of ingrained avoidance.

"Identifying all your resources is one set of APIs. Scanning a server for all the applications and libraries installed can be done by snapshotting the disk with an API and then spending as much time as needed evaluating that data without having to worry much about the performance of that scanning," says Piper.

Cybersecurity professionals who "believe that despite the value an inventory provides, the difficulties in obtaining that inventory aren't worth it" are doing their companies' cybersecurity posture a disservice in the cloud, Piper warns, as such inventory avoidance can deliver severe cybersecurity problems.

"Because they are not focusing on inventory, they are not seeing the misconfigurations. The inventory that they don't know about may have critical configuration issues that they are therefore not resolving," adds Piper.

3. CLOUD BILLS HELP TRACK ATTACKS, BUT WITH CAVEATS

Some attackers aren't interested in stealing enterprise data via ransomware or shutting down operations via DDoS. Instead, they are saboteurs looking to punish the enterprise for whatever reason. One such method includes denial of wallet (DoW) attacks designed to force your enterprise to run up lots of extra cloud charges. But it's not just increases in cloud spend that can be an early indicator of malicious activity.

"A big drop in consumption can tell you that someone is bringing down your cloud — and tell you that before your monitoring systems will," says Doug Saylors, a partner with technology advisory firm ISG. The attackers "could be removing backups for the last 90 days."

While tracking cloud spend can deliver cybersecurity intelligence, the nature of cloud billing — especially when new features and services are constantly being added — makes real-time sleuthing a challenge.

"Hyperscalers are bringing so many products to the market," explains Saylors. "Sometimes the cyber and IT teams find out about those products way beyond initial development."

As for DoW attacks, they typically work by "repeatedly triggering API endpoints to intentionally raise cloud computing bills," says Drew Firment, chief cloud strategist at IT training company Pluralsight.

"As the size of datasets grow, so does the potential financial impact of DoW attacks that exploit vulnerable endpoints and trigger large and expensive data transfers," argues Firment. "To reduce exposure, organizations should implement API Gateway rate limits to prevent abuse of endpoints, as well configure web application firewall policies to limit the number of requests from a single IP address or range."

Brian Levine, Ernst & Young's managing director for cybersecurity strategies, adds that a lack of internal transparency over cloud use can be another problem for CISOs. "Knowledge that should be shared between multiple teams, and the lack of someone senior making sure it gets shared effectively and in a timely fashion, is a common enterprise pain point," he says. "As vendors of cloud services come up with additional security offerings and packages, it can become confusing. What do we need and what is an upsell? It's a hard analysis to do."

Levine gave an example of cloud platforms that charge enterprises extra to record and save logs — something that's crucial to conducting post-event analysis and forensics, especially when attackers deliberately delete or doctor logs they can access.

4. YOUR IDP STRATEGY IS LIKELY LACKING

Identity provider (IDP) outages are relatively rare and don't last very long. Plus, switching to a backup service can cause bigger disruptions for end-users — given the possibility of requiring a behavioral change — than simply waiting a few more minutes to see whether the primary system gets restored.

But because there's no way to determine when restoration will happen, enterprises still need an IDP backup strategy, says Martin Kuppinger, principal analyst for German consulting firm KuppingerCole Analysts. Unfortunately, for the reasons cited above, many companies forego having one.

"How long can you withstand an outage of IDaaS/SaaS services when all your authentication depends on it? You need to have something in place to allow you to authenticate such services when your primary IDP is not available," urges Kuppinger, who advises having a second IDP that runs on-prem or separately from the cloud environment used by the primary IDP.

5. SAAS IS A SECURITY ISSUE YOU'RE NOT FULLY DEALING WITH

SaaS security holes are sneaky and insidious, quietly adding a massive increase in risk without many SOC staffers noticing.

"SaaS providers vary hugely in risk. SaaS apps are radically different in how much risk they present to the organization. The biggest are very good. The next couple of tiers are usable, but there is a long tail of SaaS apps that are very hard to assess," says Gartner analyst Charlie Winckless.

"This issue is compounded by the fact that many CISOs have a massive focus on the three big hyperscalers and ignore SaaS," he adds. "Code repositories are often in SaaS and may be open or much less secure than you expect."

6. DANGLING DNS POINTERS CAN BE BIG PROBLEMS

DNS is another seemingly innocuous issue that can become highly problematic in the cloud, Gartner's Winckless says.

"It's easy in the dynamic nature of cloud to be exposed by DNS. [Let's say your team] sets up a site in Azure with an azurewebsites.net DNS and creates a CNAME for yourself and points it to the site," he explains. "If you delete the site, which is common, and not the CNAME, an attacker can masquerade under your dangling DNS. This isn't cloud-unique, but the cloud dynamism makes it much easier to accidentally leave yourself with the dangling DNS pointer."

When someone provisions a resource in the cloud, it is given a name "but nobody is going to remember that name," Winckless says, so it gets thrown into DNS. "An attacker can register that underlying domain and put whatever they want there and it looks so much more" like a legitimate enterprise file.

7. API ACCESS IS A SECURITY INCIDENT WAITING TO HAPPEN

APIs may be the essence of cloud structure, but they also provide many onramps for attackers.

"Local API keys in apps are a surprisingly common yet overlooked cloud security gap. Say, for example, an employee is terminated and you disable that user's single sign-on," says Paul Querna, CTO of ConductorOne, an identity governance firm. "In many cases, there's a local API key that will continue working even after SSO has been disabled. That's because local API keys operate independently of the user's SSO status and are not automatically revoked when SSO is turned off. This means that the user might still have access to some systems or data, which poses a serious security risk."

ISG's Saylors agrees, emphasizing custom code that accesses APIs as a security issue. He gave an example of an enterprise with presences in all major cloud platforms.

"Let's say someone is using those providers and they happen to have a common identity platform, maybe SailPoint. If SailPoint is passing a data stream to AWS and Microsoft and maybe others, it could permit access to all that client's information in one of those hyperscaler environments. It might allow limited data access in the cloud. Now let's say somehow an attacker is targeting that AWS API. If that client was using the same credentials across those cloud platforms," it could provide extensive access, he says.

8. IMDSV2: WHAT YOU DON'T KNOW COULD KILL YOUR CLOUD

In March 2024, Amazon quietly rolled out an update to a critical piece of the AWS platform: the Instance Metadata Service (IMDS). Some SOCs "might not even realize that they are using [IMDS]" and therefore they are exposing their operation to a serious "security threat related to metadata exposure," says Pluralsight's Firment.

"AWS uses IMDS to store security credentials used by other applications and services and makes that information available using a REST API. Attackers can use a Server-Side Request Forgery

[SSRF] to steal credentials from IMDS, which allows them to authenticate as the instance role for lateral movement or data theft," warns Firment. "AWS introduced a newer version of IMDS, version 2, to improve the security of unauthorized metadata, although many organizations are still using the original IMDSv1 as the default. To help CISOs close this potential security hole, AWS recently announced the ability to set all newly launched Amazon EC2 instances to the more secure IMDSv2 by default."

IMDSv2 "was launched by AWS in November 2019, but the ability to set the default to the new version was not introduced until March 2024. As a result, many organizations continued to use the original vulnerable IMDSv1. Interesting to note that the default only applies to new instances launched, so existing instances with IMDSv1 still need to be reconfigured," explains Firment.

"This is a pretty significant threat for most organizations. There's probably not an awareness of the need to switch everybody to the new version," he says, adding that the risk is that attackers "could grab credentials and move laterally within your organization. ■

A CISO game plan for cloud security

CISOs are still hampered by bad assumptions and outdated approaches, and should be involved in decisions from day one

BY DAVID LINTHICUM FOR INFOWORLD

As businesses increasingly migrate to the cloud, chief information security officers (CISOs) face numerous critical challenges in ensuring robust cloud security. This sentiment was echoed by experts at a recent Gartner Security & Risk Management Summit. Gartner projects a significant 24% increase in spending on cloud security, positioning it as the fastest-growing segment within the global security and risk management market.

ADAPT, ADJUST, EXECUTE

The bottom line is that shifting to cloud computing necessitates fundamentally rethinking security. Organizations strive to integrate the cloud into standard business operations, but this transition has more pitfalls than most CISOs understand. I've seen this in my research and my experience as a consultant for 20 years, cloud and prior.

Issues that have been present in traditional IT environments persist in the cloud, such as governance, misconfiguration, insecure supply chains and pipelines, data loss or exfiltration, and failures in secrets and key management. The cloud introduces unique risks, including limited visibility, dynamic attack surfaces, identity proliferation, and misunderstandings around shared responsibility, compliance, regulation, and sovereignty. And this is just the tip of the iceberg.

Most CISOs tell me they have yet to understand exactly what should change. Many feel misled by their cloud provider regarding the work required to secure their cloud deployments. I've written plenty of advice to the contrary, but it's never a good idea to say "I told you so" to someone struggling, so we need to figure out how to do better.

THE SHARED RESPONSIBILITY MODEL

Many CISOs and security teams need clarification about the shared

responsibility model used by major public cloud providers such as Amazon Web Services (AWS) and Microsoft Azure. This model delineates the security responsibilities of the cloud provider and the customer and is normally on the first slide of any cloud security presentation since 2008.

Challenges often arise from assumptions related to technology and the extent of the cloud providers' security obligations. Compliance, visibility of sensitive data, business continuity, and confusing service-level agreements (SLAs) become problems CISOs did not see coming. As one CISO friend of mine said after 12 years of dealing with cloud security: "It was never about 'shared responsibility,' it was always all my responsibility, period."

CISOs often encounter several key pitfalls in managing cloud security:

- Business lines have inadequately addressed security needs.
- The cloud is more complex than initially understood.
- Cloud strategy, architecture, or transformation initiatives often proceed without input from the CISO, who is then expected to make it all secure.
- Failure to collaborate with CIOs to integrate security into platform engineering and DevOps bottlenecks development pipelines with outdated security processes.
- Old security patterns are applied to new technologies.

NO SUBSTITUTE FOR HARD (BORING) WORK

I recommend several strategies for navigating these challenges. Utilizing automated tools to manage cloud environment security is crucial. Automation is your friend. Moreover, establishing robust cloud security governance can help prioritize alerts and secure service edges. Running around in circles for every anomaly doesn't scale, and the risk of being "the boy who cried wolf" will likely cause a breach.

Consolidating security efforts and working towards immutability are also essential best practices. Additionally, reskilling and upskilling the security workforce is critical to adapting to the evolving landscape of cloud security. Most breaches are caused by a lack of training and not a lack of technology. CISOs understand they can have the best cloud security technology available, but they can't fix stupid. Misconfigurations are the primary cause of cloud breaches.

Of course, specific issues have to be addressed for your unique needs. CISOs often adopt good ideas from analysts and consulting firms that are

the wrong fit for them. Cloud security is never a “one size fits all” solution, and it needs to be systemic to all systems, not installed during the last step of deployment. Enterprises often get into trouble because security is loosely coupled and thus ineffective.

I wish I had a magic formula to give CISOs looking for better cloud security, but it’s about doing things smartly and purposefully to win the game. People hate to hear that – it means more boring planning and research. But there is no substitute. ■