5 Key Areas of Cloud Vulnerability Management

SANS

Created by Jonathan Risto

The Cloud is Dynamic

The cloud environment is ever-changing, with resources frequently being created and removed. It's crucial to efficiently monitor these resources to pinpoint issues within the environment.

45% **of high-risk, cloud-hosted exposure**

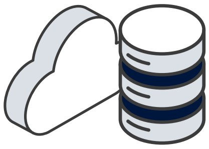
were in new services created in the past month. The reaction of new, publicly accessible cloud services, both intended and unauthorized accounts for nearly half of all high-criticality exposures at a given time.[1]

How is this impacting Vulnerability Management?

Lack of ongoing visibility and monitoring of cloud resources hampers vulnerability management. Without this, we remain unaware of the existing assets, hindering our ability to secure them effectively. Furthermore, understanding the attack surface relies on visibility into the utilized services.

Over 20%

of externally accessible cloud services change every month.[1]

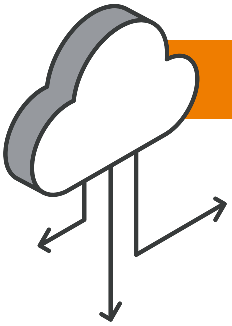


39% Responded

that staying in compliance as cloud environments change is the most challenging part of the cloud compliance process.[2]

Misconfigurations

Misconfigurations can expose data. Misconfigurations often occur due to human error, lack of oversight, or insufficient understanding of the platform being used.



51%

of respondents felt that cloud misconfigurations and improper security settings are one of the key concerns.[3]

How is this impacting Vulnerability Management?

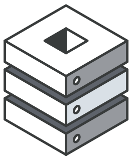
Misconfigurations can reveal data and affect how we decide which vulnerabilities to fix first. They also make it harder for us to see the real extent of a system's attack surface.

23% of cloud security incidents

are a result of cloud misconfigurations.[4]

68% of responding cyber security experts

categorize misconfigured cloud infrastructure as a pressing concern.[5]



Security incidents attributed to misconfiguration led to system downtime for

34% of respondents.[6]

Regulatory and Compliance

Laws and regulations are updated to match the needs of new technology and challenges.

How is this impacting Vulnerability Management?

Changes in rules and standards about how data should be handled affect how we manage security in the cloud. Meeting these new rules means we have to constantly adapt our security strategies to follow these changing rules.

Scaling and automating compliance activities is a challenge for

24% of respondents.[2]

Staying current with changing compliance requires is challenging for 33% of respondents.[2]

39% Responded that staying in compliance as cloud environment change is the most challenging part of the cloud compliance process.[2]

Skills Gap

Rapid and complex technology adoption requires skilled individuals to manage them. There's a significant shortage of qualified individuals to fill numerous IT roles, especially those related to cloud services.

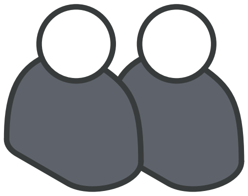
How is this impacting Vulnerability Management?

We are adopting new ways to doing business with technology like containerization and serverless functions. But our programs are not able to manage and validate these new technologies. And our people can't keep up with the rapid technology shifts.

Skills needed to understand multi providers offerings adds to misconfigurations.

75% of tech leaders are building all new products and features in the cloud moving forward, but only 8% of technologists have significant cloud-related skills and experience.[7]

53% cite lack of staff knowledge and expertise as the most challenging part of cloud compliance process.[2]



78% of all organizations say lack of resources/expertise is their top cloud challenge.[11]

87% of organizations are multi-cloud.[11]

Code is Everywhere

Everything in the cloud is software defined and controlled when we are deploying at scale. We leverage Infrastructure as Code for deployments, orchestration and management of our cloud environment.

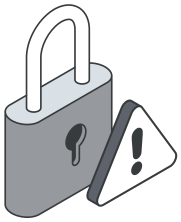
How is this impacting Vulnerability Management?

Even if your organization isn't creating products for sale through custom development Vulnerability Management teams now need to engage and evaluate code. The rise of serverless systems, Infrastructure as Code (IaC), and automation means that nearly everything, from deployments to managing the cloud, is scripted or written as code.

Over 70% **of our AWS customers**

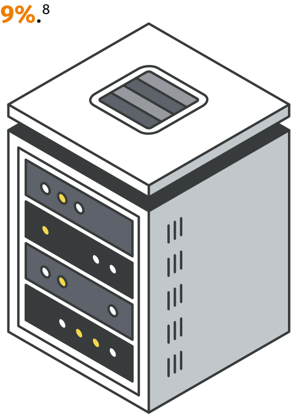
And 60% **of Google Cloud customers**

currently use one or more serverless solutions, with **Azure** following closely at **49%**.[8]



0.8 billion in 2022

projected to reach 2.3 billion in 2027, CAGR 24.0% for IaC.[9]



25% **Global IaC Growth CAGR.**[10]

References

1 - *https://start.paloaltonetworks.com/rs/531-OCS-018/images/Unit42_ASM_Threat_Report_2023.pdf*

2 - *https://resources.trendmicro.com/rs/945-CXD-062/images/2023-Cloud-Security-Report-TrendMicro-Final.pdf*

3 - *https://cloudsecurityalliance.org/blog/2022/02/17/multi-cloud-security/*

4 - *https://www.pingsafe.com/blog/cloud-security-statistics/#*

5 - *https://www.getastra.com/blog/security-audit/cloud-security-statistics/*

6 - *https://go.snyk.io/rs/677-THP-415/images/cloud-security-report-22.pdf*

7 - *https://appdevelopermagazine-com.cdn.ampproject.org/c/s/appdevelopermagazine.com/cloud-computing-skills-will-be-in-high-demand-for-2023/amp/*

8 - *https://www.datadoghq.com/state-of-serverless/*

9 - *https://www.marketsandmarkets.com/Market-Reports/infrastructure-as-code-market-115458264.html*

10 - *https://markwideresearch.com/infrastructure-as-code-iac-market/*

11 - *https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks*

CLOUD SECURITY

SANS