CYBER SECURITY HUB

The State of Cloud Configuration Security Practices

Find out where organizations need to focus their efforts to secure their cloud applications as revealed by the results of Cyber Security Hub's Cloud Configuration Security Practices survey

Inside:

- Challenges businesses face today as the number of cloud applications increases
- Why cloud delivery is self-service, but cyber security is not
- Where organizations are failing to respond fast enough to security issues

Brought to you in association with:

concourse labs

Introduction

The use of the cloud is set to grow exponentially throughout 2022. The *Cloud Configuration Security Practices survey* conducted by *Cyber Security Hub* found that as of November 2021 enterprise companies in sectors that include financial services, healthcare and communications have on average 29 applications deployed in the cloud, which is set to grow to closer to 144 applications over the next 12 months. This represents a 395 percent increase.

The survey data also reveals that on average 51 percent of security teams can only perform three applications reviews per week. This is a huge problem given the increased number of applications in the cloud that is expected. As well as being a significant security risk, this also means that businesses will not be able to reap the full business benefits of the cloud if they cannot migrate applications quickly.

Businesses face inherent risks when using the cloud and with the pace of cloud adoption and innovation there is evidence from the *Cyber Security Hub* survey that security activity is not keeping pace with these changes.

Cloud providers like Amazon, Microsoft and Google cannot secure everything because organizations are provisioning services, configuring them and using them. A 2019 recommendation by Gartner said that **through 2025, 99 percent of cloud security failures will be the customer's fault.**

The results of *Cyber Security Hub*'s *Cloud Configuration Security Practices survey* show that more than two years on from Gartner's recommendation there remain serious gaps in many organizations' cloud security practices, leaving them exposed to increase risk of a cloud breach.

Applications in the cloud are set to grow by **395 percent** over the next 12 months.

Contents

As cyber threats evolve and cloud application adoption accelerates organization's must ensure their security practices are keeping up.

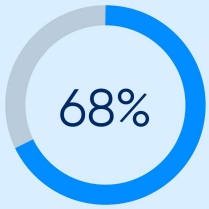
This report seeks to identify the biggest pain points facing companies who are utilizing public cloud services, what can be done to overcome these challenges and where the gaps in securing cloud misconfiguration lie.

Ultimately, without a fundamental shift left in managing cloud risk through the use of automated security tools, an organization's ability to protect cloud data and resources will erode rapidly as cloud usage accelerates.

Cloud delivery is self-service but security is not

Of those surveyed in *Cyber Security Hub's Cloud Configuration Security Practices survey*, an average of 68 percent said their organization's infrastructure services (i.e., compute, storage or databases) are provisioned using Infrastructure-as-Code (IaC) or similar software-defined tools.

IaC is the process of managing and provisioning data centers through code, rather than manually. This is related to cloud operations as it allows the automated provisioning of cloud infrastructure services and organizations can, therefore, take a process and codify it so it is both automated and repeatable.



of respondents said their organization's infrastructure services are provisioned using IaC or similar software-defined tools.

"Security-as-code is the encapsulation of your security requirements and logic into software, IaC is really the same thing except it is more about the cloud services that you need in order to perform certain business functions," explains Don Duet, chairman and co-founder of Concourse Labs.

Provisioning cloud services through IaC saves both time and money. It minimizes human error and reduces the reuse of gold masters. Moreover, every change that is made is documented, meaning there is full accountability and traceability of configuration changes.

Duet notes that IaC has been around for a number of years and is now deeply embedded in most companies' approaches to software development.

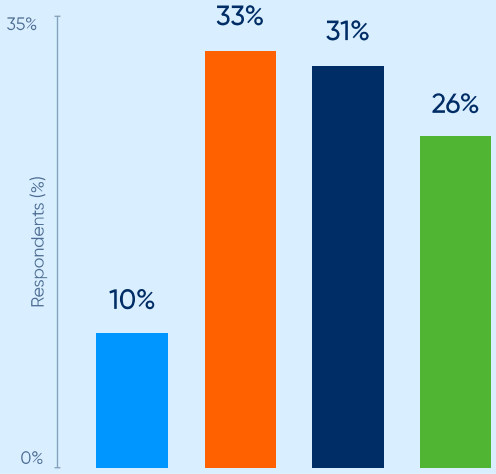
Cloud is delivered as code but security is not

It is clear that organizations are comfortable in delivering cloud services via code, however, this is not yet being seen in the delivery of cloud security services.

FIGURE 1

Which of the following best describes the use of infrastructure-as-code security tools within development and CI/CD pipelines?

- No use of infrastructure-as-code security tools within the software delivery pipeline
- Only discretionary and limited use of infrastructure-as-code security tools
- Mandatory use of infrastructure-as-code security tools for high-risk applications
- Widespread use of infrastructure-as-code security tools across all application types



Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

"The fact that most people are using IaC is great. That practice now looks like it is getting deeply entrenched and that's fantastic," Deut says. "Today, providing security preventatively is going to create substantially better ways for these companies to manage their risk."

Security tools are clearly important when developing cloud applications with IaC but the *Cloud Configuration Security Practices survey* shows there is a mixed approach to how and when security tools are being used.

While it is true that the majority of services are being delivered via IaC, the security and compliance of IaC is not widely being validated.

A total of 74 percent of respondent said that their pipelines are not using IaC security tools widely across their cloud applications portfolios.

Widespread IaC security tools across all application types were only found in 26 percent of respondents. While IaC security tools are being used in either a discretionary/limited way (33 percent) or are mandatory for high-risk applications (31 percent) there is not yet widespread use of these security tools (see Figure 1). Overall, there is a high number or organizations using IaC, but there remains a limit to the way security tools associated with IaC are being used.

Misconfiguration of cloud services is the leading cause of cloud data breaches. Duet commented that organizations must find and fix IaC vulnerabilities before they are replicated countless times within orchestration and deployed into the wild.

Speaking about the importance of IaC security tools, Bradley J. Schaufenbuel, VP and CISO at Paychex, says that the HR and payroll solutions firm had recently performed extensive evaluation of IaC security tools, but the company has not yet purchased one. IaC security tools identify vulnerabilities in IaC scripts such as embedded plaintext passwords and keys.

"If IaC is not properly secured, an attacker can leverage the IaC platform to move laterally within his victim's technology environment and gain unauthorized access to connected systems and data repositories," Schaufenbuel explains.

Duet argues that with security-as-code organizations can be empowered to achieve the same level of self-service for governing and securing the cloud that they have with the development of the cloud itself through IaC.

Organizations are failing to respond fast enough

It is clear that a fast response to security issues is required in any setting beyond the realm of cloud applications. The *Cloud Configuration Security Practices survey* found that a lot of the detection and remediation tasks are taking what many would consider to be too long for cloud environments that can change in seconds.

Organizations have been conditioned to accept that bad things are going to happen – meaning breaches and incidents will occur, so they spend most of their efforts on runtime detection and response – to try and limit the time they are exposed to a potential risk, Duet notes.

The survey found that it takes more than 70 percent of organizations more than one week to detect and remediate a single cloud services risk.

This clearly is not scalable given that most organizations concurrently manage hundreds or thousands of open cloud security tickets. The results show that 70 percent of respondents said it takes more than 24 hours to detect a violation within a cloud service; 72 percent said it takes more than 24 hours to identify the application causing the violation; 75 percent said it takes more than 24 hours to assign the issue to a developer for remediation; 80 percent said it takes more than 24 hours to correct the violation; and, finally, 72 percent said it takes more than 24 hours to verify the fix (see Figure 2).

One issue that is prevalent – not just in terms of IaC and cloud applications, but also an industry-wide problem – is that security teams are stretched, under resourced and dealing with a large number of security issues on a regular basis.

Large backlogs of security tickets have become the new normal; they are accepted because security teams do not see the alternative, Duet notes.

In addition, because traditional cybersecurity is not being delivered as code it does not have the productivity and risk reduction benefits mentioned in the previous section relating to IaC. It is not, therefore, able to keep pace with cloud self-service delivery.

FIGURE 2

On average, how long does it take to complete these required cloud security detection and remediation steps, within your organization?

Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

Shifting cloud security left is imperative

Runtime detection and response are a must for securing cloud environments, but the cloud is so big and moves far too fast for organizations to exclusively pursue a reactive cyber security strategy.

The number of security tickets continues to pile up as is evident by the results of our survey. The *Cloud Configuration Security Practices survey* found that on average 62 percent of respondents are concurrently managing hundreds or more tickets specific to cloud misconfiguration, with almost one-third managing thousands to tens of thousands of tickets (see Figure 3).

"Public cloud presents new challenges that require security leaders to adapt their strategies. A purely reactive posture to cloud security is no longer enough. Organizations must shift-left and prevent cloud misconfigurations before they are available for bad actors to exploit," Duet says.

With risk levels high, when using public cloud infrastructure organizations must be extremely confident in their ability to stop a cloud breach that could expose their critical data, or take critical services offline.

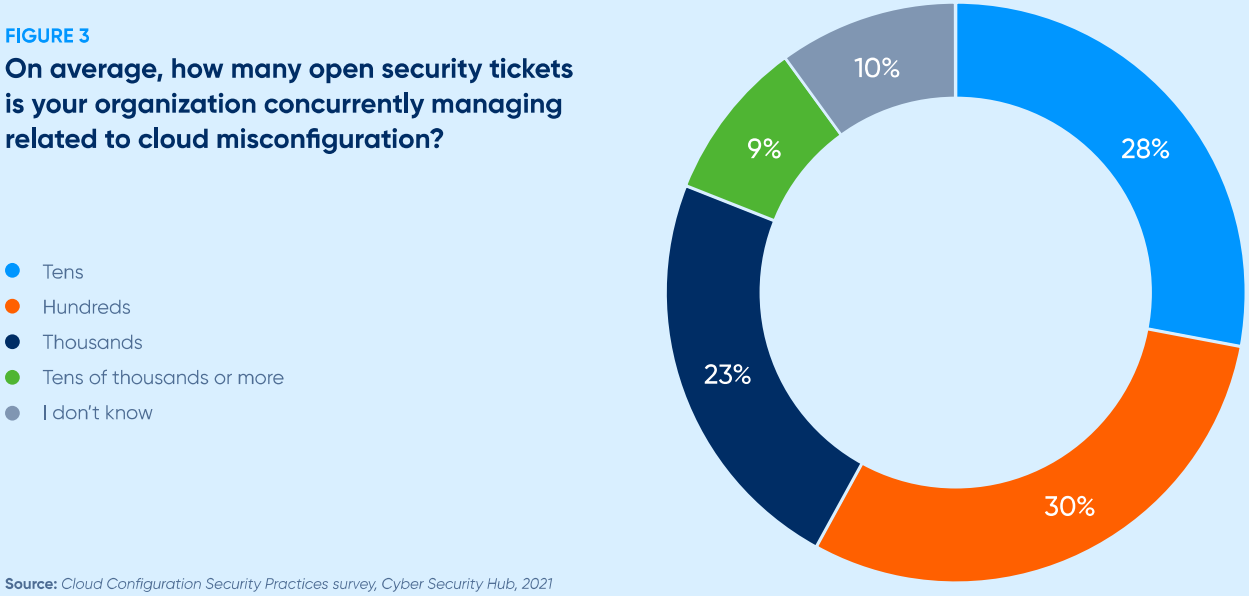
"A purely reactive posture to public cloud security is no longer enough."

Don Duet

Chairman and co-founder of Concourse Labs

FIGURE 3

On average, how many open security tickets is your organization concurrently managing related to cloud misconfiguration?

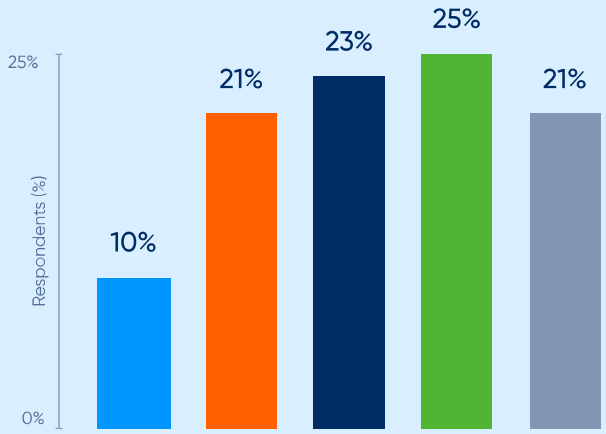


Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

FIGURE 4

How confident are you that your runtime security tools alone are sufficient to ensure your cloud security?

- Not at all confident
- Somewhat confident
- Moderately confident
- Very confident
- Extremely confident



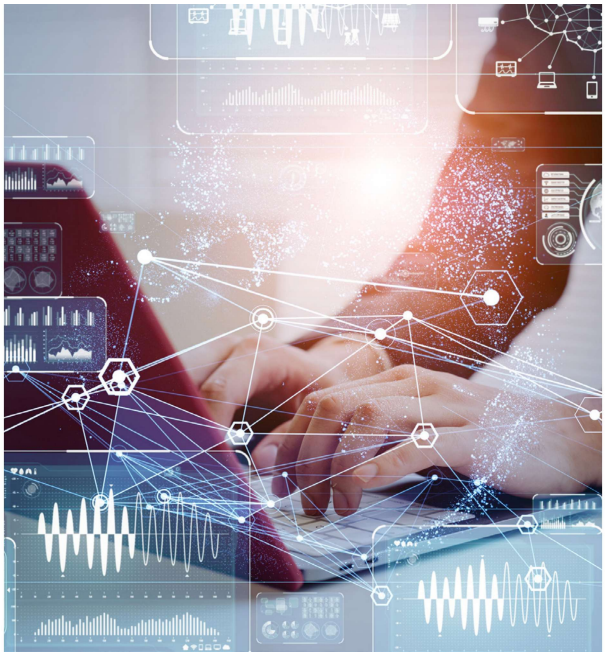
Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

The survey also showed that 79 percent of respondents said they were less than extremely confident that their runtime security tools were sufficient to keep their cloud data and workloads safe (see Figure 4).

Runtime tools are able to find and detect risks in the wild that actively expose organizations to incidents and breaches. However, in runtime it is a race to find and fix threats before bad actors exploit them. Today we are falling behind the threat actors with runtime tools alone. In addition, false negatives and false positives can be an issue with runtime tools leading to alert fatigue which poses a big challenge with regards to an organization's ability to respond quickly.

"It is, therefore, prudent to compliment runtime security tools with ones that help you to find and eliminate vulnerabilities in the first place so there is nothing that gets by a runtime security tool to exploit. Prevention is where IaC security tools are typically focused," Schaufenbuel says.

Those that are using IaC security tools are doing so in varying ways. There was an equal split between how IaC security tools were being used whether it was: alert-only to IaC violations and exposures, based on pre-established security policy guardrails, risky code is allowed to proceed to production (29 percent); to prevent code release to production due to infrastructure-as-code violations and exposures, based on preestablished security policy gates where remediation is performed manually (30 percent); and finally automatic remediation of infrastructure-as-code violations and exposures, based on pre-established security policy guardrails and gates (29 percent).



Security automation is crucial to cloud innovation [8]

Automating processes is key to maintaining efficiency across a multitude of business practices beyond the realm of cyber security and cloud computing. However, survey respondents showed a mixed level of automation when it comes to their IaC security reviews.

It is also key to keeping up with the pace of change within the cloud environment.

With over 70 percent of organizations saying it takes them more than one week to find and fix a single cloud security risk automation becomes a necessary tool for security teams to keep pace with cloud application delivery.

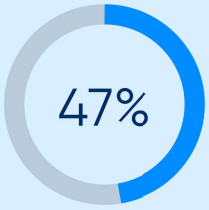
The *Cloud Configuration Security Practices survey* revealed that the average percentage of cloud application releases that undergo some type of security review is 68. While this is a positive sign there remains a high number of cloud application releases not undergoing security reviews of their IaC which could lead to further security exposure.

In total it was found that 38 percent of infrastructure-as-code security reviews are performed completely manually by security practitioners.

"In agile, DevOps-driven organizations, there are hundreds of IaC end points and changes are being made to the code almost continuously. The velocity of changes is simply too great for manual security reviews to be effective," Schaufenbuel comments.

Of those surveyed, 80 percent of organizations said it takes more than 24-hours to perform a manual review of a single cloud application's infrastructure-as-code, of which 47 percent take more than one week (see Figure 5).

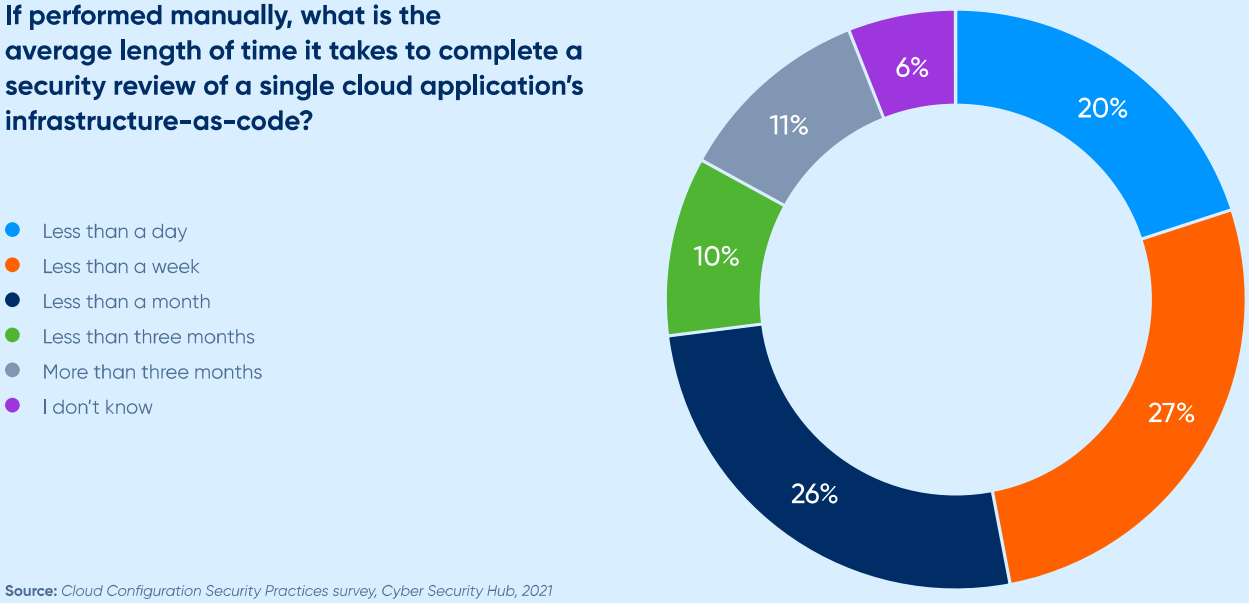
Automated testing is exponentially faster than manual processing and Schaufenbuel notes that it also tends to be more accurate, as human error within manual security reviews can result in missed vulnerabilities.



of respondents said it takes more than one week to manually review an application's infrastructure -as-code.

FIGURE 5

If performed manually, what is the average length of time it takes to complete a security review of a single cloud application's infrastructure-as-code?



Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

Q. What are the biggest challenges preventing misconfigured cloud services from being deployed?

A: "The knowledge and staff members for the review and correction of services."

Survey respondent

Preventing a misconfigured cloud service from being deployed is key to ensure an organization's cyber security remains intact.

Manual deployment, lack of skills and diminished manpower were all highlighted as challenges by those responding to the survey.

Beating the bottleneck

Security reviews remain a bottleneck to migrating cloud applications to public cloud safely. One in two survey respondents said that on average their security teams can perform up to three cloud application security reviews per week.

As noted in the introduction, respondents to the survey said that within the next 12 months they will (on average) have 144 applications deployed in cloud. Based on the findings regarding security reviews it would take 51% of security teams 48 weeks to review their cloud applications.

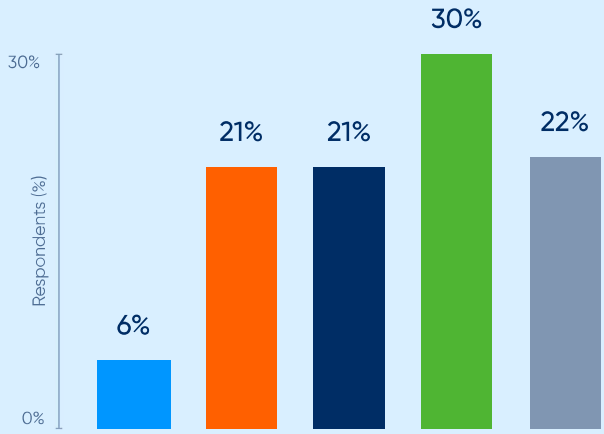
This is only for the initial application review and does not consider ongoing updates which can easily happen on a monthly basis.

"Anything you are going to do with people is impractical," Duet notes. "It is extremely difficult to get people with the knowledge of security, the knowledge of regulations, the knowledge of your business and the knowledge of your cloud applications. There is no one person that exists in most companies that knows all that.

FIGURE 6

How confident are you that your security requirements are being implemented correctly and consistently by cloud application developers?

- Not at all confident
- Somewhat confident
- Moderately confident
- Very confident
- Extremely confident



Source: *Cloud Configuration Security Practices survey, Cyber Security Hub, 2021*

"Secondly, the knowledge changes so rapidly. The security landscape changes, cloud usage changes and the cloud services themselves change. It is almost impossible to be done purely with people. This whole aspect of building a framework or having a security-as-code type program allows for those types of expertise to be encapsulated into software. Maintaining the software is still a human process but it gives you the scale that makes it reasonable to actually support it," Duet notes.

Schaufenbuel adds that a lack of cloud security expertise on staff (within security teams or within development teams) was one of the biggest challenges facing cloud security today.

Survey respondents repeatedly corroborated this claim, by saying one issue in preventing misconfigured cloud services from being deployed is not having resources available that are knowledgeable to develop cloud services properly.

In addition, many survey respondents said that they do not have full confidence that cloud security requirements are being implemented correctly and consistently.
It is clear that with the exponential increase in cloud applications that are expected, many security teams will simply be unable to keep up with the pace.

Confidence issues

In the world of cyber security, having a high level of confidence that policies and controls are properly implemented is essential and 30 percent of respondents said they were very confident that security requirements are being implemented correctly and consistently by cloud application developers, and 22 percent said they are extremely confident (see Figure 6).

Despite this, 48 percent of respondents admitted to being less than confident, 20 percent said they were only moderately confident and 22 percent said only somewhat. Six percent were not confident at all.

There remains a visible gap between an organization's security requirements and those actually being implemented both correctly and consistently by the cloud application developers. This may mean that some security requirements are being implemented correctly, but not consistently, or they could simply be being implemented but not always correctly.

Conclusion

The results of our survey show that there is a huge amount of cloud adoption ongoing with many organizations set to increase the number of applications in the cloud in the near future. There remain, however, a large number of security gaps and challenges. Many are using IaC security tools in a limited capacity, but the scope of usage is far from ideal, leaving organizations blind to security threats that pose a high risk of incident or breach.

While fragmented tools exist there remain a number of barriers to ensuring that cloud misconfigurations are not putting organizations at increased risk.

Respondents to the *Cloud Configuration Security Practices survey* noted that their issues in preventing misconfigured cloud services from being deployed include the amount of data, the cost, the lack of knowledge, the lack of automation, and the large number of security checks required. One respondent even said that it was a "big mistake" for management to take these issues "lightly".

There is clearly a need for organizations to implement cloud security in a manner consistent with how they provision public cloud services – in code.

With an avalanche of cloud applications forecast within the next 12-months security-as-code will be essential for businesses to capture the full benefits of public cloud. For innovation to continue on an upward trajectory cloud security must keep pace with cloud development and delivery.

Otherwise, businesses will have to either throttle back cloud innovation or blindly accept the risks of moving applications to public cloud. Neither of which are good for business.

With security-as-code, companies are enabled to achieve the same level of self-service for governing and securing public cloud that they have with the development and use of the cloud itself.

Please note: All comments made by the contributors of this report are solely the views of the individuals without any relation to their employers, institutions or business partners.