A REPORT ON THE CLOUD RISKS AND SECURITY CHALLENGES ORGANIZATIONS ARE EXPERIENCING IN 2022

The State of Cloud Security Report 2022

Table of Contents

Introduction

A RAPIDLY SHIFTING CLOUD SECURITY LANDSCAPE

Cloud computing ushered in the greatest transformation in IT in decades, and now the cloud is going through its own transformation — with profound implications for security.

Cloud has been used predominantly as a platform for hosting third-party applications or those migrated from a datacenter. In this model, cloud environments largely resemble their data center counterparts, with familiar-looking virtual machines and networks. IT engineers use cloud consoles to configure the infrastructure needed to host applications, or to provide infrastructure for developers who are building applications to run natively in the cloud. It's the infrastructure constraints that determine how the application must be developed.

But the adoption of infrastructure as code (IaC), DevOps, and cloud native services and architectures is changing how we use the cloud, and what's needed to keep cloud environments secure. IaC means cloud infrastructure now has its own software development life cycle (SDLC), often involving CI/CD pipelines. The boundary between infrastructure and application is blurring. Infrastructure has become a part of the application — and developed alongside it using IaC. In this model, it's the application requirements that determine the necessary infrastructure.

This shift is blurring the boundaries between the traditional silos of development, operations, and security — and leading to a convergence of security responsibilities. The use of IaC presents the opportunity to shift left and address cloud security earlier in the SDLC, when it's faster and easier to do so. Engineers are taking more ownership over cloud security, motivated in part by the desire to improve productivity and deployment speed.

For this report, Snyk surveyed more than 400 cloud engineering and security professionals to better understand the cloud risks and challenges they face, and how they're successfully improving their cloud security efforts.

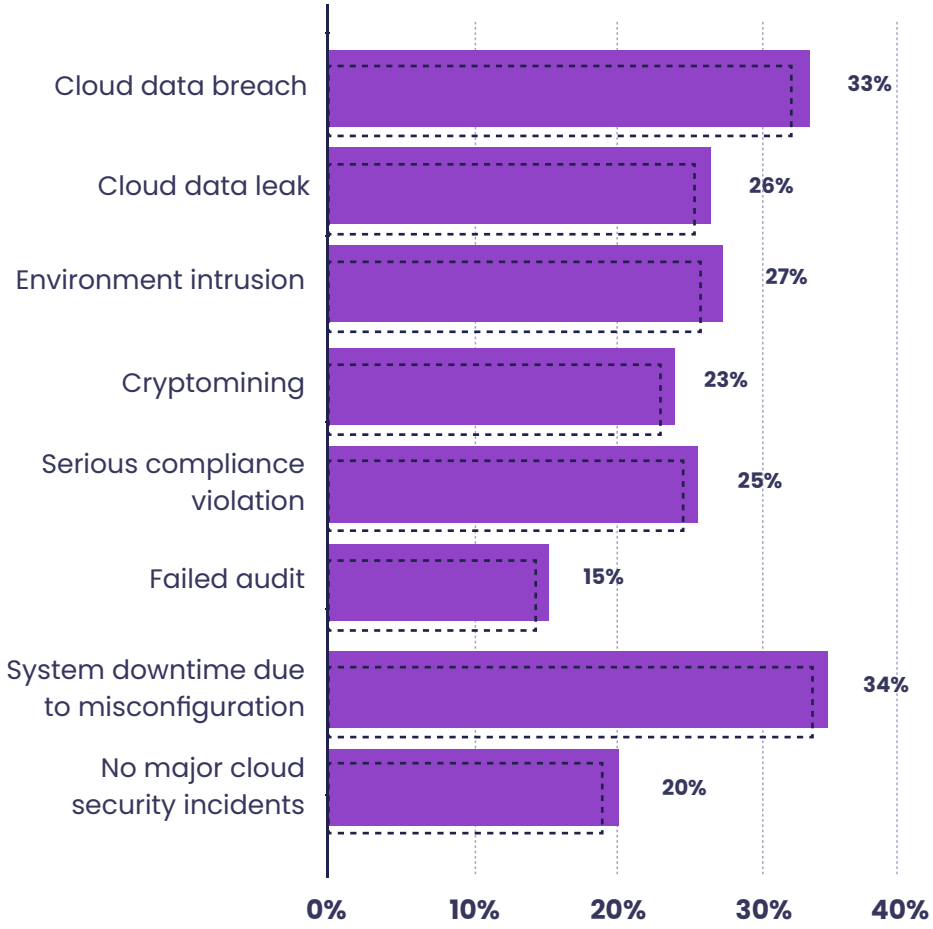
An overview of cloud risks

OF ORGANIZATIONS EXPERIENCED A SERIOUS CLOUD SECURITY INCIDENT DURING THE LAST YEAR

Cloud customers suffered a range of major security events within the past year, with data breaches, data leaks, and intrusions into their environments among the most serious. Among survey respondents, 25% worry that they've suffered a cloud data breach and weren't aware of it. These security incidents can carry a high cost: fines for failed audits and compliance violations, cryptomining on the customer's cloud bill, and loss of business due to system downtime.

In fact, concerns about the risks posed by possible misconfigurations are not new; the 2021 State of Cloud Security Report revealed that more than 8 out of 10 respondents were worried that they were vulnerable to a major data breach related to cloud misconfiguration. This points to a persistent challenge for organizations investing in cloud infrastructure and underpins the argument for better cloud security.

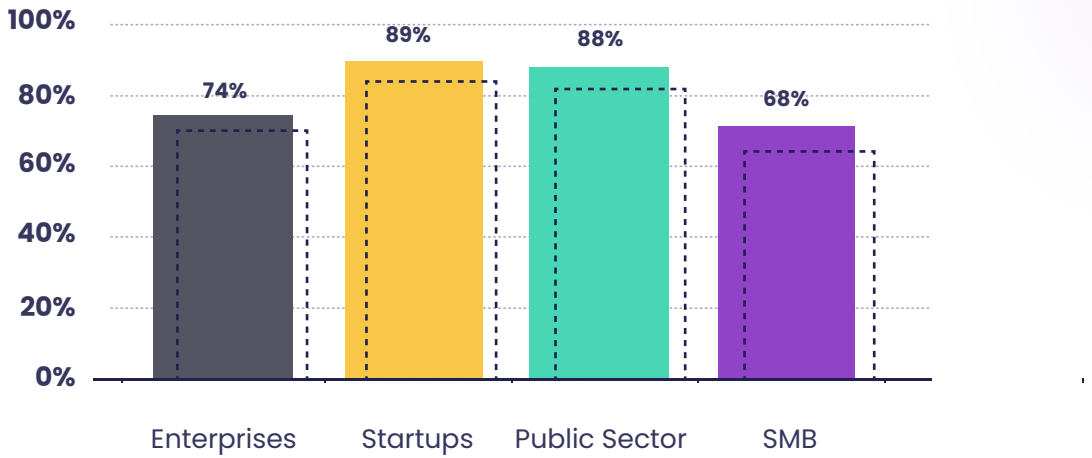
Serious cloud security incidents experienced



PUBLIC SECTOR ORGANIZATIONS (88%) AND STARTUPS (89%) WERE MOST IMPACTED

Cloud customers representing organizations of all sizes and industry sectors were impacted by major cloud security events.
Fast-growing startups fared the worst, with 80% impacted. Public sector entities (government agencies and not-for-profit organizations) experienced nearly the same impact. Enterprise companies did better — most likely due to more investment in cloud security and a bigger focus on infrastructure as code security. Small and mid-sized businesses reported faring the best, likely due to smaller cloud scale, less infrastructure complexity, and fewer changes made to their environment — or to being unaware of cloud security incidents that did occur. In all segments, more than 80% of respondents experienced a serious incident in the last year. This is clear evidence that the traditional approach to securing the cloud is failing.

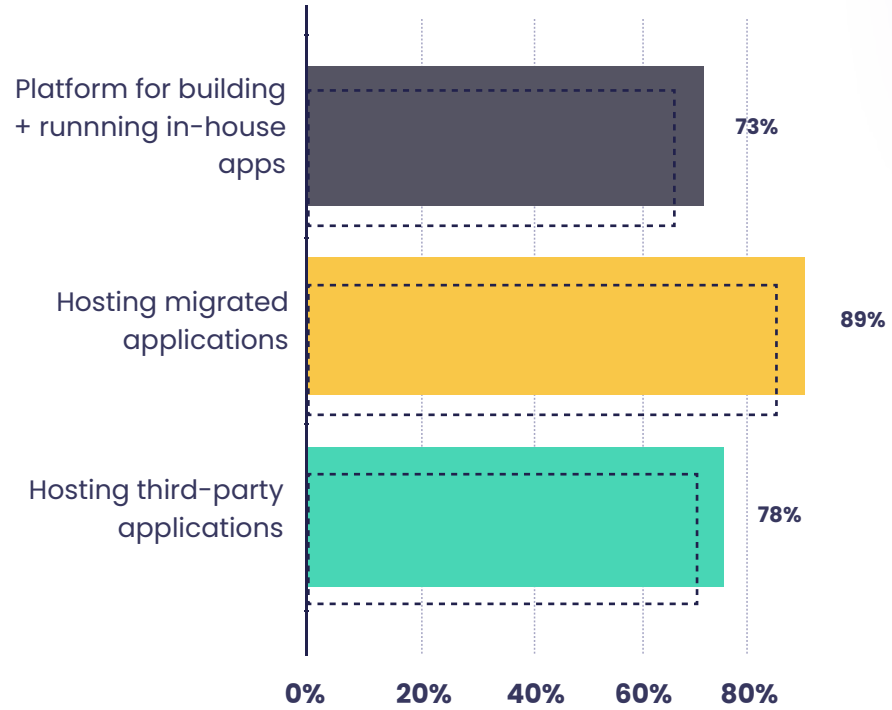
Experienced a serious cloud security incident in the past year



ORGANIZATIONS HOSTING APPLICATIONS MIGRATED FROM A DATA CENTER SUFFERED THE MOST

Companies using the cloud primarily as a platform for hosting applications that were migrated from a data center most often reported serious cloud security incidents in the past year, at 89%. Of companies using their cloud environment to host third-party applications, 78% reported serious security incidents in the past year. Teams using the cloud as a platform for building and running their own in-house applications reported the fewest cloud security incidents (73%), which may be explained by them having more visibility into, and control over, the development life cycle of their applications and cloud infrastructure. These figures show that using existing cloud security tools and approaches are profoundly failing the market.

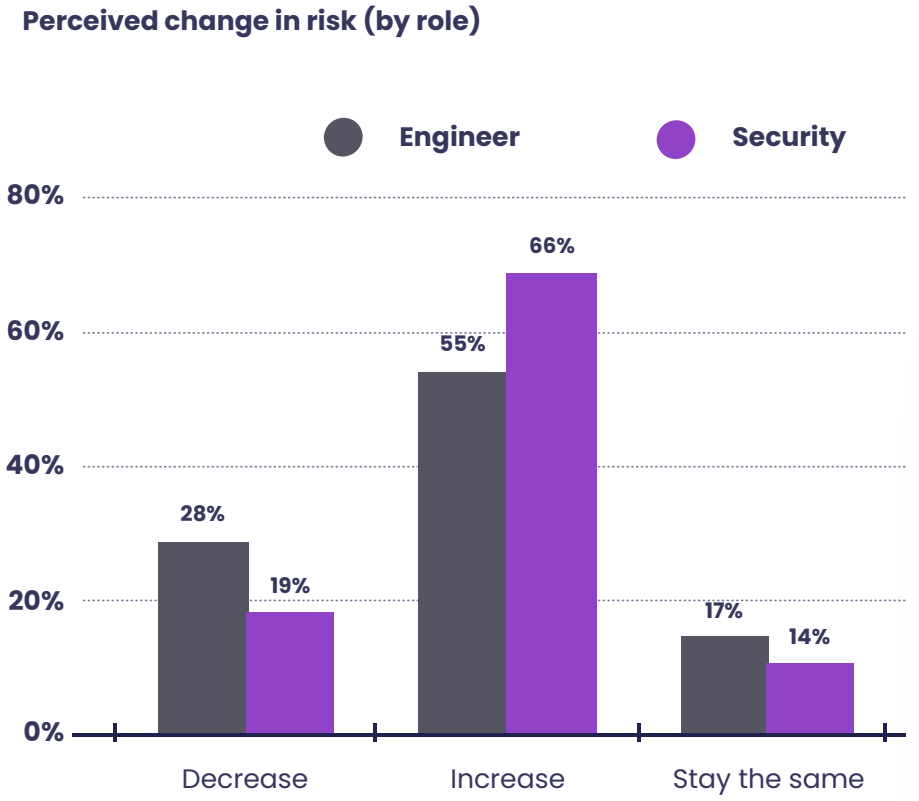
Serious cloud security incidents by use case



Cloud risk predictions

58% OF DEVELOPERS AND SECURITY PROFESSIONALS PREDICT INCREASED RISK OVER THE NEXT YEAR

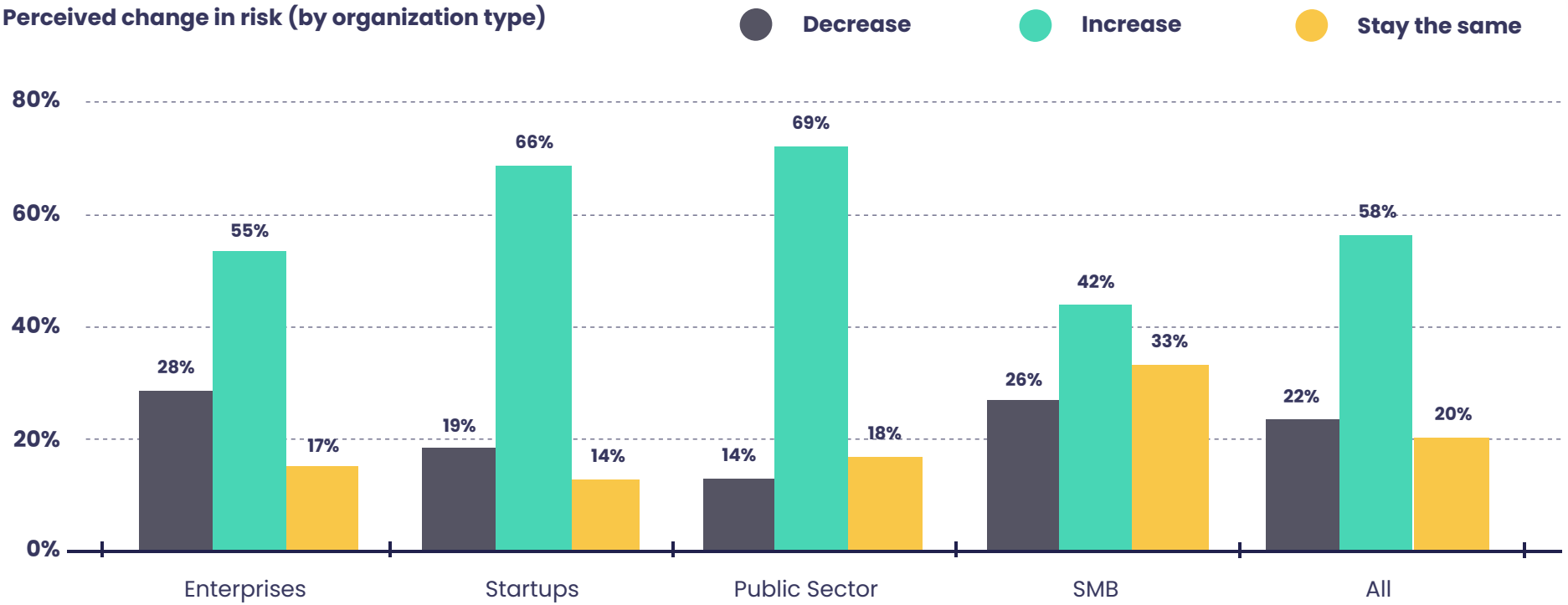
A clear majority of cloud security and engineering professionals believe that the risk of a cloud data breach at their organization will increase over the next year, with only 20% expecting risks to decrease. Security professionals are more pessimistic than cloud engineers, with 66% believing cloud risks will increase, as opposed to 55% of engineers. This may be because cloud engineers more often address security in development and CI/CD using IaC security methods, significantly reducing the rate of misconfiguration by a median of 70%. Despite the delta between the views held by security professionals versus engineers, it is notable that a majority of both groups view the problem as getting worse, not better.



STARTUP AND PUBLIC SECTOR PROFESSIONALS ARE MORE PESSIMISTIC ABOUT CLOUD RISK

Startups and public sector organizations expressed the most pessimistic outlook about cloud risks for the upcoming year. Because these organizations experienced the highest rate of major security incidents during the past year, and because their infrastructure as code adoption rate is lower, this position is understandable.

Perceived change in risk (by organization type)



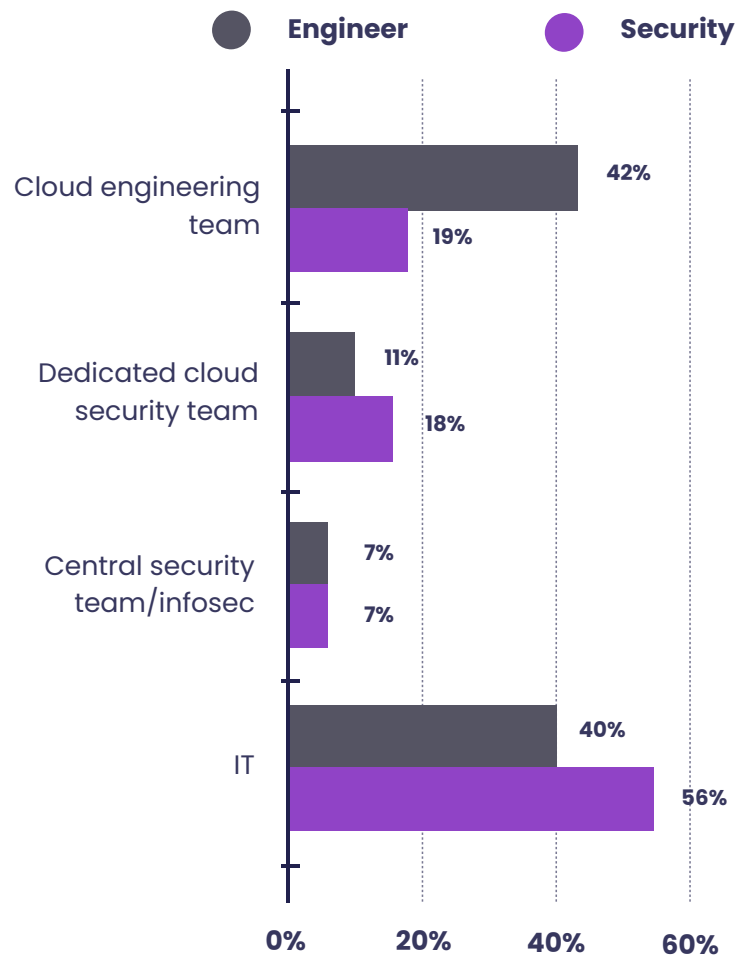
Who owns cloud security?

IT MANAGES CLOUD SECURITY IN HALF OF ALL ORGANIZATIONS... BUT NOT EVERYONE THINKS SO

The responsibility of cloud security consistently falls to IT in roughly half of organizations. Responses differ, however, depending on who you ask. 42% of cloud engineers say that their team is primarily responsible for cloud security, while only 19% of security professionals believe that to be the case. This may be explained by the increased adoption of infrastructure as code for deploying and managing cloud environments, and the desire to find and fix issues in development rather than post-deployment (when remediations require more time and resources).

This illustrates that there is a communication gap between engineering and security, likely exacerbated by separate teams having different views into the cloud from different tools. To make significant improvements, there needs to be a common toolset and common information on cloud security between the development, operations, and security teams.

Who's primarily responsible for cloud security?

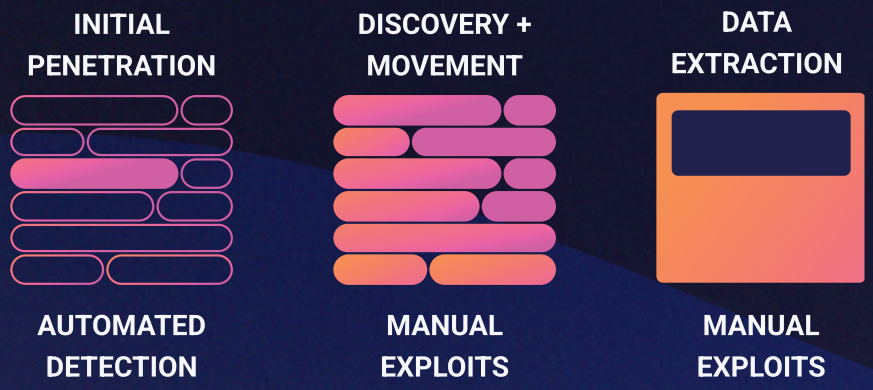


In depth: Cloud vulnerabilities

MISCONFIGURATION AND CONTROL PLANE COMPROMISE RISK

The cloud control plane is the collection of APIs that cloud providers make available to engineers so they can build and configure environments. Access to these APIs includes resource access to policies, as well as identity and access management (IAM) settings. Cloud "console" interfaces and infrastructure as code (IaC) tools operate against these APIs.

This granting of access is what makes the cloud control plane such a useful attack surface. Cloud attackers use automation to detect misconfigurations and other vulnerabilities they can exploit. After they gain access to an environment, they use resource API keys to compromise the cloud control plane for discovery, movement, and data extraction — outside of the oversight of traditional network security and intrusion detection tools.

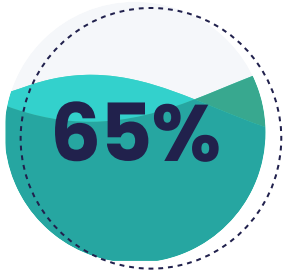


Data Center Attack Strategy	Cloud Attack Strategy
1. Pick a target	1. Search for vulnerabilities
2. Search for vulnerabilities	2. Pick a target
3. Low and slow data exfilration	3. "Smash and grab" data exfiltration

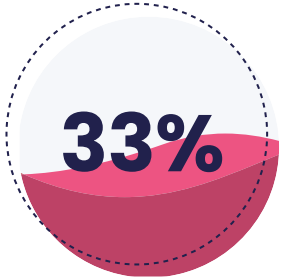
Unlike data center breaches, which are typically "low and slow" exfiltration exercises designed to evade network monitoring tools, cloud attacks are often "smash and grab" events. These events occur on the cloud provider backplane, which cannot be monitored with network security tools. Some of the most sophisticated cloud customers have fallen victim to control plane compromise attacks.

PROTECTING AGAINST CONTROL PLANE COMPROMISE RISKS

Every major cloud data breach involves attackers compromising the cloud API control plane for discovery, movement, and extraction. The good news is that there is solid awareness of control plane compromise risk equally among cloud engineering and security professionals. Two-thirds of respondents to the survey reported that their organizations are adequately protecting against control plane compromise attacks.A third of respondents, however, say they aren't practicing these protective measures.



ADEQUATELY PROTECTING AGAINST CPC RISKS



INADEQUATE OR NO EFFORT TO ADDRESS CPC RISKS

THE ROLE OF CLOUD SECURITY ARCHITECT

CLOUD SECURITY ENGINEERS AND ARCHITECTS ON THE TEAM

Cloud control plane compromise attacks exploit architectural misconfigurations that involve more than one resource. Because of this complex risk factor, the role of cloud security architect has become increasingly important for organizations that want to understand and address this problem. More than two thirds of all organizations have cloud security architects on their teams.

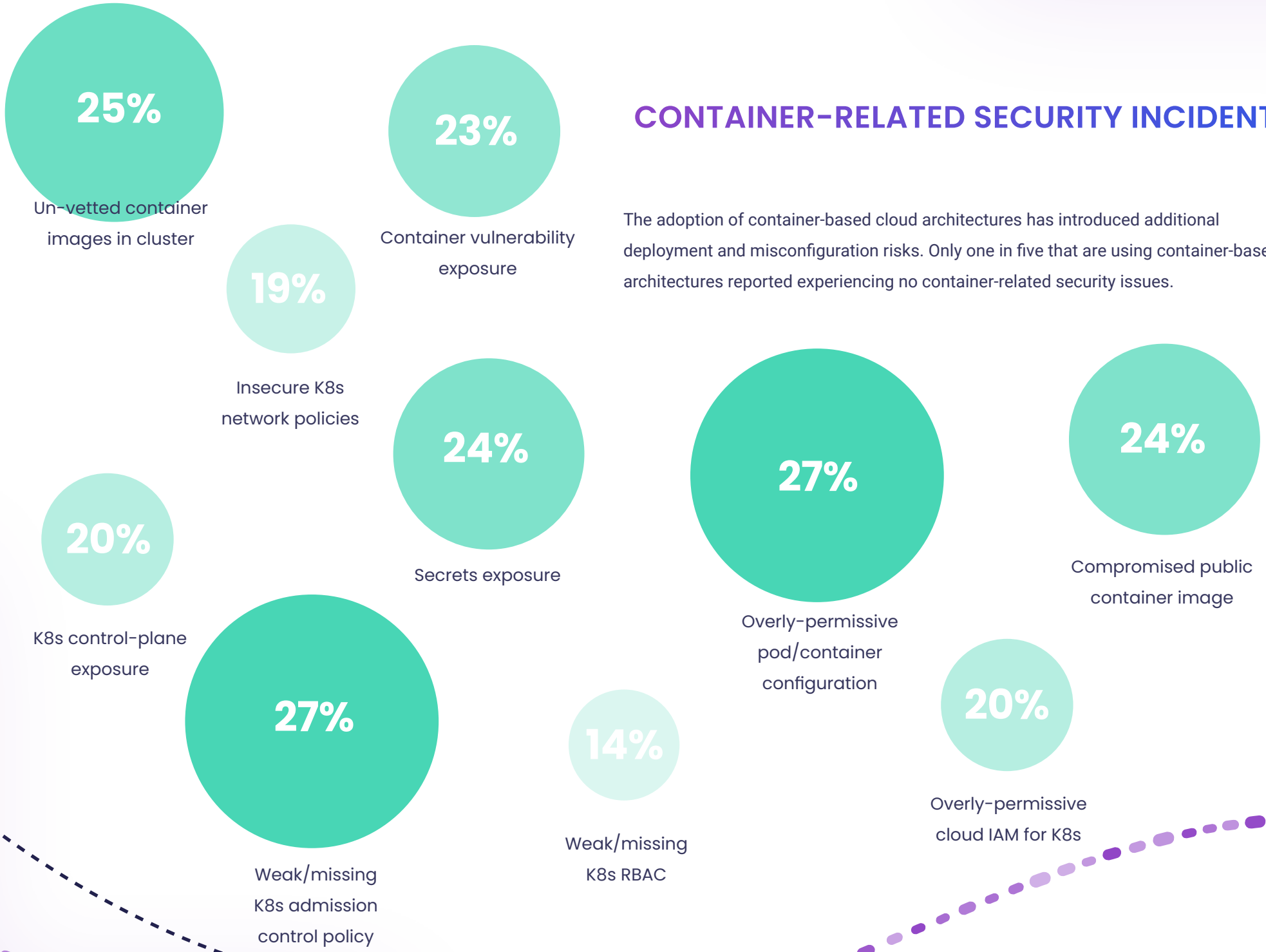
CLOUD SECURITY INCIDENTS

Cloud resource misconfigurations represent the primary risk for every organization using the cloud. These mistakes happen when organizations use either cloud provider consoles or infrastructure as code to configure and deploy their cloud infrastructure.

When IaC isn't being used, or when runtime misconfigurations can't be tied back to the IaC templates that were used to create and manage an environment, it's common for the same vulnerability to appear over and over again after remediation. The combination of deployment misconfiguration and unapproved changes made post-deployment results in a significant rate of cloud security incidents to be addressed.

CONTAINER-RELATED SECURITY INCIDENTS

The adoption of container-based cloud architectures has introduced additional deployment and misconfiguration risks. Only one in five that are using container-based architectures reported experiencing no container-related security issues.

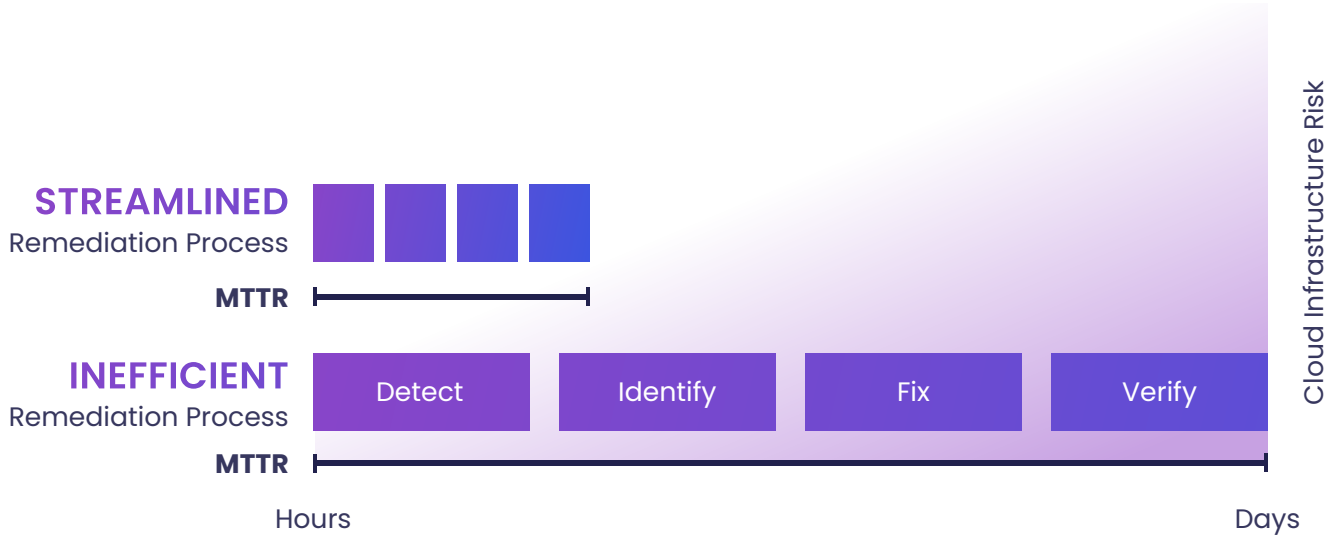


REMEDIATING CLOUD MISCONFIGURATION INCIDENTS

Cloud attackers have adopted automation tools to scan the internet, searching for cloud misconfigurations they can exploit to gain access to an environment. Due to the mutability of cloud resource configurations and the increased adoption of CI/CD, the rate of misconfiguration can become quite significant. Our 2021 survey revealed that half of organizations surveyed are experiencing 50 or more cloud misconfigurations per day.

Mean Time to Remediation (MTTR) is a key security metric for measuring the response effectiveness of cloud misconfiguration risk. The longer cloud misconfigurations go unaddressed, the greater the risk of a major security incident. Where there is a lack of effective collaboration, automated tooling, and an ability to tie runtime issues back to IaC, the MTTR for cloud misconfiguration is often days or weeks.

HAVE AN MTTR OF UNDER AN HOUR FOR CLOUD MISCONFIGURATION



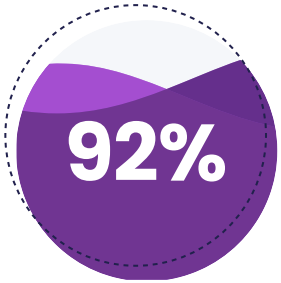
Shifting left: infrastructure as code (IaC) security

THE ADOPTION OF IAC ENABLES ORGANIZATIONS TO SHIFT LEFT ON CLOUD SECURITY

The introduction and rapid adoption of infrastructure as code (IaC) and continuous integration /continuous deployment (CI/CD) have led cloud operations teams to borrow key principles from the software development lifecycle. The phases of the cloud infrastructure SDLC include design, development, testing, deployment, and monitoring.

When cloud engineers spin up cloud environments, they are defining the security of their infrastructure through configuration — and changing it often. IaC brings the risk of automating the deployment of cloud misconfigurations at scale. However, IaC also presents teams with the opportunity to verify the security of cloud infrastructure earlier in the SDLC — pre-deployment — which can save time and reduce the frequency of runtime misconfiguration issues.

THE ROI FOR IAC SECURITY: RISK REDUCTION

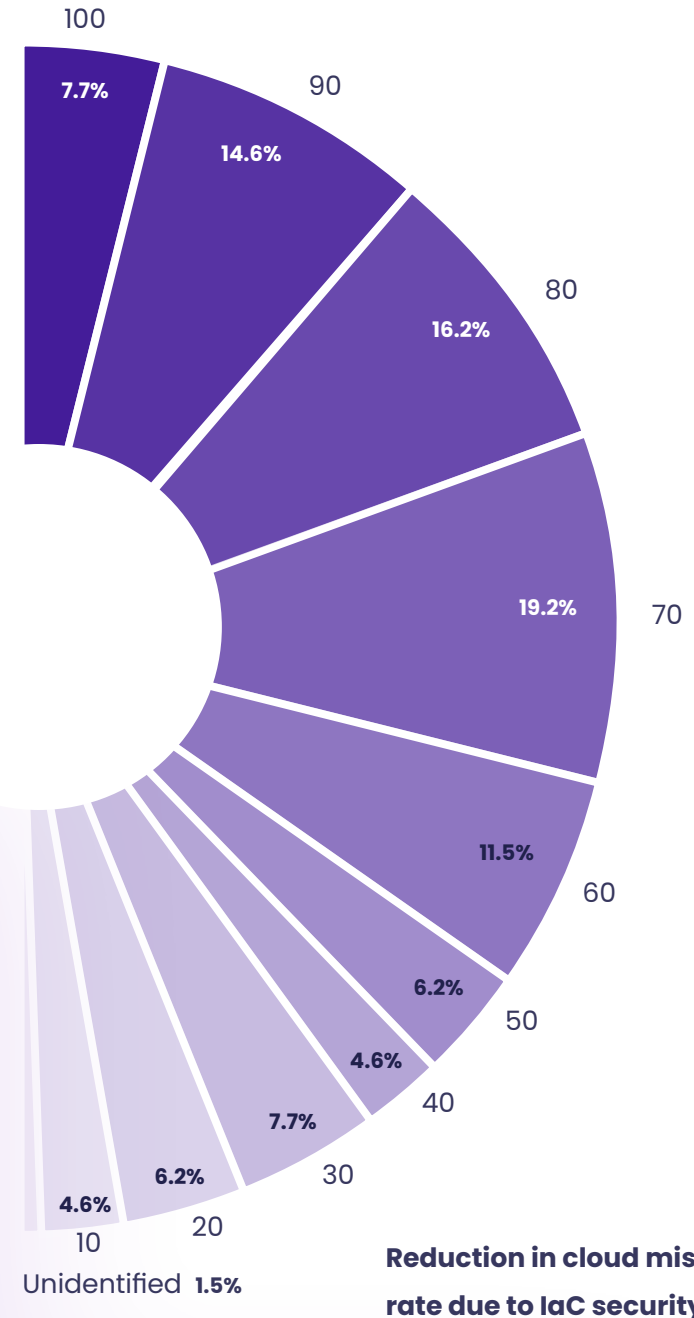


IAC SECURITY USE AMONG IAC USERS

MEDIAN REDUCTION OF MISCONFIGURATION RESULTING FROM IAC SECURITY

-

By confirming the security of IaC pre-deployment, cloud engineering and security teams can significantly reduce the rate of runtime misconfiguration and improve productivity across teams. When cloud misconfigurations can be tied back to the IaC that deployed it, the process of remediations can be considerably streamlined and the MTTR minimized.



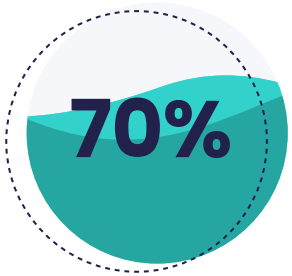
Reduction in cloud misconfiguration rate due to IaC security

INFRASTRUCTURE AS CODE SECURITY REDUCES MISCONFIGURATION BY 70%

A significant factor in improving cloud security efforts is infrastructure as code (IaC) security addressed pre-deployment, during development and CI/CD. The adoption of IaC means there's a software development lifecycle for cloud infrastructure — and the opportunity to shift left on cloud security. Poll respondents reported that using infrastructure as code methods resulted in a 70% median reduction in cloud misconfiguration, significantly reducing cloud risk.

In addition to empowering cloud engineers with tools to verify the security of IaC in development (92%), many teams are building IaC security checks into their CI/CD pipelines (80%).

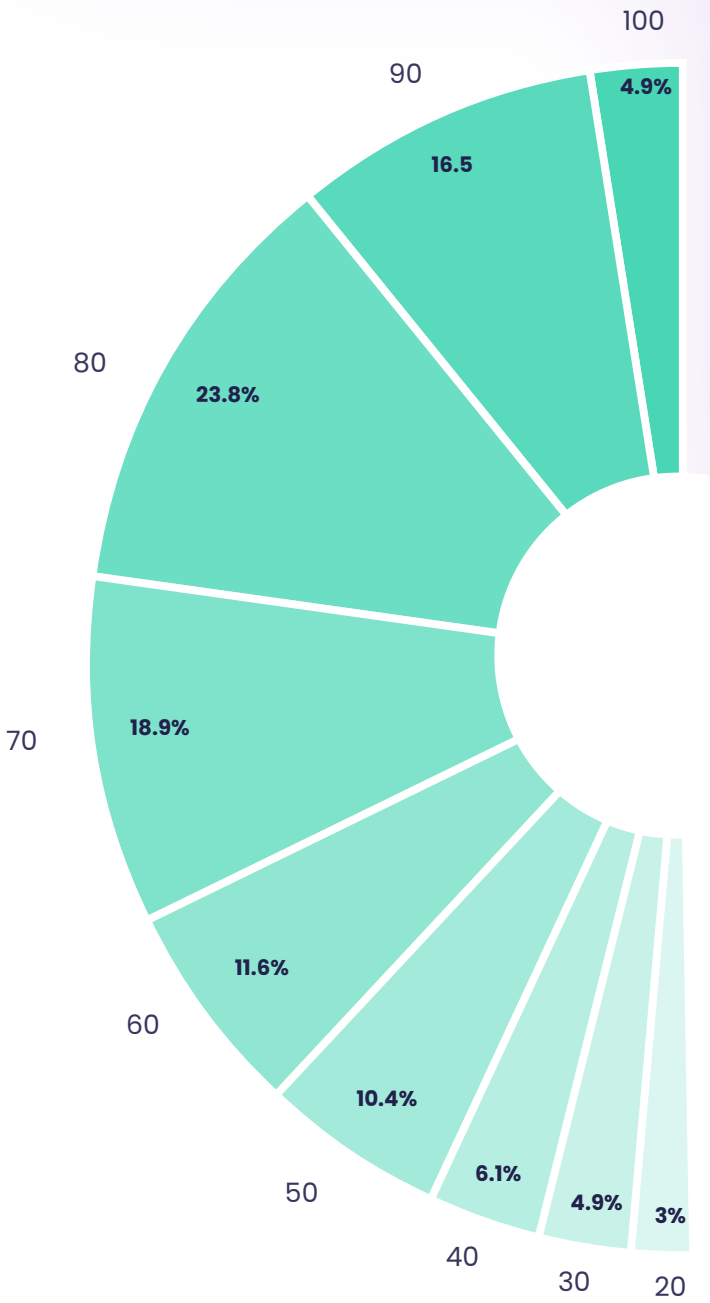
THE ROI FOR IAC SECURITY: INCREASED PRODUCTIVITY



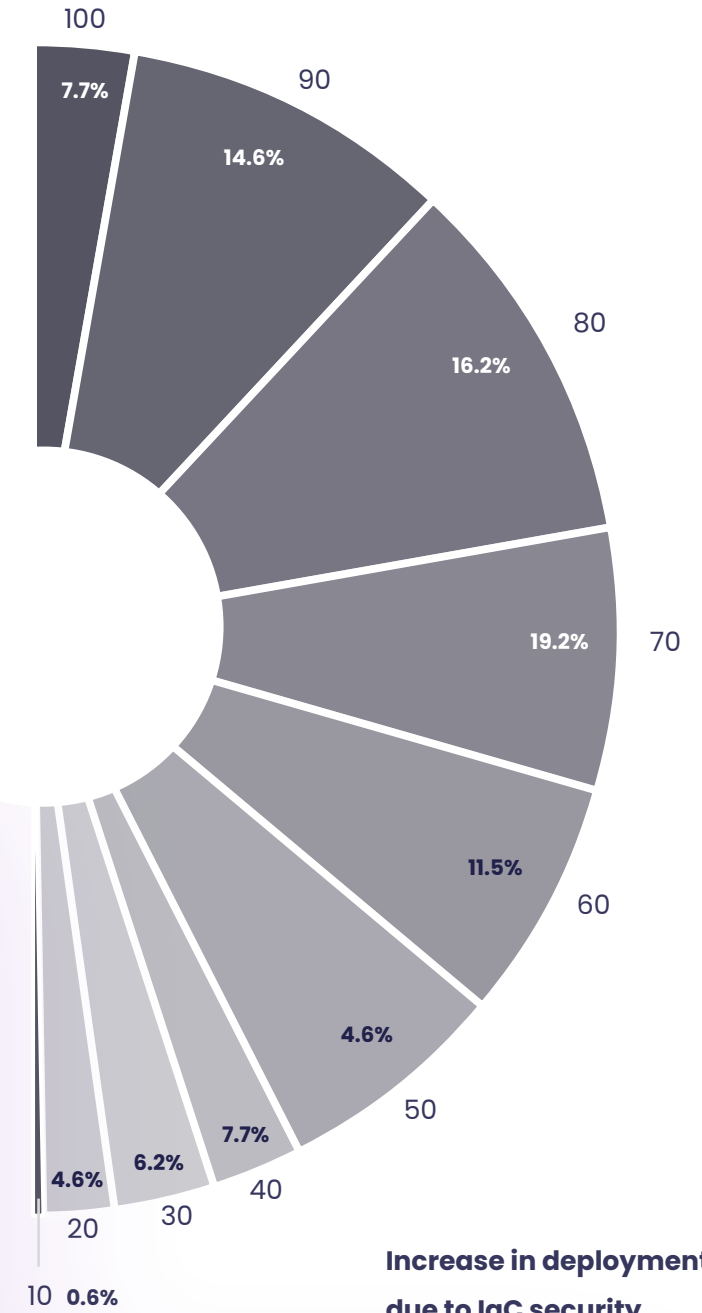
MEDIAN PRODUCTIVITY IMPROVEMENT FOR CLOUD ENGINEERS RESULTING FROM CHECKING IAC IN DEVELOPMENT

45% of respondents in 2022 said that cloud security processes require significant cloud engineering resources. (Notably, our 2021 survey revealed that half of cloud engineering teams invest 50 or more hours per week managing cloud security issues.)

Because using and regulating IaC in development creates a reduction in runtime misconfigurations, it also increases productivity for the cloud engineers who are responsible for remediation. Nearly a quarter of respondents claimed productivity improved by 80% among engineers responsible for cloud security tasks.

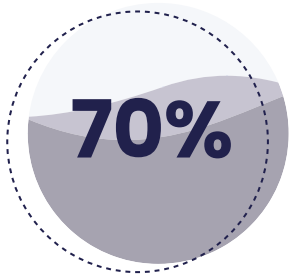


Increase in engineer productivity due to IaC security



Increase in deployment approval speed due to IaC security

THE ROI FOR IAC SECURITY: DEPLOYMENT SPEED



MEDIAN INCREASE IN SPEED OF DEPLOYMENT APPROVALS RESULTING FROM CHECKING IAC IN DEVELOPMENT

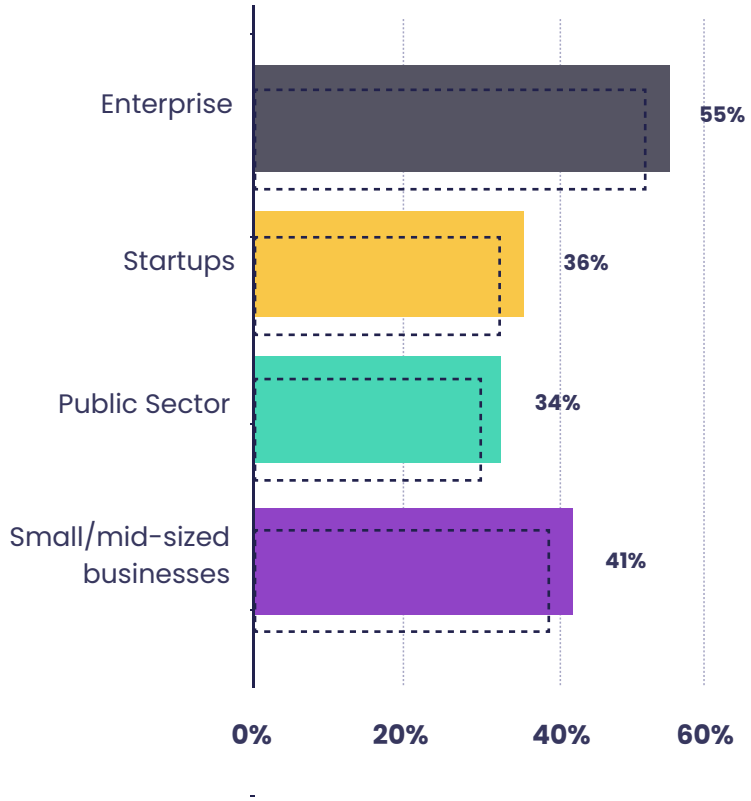
Cloud engineering teams have increasingly automated the integration and deployment of IaC, but security review and approval processes can slow down the pace of deployments.

Verifying IaC security in development can significantly reduce the time required to certify the security of cloud deployments. Deployment speed increased by a median of 70% due to IaC security checks, largely because IaC security checks can power automated approvals and reduce the need for rework.

ENTERPRISES LEAD THE WAY IN USING INFRASTRUCTURE AS CODE

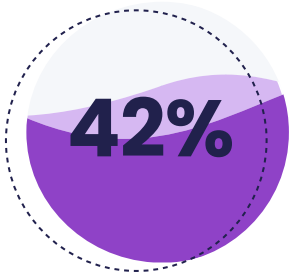
The adoption rate of IaC is not distributed evenly. Enterprises are out in front in leveraging the technology — and the ability to get security right pre-deployment. This may be because enterprises focus more on planning, and are increasingly making IaC a requirement for cloud deployments due to its speed and efficiency benefits. This may also explain why preventing security issues pre-deployment is the top enterprise cloud security objective. On the other hand, startups tend to build fast and experiment, which may result in a failure to use IaC from the beginning. Public sector organizations lag behind all other categories when it comes to adopting IaC.

Infrastructure as Code Adoption



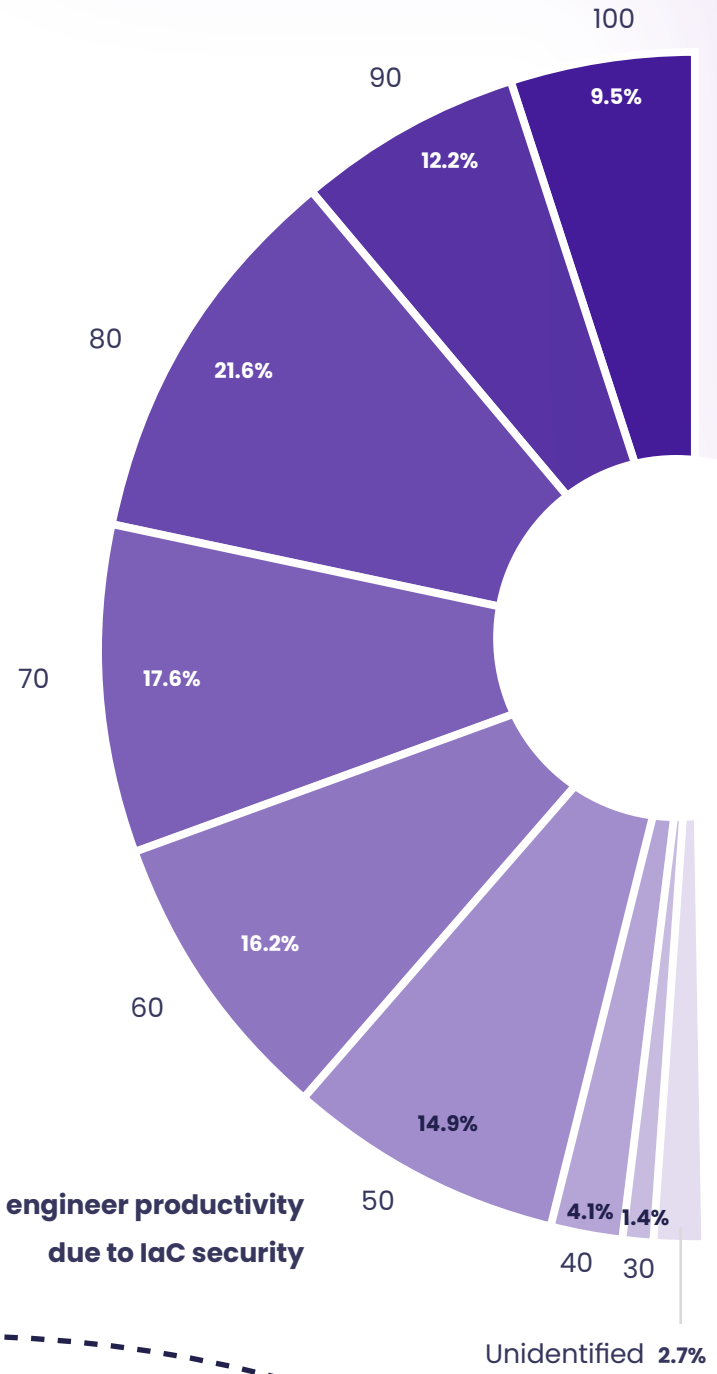
THE SCOPE OF IAC USE FOR CLOUD ENVIRONMENTS

When IaC is used for cloud infrastructure, it's typically done alongside the cloud service provider consoles. A majority of IaC users are still using it only for the initial provisioning of cloud infrastructure, and then rely on cloud consoles for ongoing updates and management of their environment. However, 42% of IaC users are now using IaC for provisioning and ongoing management of their cloud infrastructure — a positive trend that makes it possible to continue using IaC security and to connect runtime issues back to code to streamline the remediation process and avoid mistakes.



USING IAC FOR CLOUD PROVISIONING AND ONGOING MANAGEMENT

Also important to note: when IaC is used, it generally doesn't involve the entire cloud environment; cloud consoles are used to create some of the infrastructure. Cloud security For organizations that have adopted IaC, the median percentage of their cloud environment they manage using IaC is 70%, which is considerable, and a positive sign for cloud security.

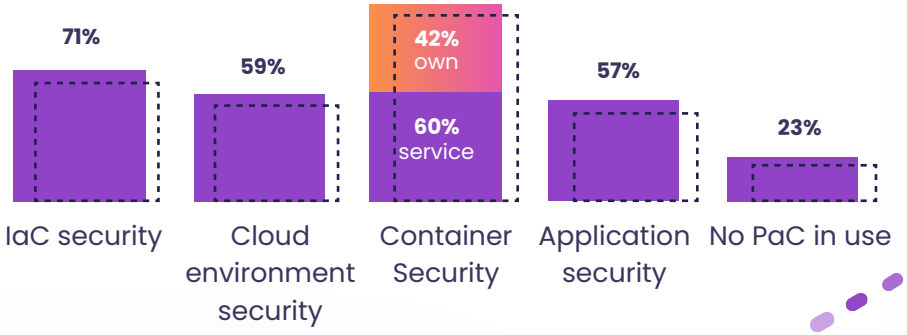


POLICY AS CODE USE FOR CLOUD SECURITY

Policy as code (PaC) — sometimes called “security as code” — makes it possible to express security and compliance rules in a language that an application can use to automatically validate correctness. In the cloud security context, PaC can be used to check other code (i.e. IaC) and running environments for unwanted conditions that could invite exploitation or result in a regulatory compliance violation.

PaC can reduce human error by removing ambiguity and differences in how policies should be interpreted, applied, or enforced. PaC options for cloud security include proprietary vendor offerings and open source frameworks, such as Open Policy Agent (OPA), a project of the Cloud Native Computing Foundation.

Use of policy as code



ABOUT OPEN POLICY AGENT

Open Policy Agent (OPA) is an open source policy as code framework and a project of the Cloud Native Computing Foundation (CNCF). OPA is popular in the Kubernetes community and can be used for a wide range of use cases, including evaluations of infrastructure as code and running cloud infrastructure. OPA includes the Rego query language and an active ecosystem of support and tooling, and tooling purpose-built for IaC security, such as Regula. Companies like Netflix, Capital One, Atlassian, Goldman Sachs, and CloudFlare use and support OPA, and it should be considered in any PaC selection process.

Learn more about OPA at https://www.openpolicyagent.org/.

Cloud security challenges

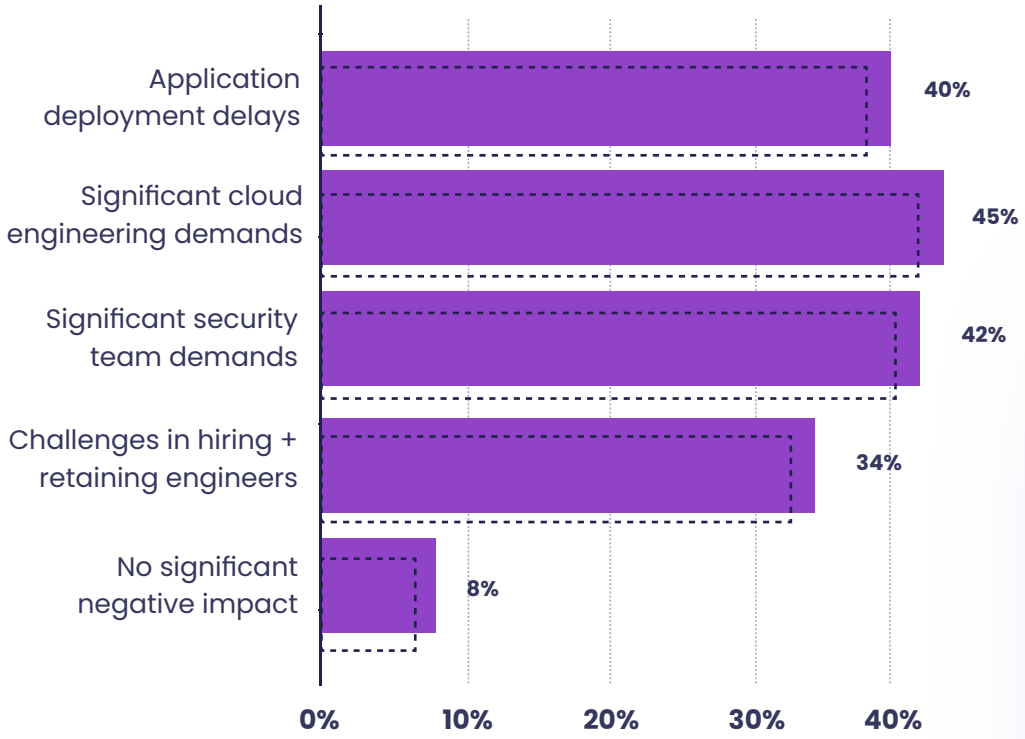
45% OF RESPONDENTS AGREE THAT CLOUD SECURITY WORK TAKES UP SIGNIFICANT ENGINEERING RESOURCES

Inefficient cloud security processes can be the rate-limiting factor for how fast teams can work in the cloud — and how productive they can be. Respondents identified significant demands on cloud engineers as the top impact of poor cloud security processes. Cloud runtime misconfiguration incidents can demand significant security team resources: identifying, prioritizing, and routing misconfigurations to engineering teams is time-consuming. Long security and review processes can delay application and feature deployments, and time spent on manual security work and approvals can make it more difficult to hire and retain engineering talent.

Top impact of inefficient cloud security process (by org)

Enterprises	Significant investment of security team resources
Startups	Significant investment of cloud engineering resources
SMBs	Significant investment of cloud engineering resources
Public sector	Application and feature deployment delays

Impact of inefficient cloud security efforts



77% OF ORGANIZATIONS CITE PROBLEMS WITH POOR TRAINING AND COLLABORATION AS A MAJOR CHALLENGE

Many cloud security failures result from a lack of effective cross-team collaboration and team training. When different teams use different tools or policy frameworks, reconciling work across those teams and ensuring consistent enforcement can be challenging. Insufficient tooling that produces false positives leads to alert fatigue within security teams, which itself contributes to human error when identifying critical issues that need to be addressed quickly. Issues with inconsistent policy interpretations and a lack of education most likely reveal the need for policy-as-code based tooling and automation.

What cloud security challenges exist within your organization?

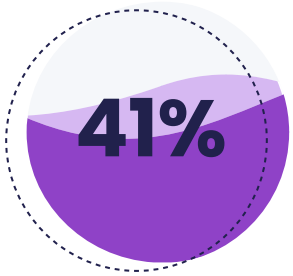
CHALLENGES RELATED TO TRAINING AND COLLABORATION

- 13% We lack sufficient cloud security expertise
- 17% Not enough cloud security education and training
- 22% Poor collaboration between teams
- 19% Understanding how security policies apply to specific use cases
- 21% Different interpretations of cloud security policies across the organization
- 30% Human error when identifying, prioritizing, or remediating issues
- 20% Different teams using different cloud security tools or policy frameworks

OTHER CHALLENGES

- 20% Alert fatigue and false positives
- 18% Poor visibility into our environment and security posture
- 21% Addressing cloud security issues pre-deployment
- 19% Audit preparation and reporting
- 22% Lack of security investment

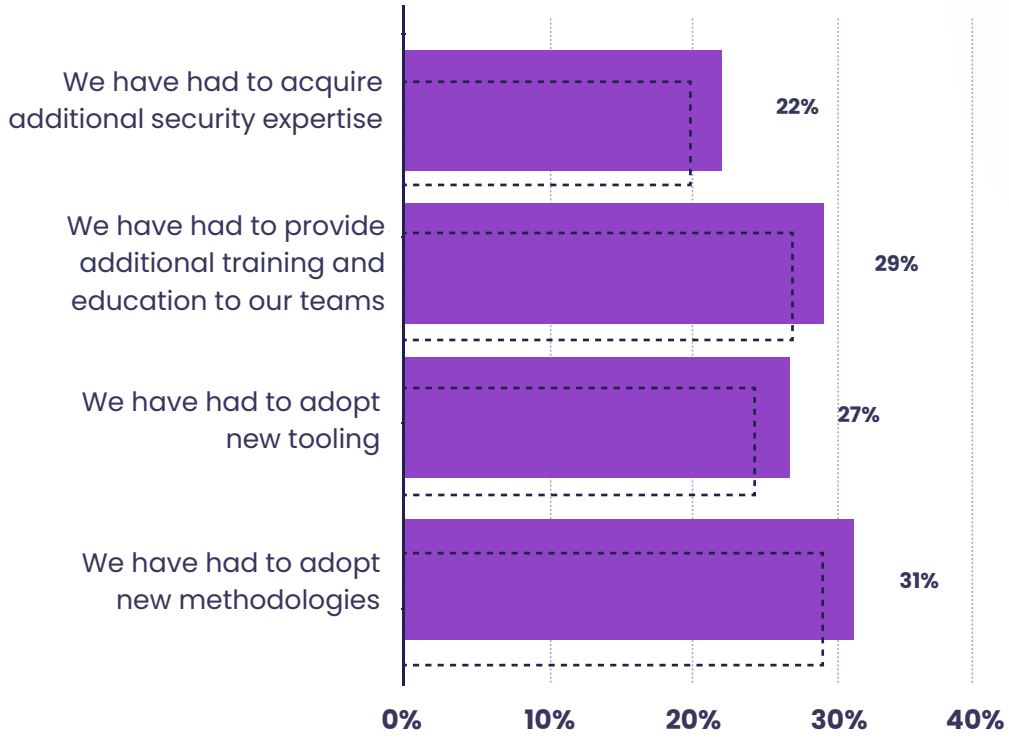
CLOUD NATIVE TEAMS NEED MORE EXPERTISE, DIFFERENT TOOLING, AND NEW APPROACHES



INCREASED SECURITY COMPLEXITY DUE TO CLOUD-NATIVE SERVICE ADOPTION

The adoption of cloud-native services and architectures, such as container-based and “serverless” (i.e Functions as a Service), raises new security considerations and requirements. A cloud native approach can improve developer speed and agility, but 41% of respondents cited it as a major impact on their cloud security effort because it creates more complexity. To address security issues pre-deployment, teams have to add specific expertise related to cloud native security, set up additional training and education, and shift left on cloud security.

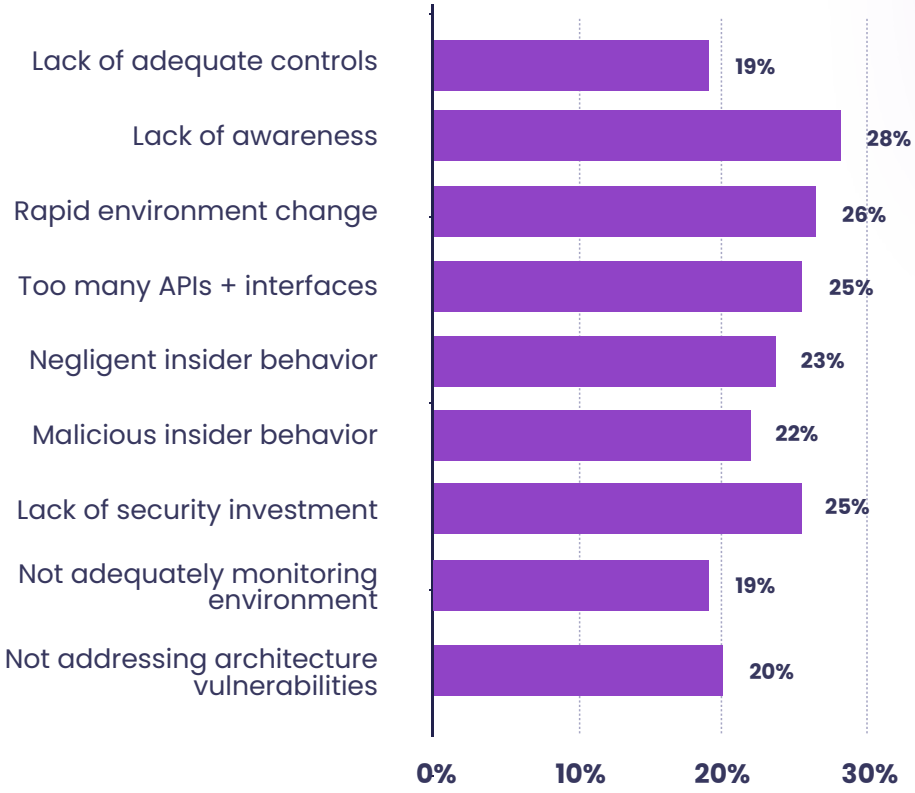
Impact on security from cloud native architecture adoption



CAUSES OF CLOUD SECURITY FAILURES

There are as many underlying causes of cloud security failures as there are types of cloud misconfigurations. The top cause cited is a lack of awareness of cloud security policies — an issue cloud engineers are increasingly addressing with policy-based automated tooling. The next most-cited causes are rapid environment change and too many APIs and interfaces to govern — both challenges that are likely to increase as more teams adopt continuous deployment methodologies and cloud native architectures (which can involve complex API interactions in cloud environments).

Causes of security incidents



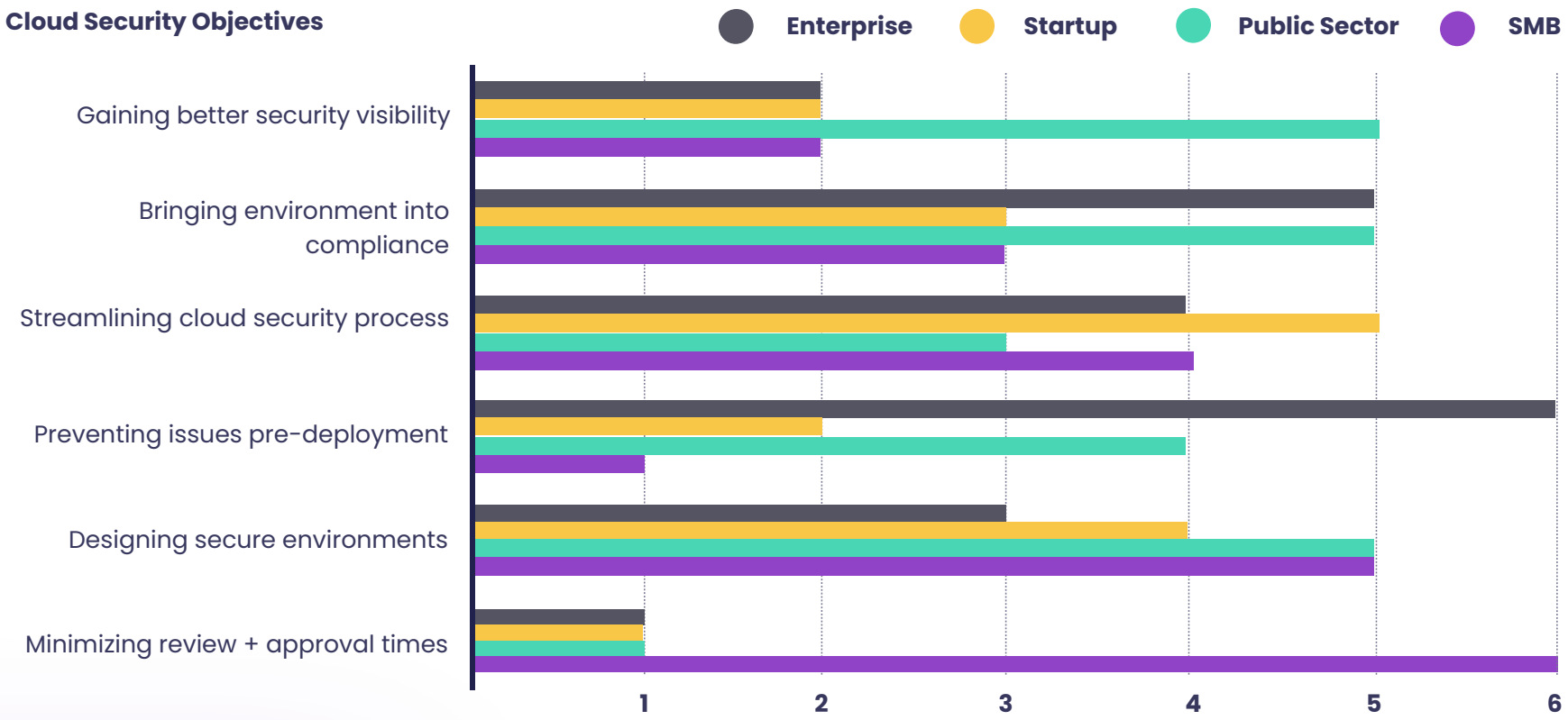
Cloud security objectives

Because cloud security programs can have a significant impact on the productivity and speed of application developers and cloud engineering teams, efforts to improve cloud security programs involve a wide range of objectives beyond security-focused priorities.

1. Designing environments to be more secure against control plane compromise attacks
2. Streamlining the process of identifying, prioritizing, and remediating misconfigurations
3. Bringing our cloud environment into compliance with regulatory requirements
4. Preventing misconfiguration pre-deployment (i.e., “Shift Left”; DevSecOps)
5. Gaining better visibility into our cloud environment and security posture
6. Minimizing the time it takes to review and approve deployments and changes

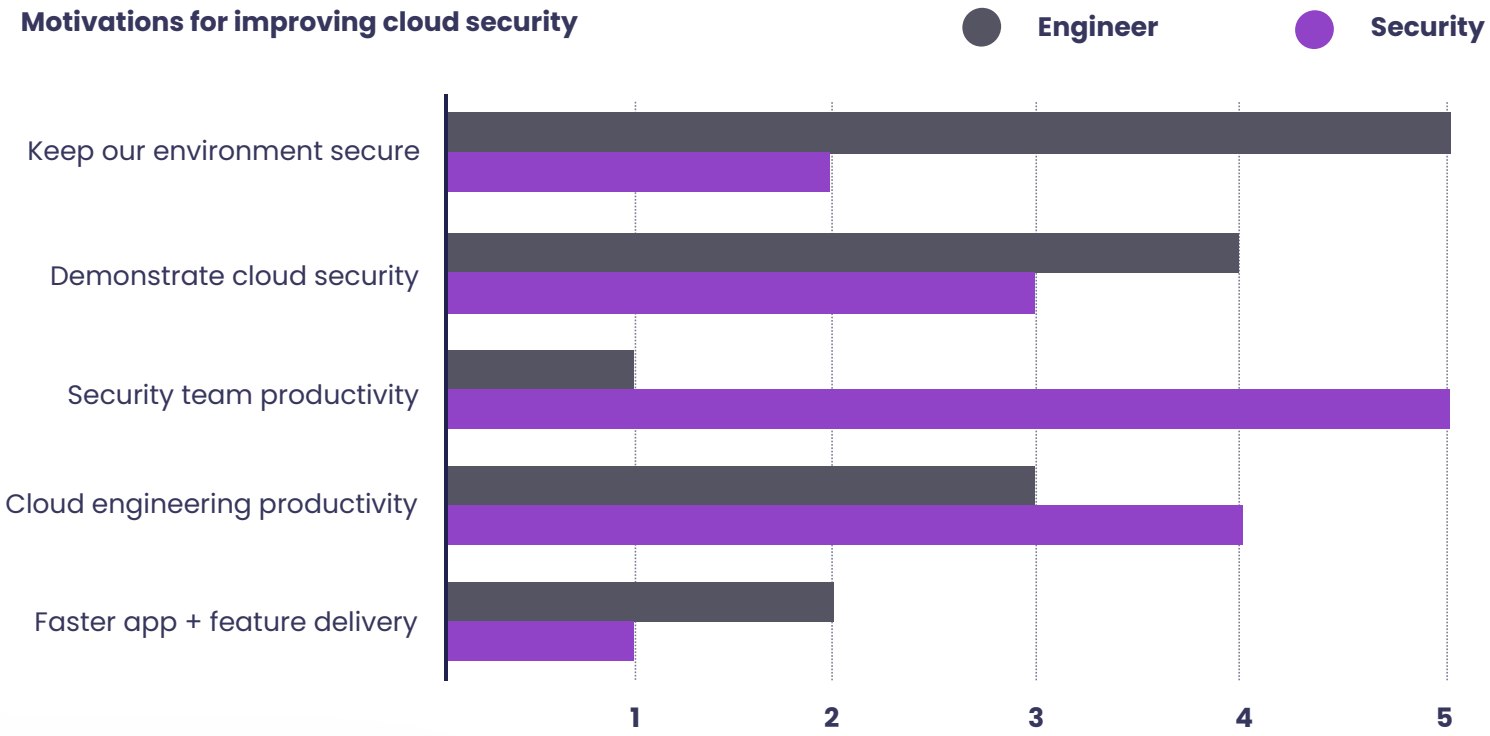
ENTERPRISE ORGANIZATIONS PRIORITIZE SECURING ENVIRONMENTS, BUT SMALL BUSINESSES ARE MORE INTERESTED IN FASTER REVIEW CYCLES

Every organization is pursuing a number of cloud security objectives, but priorities differ considerably depending on the organization type. Enterprises are focused on preventing cloud misconfiguration pre-deployment, while minimizing reviews and approval time ranks lowest for them. Small and mid-sized businesses, however, are very interested in speeding up approval times, while pre-deployment security ranks as a lower priority for them. Public sector organizations are focused on designing secure environments and bringing existing ones into compliance, while startups are equally focused on getting better security visibility and streamlining security processes.



BOTH ENGINEERS AND SECURITY EXPERTS WANT TO PRIORITIZE CLOUD SECURITY, BUT FOR DIFFERENT REASONS

While the motivation to improve cloud security efforts is primarily driven by the desire to keep cloud environments secure, there are a number of other desired outcomes, including the ability to better demonstrate that cloud security is an organizational priority. Inefficient cloud security processes can be a significant drag on team productivity, and security professionals cite a desire to improve their own productivity as their top motivation. Among all respondents, cloud engineering productivity ranked just behind keeping their environment secure.



MOTIVATIONS TO IMPROVE CLOUD SECURITY

Beyond official organization and team objectives for improving cloud security, we wanted to understand more about the underlying motivations for doing so.

Motivations for improving cloud security efforts differ by organization, and among engineers and security professionals.

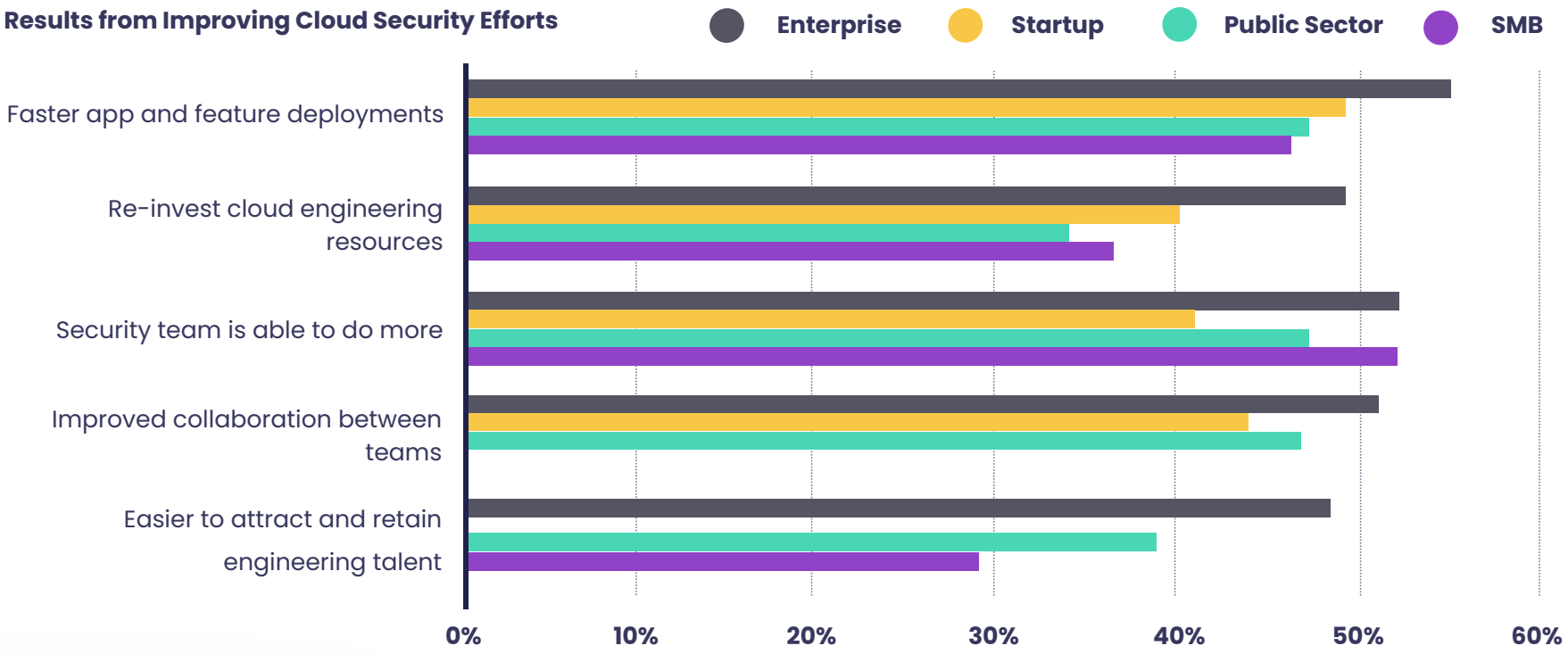
ENTERPRISE	Help cloud engineers deliver and update infrastructure faster
STARTUP	Better demonstrate cloud security to management, customers, and regulators
PUBLIC SECTOR	Help our security team do more with the resources they have
SMBS	Keeping our cloud environment secure

ENGINEERS	We will be able to do a better job of keeping our cloud environment secure
SECURITY	Our security team will be able to do more with the resources they have

1. We will be able to do a better job of keeping our cloud environment secure
2. Our cloud engineers will be able to deliver and update infrastructure faster
3. We will be able to better demonstrate cloud security to management, customers, and regulators
4. Our security team will be able to do more with the resources they have
5. Our application developers will be able to deliver applications and features faster

49% OF ORGANIZATIONS FIND THAT DEPLOYMENT HAPPENS FASTER AS A RESULT OF IMPROVED CLOUD SECURITY

Organizations and teams each have their own cloud security objectives and motivations for improving their effort, and success delivers real results across the board. 49% of respondents said that cloud security improvements resulted in faster application and feature deployments, and 48% said their security team is able to do more with the resources they have. 44% said that security improvements have led to better collaboration between teams, and 41% said it's now easier to attract and retain cloud engineering talent. When cloud security improvements result in fewer misconfiguration issues to remediate, engineering teams can reinvest their time in building value, and 40% said they've been able to do so.



Recommendations for improving cloud security

Cloud security is about the prevention of misconfigurations and architectural design vulnerabilities that make cloud control plane compromise attacks possible. Successful cloud security and engineering teams are focusing on five fundamental areas to address these threats. By operationalizing cloud security, they're reducing risk, innovating faster, and improving team productivity.

1. KNOW YOUR ENVIRONMENT

Maintain awareness of every resource running in your cloud environment, how each resource is configured, and how they relate to each other. Know the applications associated with your cloud infrastructure, and understand the data involved and how it's used. Maintain visibility over the software development lifecycle for your cloud infrastructure, including any infrastructure as code in development and any CI/CD pipelines used.

2. FOCUS ON PREVENTION AND SECURE DESIGN

The way to avoid cloud breaches is to prevent the conditions that make them possible, including resource misconfigurations and architectural design flaws (for example, design that includes insecure use of Identity and Access Management (IAM) and resource access policies). Design cloud environments that are inherently secure against cloud API control plane compromise attacks. The role of cloud security architect is critical for cloud security teams.

3. EMPOWER CLOUD DEVELOPERS TO BUILD AND OPERATE SECURELY

As infrastructure as code adoption goes mainstream, cloud engineers need tools to get security right in design and development phases of the SDLC. When engineers can develop secure infrastructure as code, they can catch and correct issues early, avoid time-consuming remediations and rework later, and deliver secure infrastructure faster. Use IaC everywhere you can, build security guardrails into CI/CD pipelines to prevent misconfigurations from being deployed, and tie runtime issues back to IaC for remediation.

4. ALIGN AND AUTOMATE WITH POLICY AS CODE (PAC)

When security policies are expressed solely in human language and exist in PDF documents, they might as well not exist at all. PaC allows for rules to be expressed in a language that other tools and applications can use to validate the correctness of code and configurations. PaC eliminates differences in interpretation, implementation, and enforcement, and makes it possible for cloud security teams to scale their efforts without having to increase headcount.

5. MEASURE WHAT MATTERS AND OPERATIONALIZE CLOUD SECURITY

Cloud security is about operational discipline and getting the right processes in place. Successful security teams identify what matters the most, be it reducing the rate of misconfiguration, speeding up approval processes, or re-allocating resources to higher-value work. They establish their baselines, set goals, and then work diligently toward achieving them. And they're able to demonstrate the security posture of their environment — and their progress — at any time.

Survey Demographic Overview

ROLE

- 24% Security executive
- 40% Security practitioner
- 16% Cloud engineering executive
- 21% Cloud engineering practitioner

CLOUD SERVICE PROVIDERS USED

- 31% Amazon Web Services
- 18% Microsoft Azure
- 23% Google Cloud
- 28% Multi-Cloud

ORGANIZATION TYPE

- 29% Enterprise
- 25% Fast-growing startup
- 23% Small/medium sized business (SMB)
- 24% Public sector (government or not-for-profit organization)

PRIMARY CLOUD USE CASE

- 29% Hosting migrated applications
- 32% Hosting third party applications
- 25% Building/running native cloud apps
- 14% A mix of hosting and building apps

snyk

DEVELOPER LOVED, SECURITY TRUSTED.

Find and automatically fix vulnerabilities in your code,open source dependencies, containers, and infrastructure as code — all powered by Snyk's industry-leading security intelligence.

Learn more at snyk.io