THE STATE OF CLOUD SECURITY 2021

A report on the risks, costs, and challenges organizations and cloud teams are experiencing in 2021.

REPORT CONDUCTED BY: Fugue | sonatype

Introduction

The cloud and digital transformation have radically changed the IT landscape and introduced new kinds of threats and security requirements. The Shared Security Model of Cloud has relieved organizations from the burdens of securing physical IT infrastructure, which is now the responsibility of the Cloud Service Providers (CSPs) such as Amazon Web Services, Microsoft Azure, and Google Cloud.

But cloud customers are responsible for the secure use of virtual cloud resources, which requires different approaches and tooling to accomplish than it did in the data center. Attackers operate differently in the cloud than in data centers as well, and how organizations go about keeping your data safe in the cloud needs to be different. According to Gartner, through 2023, at least 99% of cloud security failures will be the customer's fault, mainly in the form of cloud resource misconfiguration.

Cloud and DevOps engineers are focused on the configuration of cloud resources, including security-sensitive resources such as networks, security groups, and access policies for databases and object storage. Organizations need to ensure that the configuration of their cloud resources is correct and secure on day one—and stay that way.

Industry analysts call this Cloud Security Posture Management (CSPM), which involves ensuring secure cloud resource configuration at every stage of the software development lifecycle (SDLC) from infrastructure as code to running cloud environments. We find that resource misconfiguration is what cloud customers tend to get wrong, sometimes with devastating consequences. Many of the data breaches that make the headlines are the result of the exploitation of cloud misconfiguration mistakes.

For the State of Cloud Security Report 2021, we surveyed 300 cloud professionals, including cloud engineers, cloud security engineers, DevOps, and cloud architects, to better understand the risks, costs, and challenges they are experiencing managing cloud security at scale.

The Nature and Scale of Cloud Misconfiguration Risk

Misconfiguration: The #1 Cause of Cloud Breaches

36% suffered a serious cloud security leak or breach in the past year

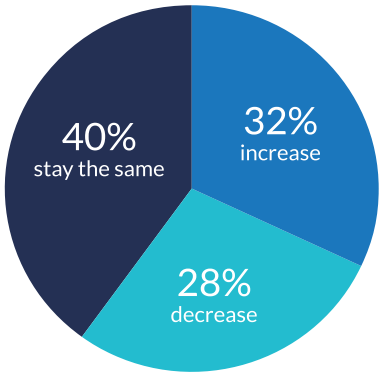
Misconfigurations represent the number one risk for every organization using the cloud. 36% of cloud professionals say their organization has experienced a serious cloud data leak or a breach in the past 12 months. More than 8 out of 10 are worried that they are vulnerable to a major data breach related to cloud misconfiguration.

32% of respondents believe the rate of cloud misconfigurations will increase over the next year, and 40% believe the rate of misconfiguration will stay the same. Only 28% are optimistic that the rate of cloud misconfigurations will decrease.

83% concerned their organization is at risk

36% experienced a serious cloud data leak or breach in the past 12 months

Over the next year, cloud misconfiguration will



Cloud Misconfiguration: By The Numbers

The rate of drift and misconfiguration remains extremely high

Deployment mistakes and compliance violations in infrastructure as code files constitute a significant contribution to cloud misconfiguration risk. However, cloud infrastructure environments are highly dynamic and subject to unapproved post-deployment configuration changes, called drift, which require constant monitoring for configuration errors. It is also commonplace to see the same vulnerability appear over and over again, often via infrastructure as code deployments..

The combination of deployment misconfiguration and unapproved changes made post-deployment results in a significant rate of cloud security incidents that need to be addressed.

49%: Teams experiencing 50 or more cloud misconfigurations per day.

Cloud Misconfiguration Incidents (per day)	2021
1 - 10	24%
10 - 50	21%
50 - 100	19%
100 - 250	13%
250 - 500	6%
500 - 1,000	8%
More than 1,000	3%

Misconfiguration Mistakes: The Ultimate Insider Threat

Customer mistakes result in dangerous cloud vulnerabilities

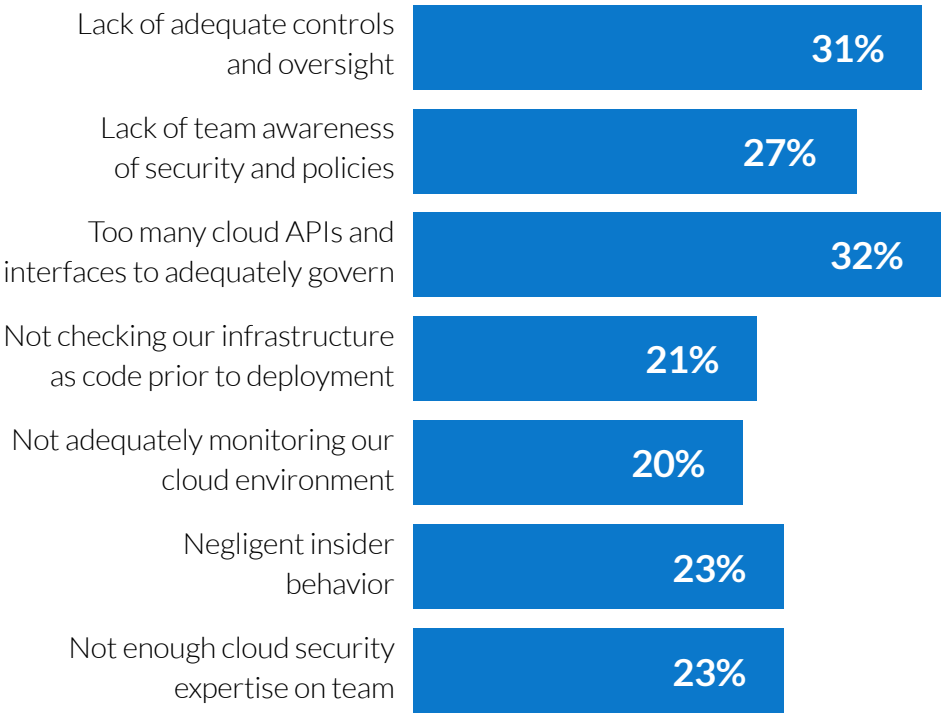
Cloud misconfiguration is a problem born of many causes—all of which can be attributed to human error of one kind or another. Enterprise cloud environments are vast and complex, and the dynamism of these environments creates many opportunities for critical mistakes. The nature and scale of the challenges outstrip the capacity of cloud engineering and security teams to effectively manage the risk.

The number one cause of cloud misconfiguration cited in our survey is the number of APIs and interfaces that require governance A lack of adequate controls and oversight (31%), and lack of awareness of policies (27%) were also cited.

21% said they are not checking infrastructure as code prior to deployment, which can result in automating the propagation of misconfiguration and compliance violations at scale in a cloud environment. 20% said they are not adequately monitoring their cloud environment for misconfiguration, and 23% cited the negligence of team members as a cause of misconfiguration.

With 45% reporting that they are using more than one cloud provider, the problem can compound if teams choose a cloud service provider's native security tooling, which doesn't work in multi-cloud environments. Each cloud platform has its own resource types, configuration attributes, and interfaces to govern, and policies, controls, and expertise must effectively span the cloud platforms in use.

Causes of Misconfiguration



The Most Prevalent Cloud Misconfigurations

Identity and Access Management (IAM) is now #1

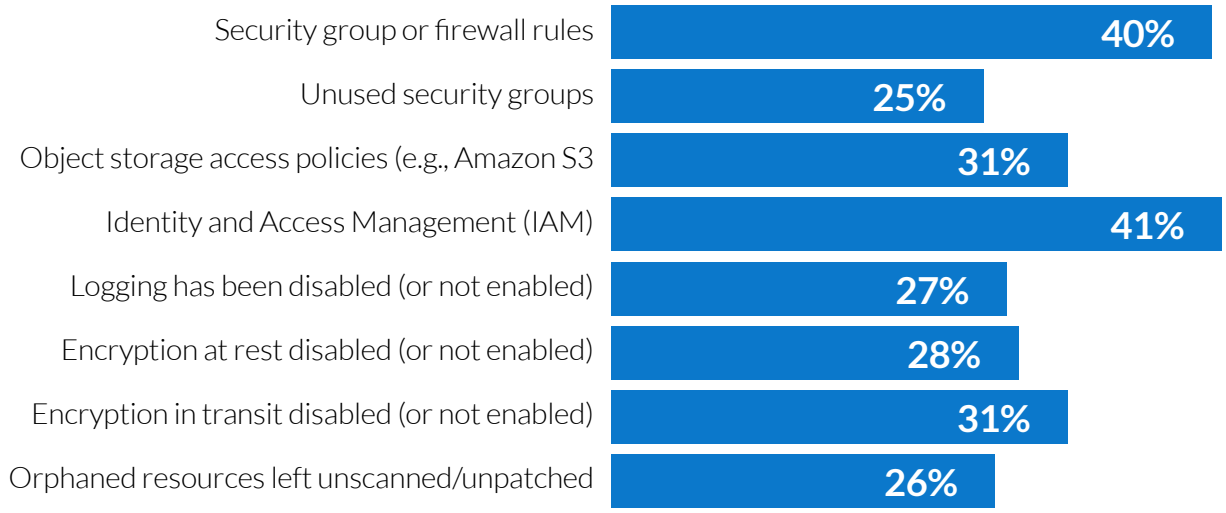
One of the many aspects of the cloud that differentiate it from the data center is the sheer number of unique cloud services available, each with its risks and security best practices. This means teams are experiencing a variety of dangerous kinds of misconfiguration.

The types of misconfiguration remain largely unchanged, but Identity and Access Management (IAM) is now the most commonly cited cloud misconfiguration (cited by 41%). Because cloud IAM resources effectively serve as a new network, IAM misconfiguration has played an increasing role in cloud breaches over the past few years as attackers use it to discover resources, move laterally, and access data for extraction.

- The rate of security group misconfiguration—long the most commonly cited resource misconfiguration—is down 4% from 44% last year.
- Object storage access policy misconfigurations, such as those for Amazon S3 or Azure Blob Storage, are down slightly as cloud service providers provide more notifications and alerts of these vulnerabilities.

Orphaned cloud infrastructure has been long recognized as a cost problem, but few recognize it as a security problem. These costly orphans can invite malicious actors into your cloud environment, and they've played a key role in recent major cloud breaches. By their nature, orphaned resources aren't tracked in your management tools, aren't scanned for vulnerabilities or compliance violations, and are not patched with security updates (where applicable).

Common cloud misconfigurations experienced



Preventing Cloud Misconfiguration

Cloud Security: Whose Job Is It?

A shared responsibility, with engineering teams bearing the biggest burden

Cloud security is largely a responsibility shared across functions, including cloud engineering, security teams, compliance analysts, and outside consultants. The application developers and cloud engineers that develop, deploy, and maintain their cloud environments generally own the security of those environments. When developers spin up cloud environments for their applications, they are also defining the security of their infrastructure through configuration (and re-defining it daily).

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

Different teams are generally concerned with different phases of the cloud SDLC:

- Cloud developers are using IaC to develop and deploy cloud infrastructure.
- Security teams are monitoring cloud environments for vulnerabilities.
- Compliance teams are managing compliance audits.

Cloud security requires more cross-team collaboration than in the data center, and 38% cited friction between different teams over cloud security roles and issues. 45% cite challenges in using different tools and policies for different phases of the SDLC. More than 50% cite issues related to gaining visibility into their environments.

Who defines cloud policy?

Engineering: **66%**

Security: **55%**

Compliance: **50%**

Outside Consultants: **22%**

Who audits and enforces cloud policy?

Engineering: **56%**

Security: **54%**

Compliance: **49%**

Outside Consultants: **29%**

Cloud Policy: Approaches to Implementation and Enforcement

35% still rely on written cloud security policies and manual processes

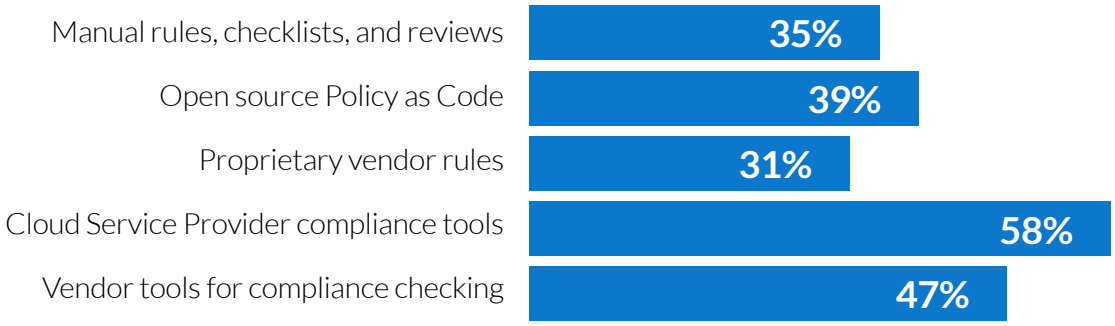
Every organization operating in the cloud has a set of policies intended to govern how they use it, from internal rules to compliance standards such as SOC 2, NIST 800-53, GDPR, and HIPAA. Traditionally, such policies were expressed in writing, and the implementation and enforcement of policies were largely manual.

The advent of policy as code (PaC) has revolutionized how IT policy is implemented. Rather than written rules and checklists, policies are expressed "as code" and can be used to automatically assess the compliance posture of infrastructure as code and running cloud environments. Using PaC for cloud security is significantly more efficient—it's repeatable, shareable, scalable, and consistent. And most importantly, PaC greatly reduces security risks due to human error.

Our survey found that the adoption of PaC continues to grow, but there are a wide variety of tools and implementation patterns, including open source policy as code (39%, an increase of 8% over 2020) and proprietary vendor rules (31%, a decrease of 5%).

35% still rely on manual checklists for cloud security, which is time-consuming and introduces the risk of human error. This represents an improvement of 4%. 58% are using compliance tools offered by cloud service providers, which don't work in multi-cloud environments.

58% use native cloud security tools that don't work in multi-cloud environments



Securing Infrastructure as Code Pre-Deployment

More than 90% of cloud teams are using at least some Infrastructure as Code

A key component of the Cloud Development Lifecycle (CDLC) is the early development phase involving infrastructure as code (IaC), which is used to define and provision the initial cloud resources and configurations in code files. The use of IaC is now mainstream, with more than 90% of respondents citing at least some IaC usage. But are they checking IaC for risks? This is an opportunity to *shift left* on cloud security.

When IaC contains misconfiguration or compliance violations, it becomes a means of deploying those vulnerabilities at scale, representing significant cloud risk. But IaC provides for the ability to run security checks prior to provisioning cloud resources, which wasn't possible before. Ensuring IaC is free of misconfiguration and adheres to policy is critical to cloud security.

Many respondents said they're using some kind of IaC checking tool, such as the open source Regula policy engine (14%) or AWS CloudFormation Guard (29%). 33% continue to rely on manual reviews of IaC files, and 27% aim to catch misconfigurations post-deployment.

33% manual (slow, error-prone, time intensive)

27% aim to catch misconfigurations post-deployment

"[Shift] risk as early in the provisioning process as possible by embedding guardrails, governance, testing, and security assessment in line to drive uniformed compliance."

McKinsey & Company, How CIOs and CTOs can accelerate digital transformations through cloud platforms

Infrastructure as Code Security: Level of Effort

Half of cloud teams are investing 50+ hours per week to IaC security

The adoption of infrastructure as code (IaC) presents cloud teams with the opportunity to shift left on cloud security and compliance and build security into cloud development, but there isa level of effort required.

Implementing IaC security checks, mapping IaC rules to compliance controls, remediating IaC violations, and reconciling cloud runtime violations with the corresponding IaC templates requires engineering investment. IaC security burdens are amplified when automated IaC checks using policy as code aren't used consistently across the organization.

Engineering Hours Invested in IaC Security Per Week

Fewer than 10	**13%**
10-50	**35%**
50-100	**31%**
00-500	**15%**
More than 500	**4%**

Managing Cloud Misconfiguration

Detecting and Remediating Cloud Misconfigurations

A reliance on manual processes and cloud service provider tools can create new challenges

Managing cloud vulnerabilities is a race between attacker and defender, as attackers use automation tools to scan the internet to find cloud misconfigurations within minutes of their deployment. So, even if developers get the security of their cloud infrastructure correct on day one - by securing their infrastructure as code - they may introduce a misconfiguration vulnerability on day two (or hour two).

47% of teams analyze cloud provider logs to identify dangerous drift events and misconfigurations, and 35% rely on manual audits of their environment. Nearly half of teams leverage their cloud service provider's native security tools, which don't work in multi-cloud environments. 33% are using a third-party cloud security posture management (CSPM) solution, which can typically work in a multi-cloud environment.

More than 50% of cloud teams cite challenges in getting visibility into their cloud environments, with those saying they have excellent visibility into their environment falling below 50% over last year.

Multi-cloud environments can create challenges with gaining visibility across a cloud estate, with the accelerating pace of multi-cloud adoption making this more difficult.

Non-production environments (e.g., dev and test), which often contain production data used for development and testing purposes, are typically not monitored for misconfiguration vulnerabilities.

47.2% rely on their own analysis of cloud logs to catch dangerous changes and misconfigurations

35.3% manually audit environments

More than 50% cite visibility issues leading to missing misconfiguration

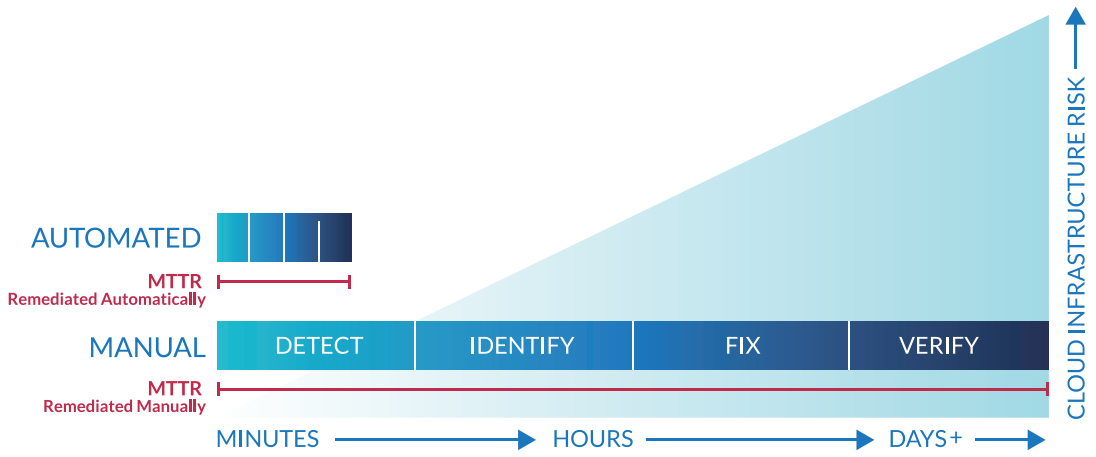
Measuring the Success of Cloud Security

Mean Time to Remediation lags behind attackers' speed in exploiting misconfigurations

A lot has changed with how hackers go about stealing data or otherwise damaging an organization. The traditional approach involves picking an organization to target and then searching for vulnerabilities to exploit. With the cloud, malicious actors now use automation tools to scan the entire internet searching for cloud misconfigurations, such as unrestricted SSH access (e.g., 0.0.0.0/0 on Port 22), orphaned and unpatched compute instances, and many others.

They don't have to look too hard. Within minutes of adding a new endpoint to the internet, a potential attacker has scanned it, and what they get back is essentially a long shopping list of cloud environments they can attack. It's relatively trivial to discover who owns these environments, so the attacker goes shopping.

Mean Time to Remediation (MTTR) is the key security metric for measuring cloud infrastructure risk. It is one every cloud team should track, and every CISO should know. Threats to cloud infrastructure are fully automated, constantly probing for attack vectors to exploit. The longer cloud misconfigurations go unaddressed, the greater the risk of a major security incident.



An attacker can typically detect a cloud misconfiguration vulnerability within 10 minutes of deployment, but cloud teams are slower in detecting their own misconfigurations. Only 10% are matching the speed of hackers.

- Only 10% are remediating misconfigurations before the hackers can find them

About half of respondents say their MTTR for cloud misconfiguration should be under one hour, but many are falling short of that goal.

The MTTR for cloud misconfiguration remains largely unchanged from 2020.

MTTR for Cloud Misconfiguration

	Ideal MTTR	Real MTTR
Fewer than 15 minutes	**14%**	**10%**
15 minutes to 1 hour	**36%**	**39%**
1 hour to 1 day	**30%**	**33%**
1 day to 1 week	**13%**	**12%**
1 week to 1 month	**5%**	**5%**

Auditing Cloud Environments for Compliance

Cloud compliance audits are too manual and periodic to address modern threats

Cloud environment audits are routine for practically every organization operating in the cloud, and failing a cloud audit is also quite routine, with 45% citing a cloud audit failure.

While the daily rate of misconfiguration remains high and attackers are armed with automation tools designed to detect it, cloud compliance audits remain largely periodic, point-in-time exercises.

Only 26% continuously audit their environment (i.e., "daily"), with 74% relying on periodic audits—insufficient to the task of addressing cloud misconfiguration at the daily rates cited in this report.

Compliance typically only requires audits of production environments, omitting non-production environments (e.g., dev, test) that often contain production data.

45% have failed a cloud compliance audit

81% take a week or longer to address compliance issues after an audit

Cloud Audit Frequency

Daily **26%**

Weekly **37%**

Monthly **20%**

Quarterly **11%**

Twice per year **3%**

Annually **3%**

Average time to bring cloud environments into compliance

Less than 1 week **19%**

About 1 week **30%**

1 week to 1 month **24%**

1 to 3 months **14%**

3 to 6 months **7%**

6 months to 1 year **3%**

Longer than a year/never **2%**

Managing Cloud Security and Compliance Issues: Level of Effort

Half of cloud teams invest 50+ hours per week managing cloud security

With the high rate of cloud misconfigurations and a reliance on manual processes to manage it, the costs of cloud security and compliance are predictably high.

Teams need to manually review alerts and tickets, identify critical misconfigurations that need remediation, manually fix the cloud misconfigurations or IaC templates themselves, and complete incident reports.

With the average salary of a cloud engineer at roughly $125,000 (typically much higher for experienced cloud engineers and cloud security experts), 50% of teams are investing at least one FTE engineer on the problem, and 15% are investing more than $250,000 per year.

Hours per week	
Fewer than 10	**22%**
10-50	**29%**
50-100	**35%**
00-500	**11%**
More than 500	**4%**

Cloud Security: Team Challenges and Organizational Consequences

Cloud Security Challenges: People Factors

An over-reliance on manual processes is creating new problems and challenging teams

While cloud misconfiguration vulnerabilities are preventable with proactive approaches, such as policy as code checks on infrastructure as code, and automated drift detection, an over-reliance on manual processes and a mix of tools and methods stresses teams already under pressure to do more with what they have.

The number one cloud security challenge cited is the different teams using different tools and policy frameworks for different stages of the SDLC, from infrastructure as code checks to monitoring running cloud environments (45%). Multi-cloud usage only exacerbates this problem.

Traditional security challenges that long predate the cloud all play a significant role in cloud security, such as alert fatigue (21%) and false positives (27%). While the adoption of cloud security automation continues to grow, human error in missing, miscategorizing, or remediating critical cloud misconfigurations remains a serious problem (38%).

The demand for cloud engineering and security expertise continues to outpace supply, and 36% cite challenges in hiring and retaining the cloud security experts they need. 35% cite challenges sufficiently training their cloud teams on security and compliance risks and policies.

#1 Challenge: Different tools and rules for different stages of the SDLC: 45.2%

Cloud Security Issues Experienced

Cloud Security Challenges: Technology Gaps

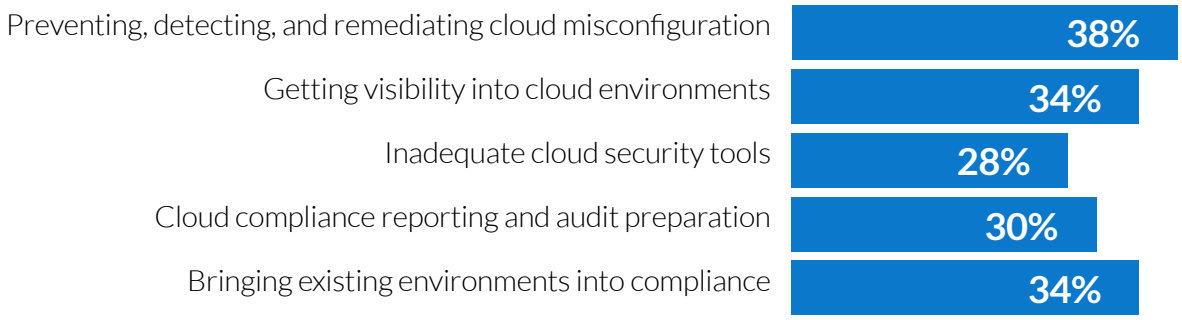
Cloud security is still full of challenging and time-consuming tasks

While the promises that automation and policy as code can deliver for cloud security and compliance are real, the reality is that teams are still struggling to stay out in front of continuous change to ensure their cloud environment stays secure.

The number one issue cited by respondents is the prevention, detection, and remediation of cloud misconfiguration (38%), and several issues that factor into this, including challenges in getting visibility into cloud environments (34%) and inadequate cloud security tooling (28%).

Compliance reporting and preparing for cloud compliance audits is a challenge for 30%, and bringing existing cloud environments into compliance after an audit was cited as a challenge by 34%.

Cloud Security Challenges



The Cloud Security Effect on the Organization

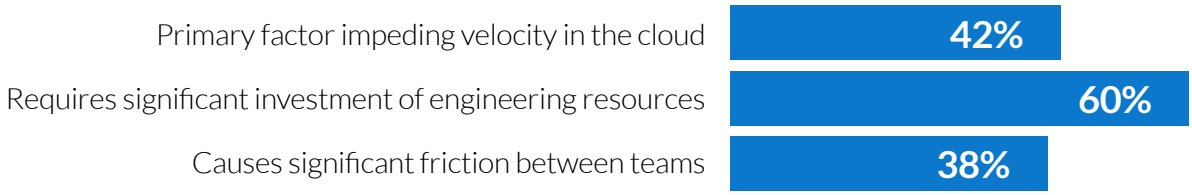
Speed, spending, and cross-team collaboration are impacted

While cloud computing is a major facilitator of digital transformation and speed of innovation, cloud security and compliance requires investment and can represent the number one rate-limiting factor for how fast organizations can develop and release in the cloud, and ultimately how successful digital transformation can be.

Six in ten respondents describe the engineering resource investment in cloud security and compliance as "significant" to cover audits, monitoring, remediation, and reporting for both infrastructure as code and running cloud environments. 42% say that security and compliance is the primary factor impeding their velocity in the cloud, and 38% cite significant friction between teams over cloud security and compliance issues.

If automated checks using policy as code aren't integrated early in the SDLC, security and compliance approval processes can prevent the full realization of continuous integration and continuous delivery (CI/CD). 26% cite approval times for deployments of up to one week, and 36% say approvals can take about one day. 8% say approvals can take up to one month.

The impact cloud security has on the organization



What Cloud Professionals Say They Need

More automation, better visibility, and a unified approach to cloud policy

When asked what would help them keep cloud environments secure, move faster, and save money, 47% say they need better visibility into their cloud environment and how it's changing. 45% say that having a unified approach to cloud policy across the SDLC and cloud platforms would be the biggest factor in improving cloud security operations, and (96% say this would be valuable).

Automation is a common theme, with 43% wanting automated and immediate cloud infrastructure audits and deployment approvals, and 37% wanting automated cloud compliance assessments and reporting. 35% say they need better guidance on remediating misconfiguration in cloud environments and infrastructure as code.

45%: One set of rules across the SDLC

47%: Better visibility

43%: Automated audits and approvals

37%: Automated compliance reporting

Conclusions: Where Cloud Security is Going

The scale and complexity of cloud risk is growing

Cloud adoption continues at a rapid pace and shows no signs of slowing, which means the average enterprise cloud footprint keeps expanding. Multi-cloud usage (leveraging multiple cloud platforms such as AWS, Microsoft Azure, and Google Cloud Platform) is also growing, with 45% of respondents now saying they manage cloud environments that span providers.

The proliferation of cloud resource types also continues unabated, with AWS alone offering more than 200 infrastructure services delivered via availability zones across the globe. Each cloud service has unique configuration attributes and security profile that must be carefully considered in the full context of each organization's environment and use case.

The nature of cloud threats has also evolved, and attacks have become more sophisticated. Attackers now employ automation to scan the internet for misconfigured cloud resources in minutes, placing pressure on engineering and security teams to find and remediate them quickly.

The result: a vast majority of respondents (83%) are concerned their organization is at risk of a cloud-based data breach.

Cloud security is both a people problem—and a technology one

Cloud misconfiguration is the result of human error—and the number one cause of cloud-based data breaches. Modern enterprise cloud environments—along with the compliance and security policies intended to protect them—are too vast and complex for humans to manage without effective tooling. And the adoption of infrastructure as code without security checks can increase the scale of cloud vulnerabilities.

As a result, half of the cloud teams surveyed are now experiencing a significant number of misconfiguration incidents per day. Teams often lack the cloud security expertise they need, and team members lack awareness of all of the security policies required to operate safely. And there is an over-reliance on slow, error-prone manual cloud security and compliance processes.

The result: cloud security requirements are placing significant demands on cloud engineering and security teams, and they are soaking up resources and slowing them down. Most teams often invest in a full-time equivalent (FTE) engineer managing misconfiguration and compliance and another FTE engineer in securing infrastructure as code.

Cloud compliance frameworks offer a standardized approach to cloud governance (often mandated depending on industry and use case), but these policy frameworks can be quite expansive and require expertise and technical interpretation to apply them to cloud environments and specific use cases.

Cloud professionals point the way forward on cloud security

Cloud professionals are telling us that they need better tooling and automation to operate securely in the cloud without slowing down the pace of innovation.

96% of cloud professionals say that having a cloud security platform and policy framework that work across the SDLC—from infrastructure as code through the runtime—would be valuable.

Respondents also said that better cloud compliance tooling, including automated audit preparation, reporting, and deployment approvals would be helpful. The need for better visibility into cloud environments and security posture was also commonly cited.

Recommendations

Because cloud security focuses on the prevention of misconfiguration mistakes, effective automation used at every stage of the SDLC can have the dual benefit of empowering teams to move faster while being more secure.

Some recommendations from cloud professionals to accomplish this include:

- Establish and maintain comprehensive visibility into your cloud environment across cloud platforms and continuously evaluate the policy impact of changes.
- Prioritize solutions that provide a unified policy approach to infrastructure as code and running cloud environments, so all teams operate from the same "rulebook".
- Use infrastructure as code wherever possible and check it for security early in the SDLC using policy as code.
- Automate as much of your cloud compliance processes as possible, including assessments, reporting, audit preparation, and deployment approvals.
- Establish what your current Mean Time to Remediation for misconfiguration is for security-critical resources and set goals to bring it down to a safe level measured in minutes

SPONSORS

ABOUT FUGUE

Fugue helps organizations move faster in the cloud—without breaking the rules needed to keep cloud environments secure. The Fugue platform secures cloud infrastructure across the entire software development lifecycle—from infrastructure as code through the cloud runtime. Fugue empowers cloud engineering and security teams to prove continuous compliance, build security into cloud development, and eliminate cloud misconfiguration vulnerabilities. Fugue supports Amazon Web Services, Microsoft Azure, and Google Cloud, and provides one-click reporting for CIS Foundations Benchmarks, CIS Controls, CIS Docker, CSA CCM, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. Customers such as AT&T, SAP NS2, and Red Ventures trust Fugue to protect their cloud environments. To learn more, visit www.fugue.co.

ABOUT SONATYPE

Sonatype is the leader in developer-friendly, full-spectrum software supply chain automation providing organizations total control of their cloud-native development lifecycles, including third-party open source code, first-party source code, infrastructure as code, and containerized code. The company supports 70% of the Fortune 100 and its commercial and open source tools are trusted by 15 million developers around the world. With a vision to transform the way the world innovates, Sonatype helps organizations of all sizes build higher quality software that's more aligned with business needs, more maintainable and more secure.

Sonatype has been recognized by Fast Company as one of the Best Workplaces for Innovators in the world, two years in a row and has been named to the Deloitte Technology Fast 500 and Inc.