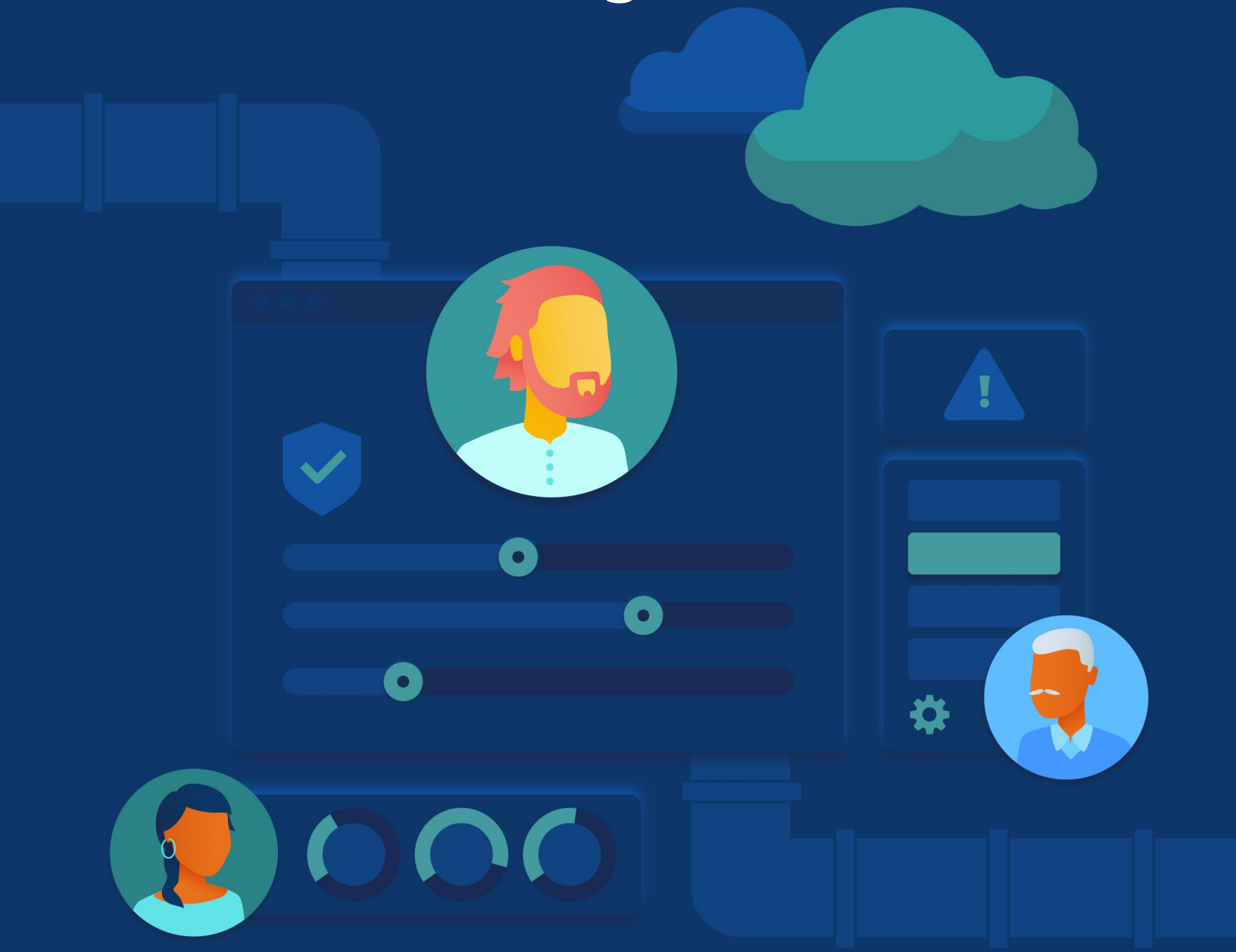
The State of Cloud Security Risk, Compliance, and Misconfigurations



CloudHealth by vmware

CSA cloud security alliance®

Acknowledgments

Lead Author:

Hillary Baron

Contributors:

Josh Buker
Sean Heide
Alex Kaluza
Shamun Mahmud
John Yeoh

Designers:

Stephen Lumpe
AnnMarie Ulskey

Special Thanks:

Nikhil Girdhar, *Product Marketing Leader, CloudHealth® by VMware*

Lauren van der Vaart, *Senior Content Marketing Specialist, Multi-Cloud, VMware*

Table of Contents

Executive Summary 6
- Key Finding 1: Lack of knowledge and expertise continue to plague security teams 6
- Key Finding 2: Information security and IT operations held responsible for reducing cloud misconfigurations 6
- Key Finding 3: DevSecOps approach to security still out of reach 7
  - Departments are struggling to align on security policies and/or their enforcement 7
  - Interdepartmental alignment on security policies and enforcement is crucial for proactive security 8

Current State Of Cloud Security Programs 9
- Public Cloud Providers Used 10
- Annual Budget for Public Cloud 10
- Overall Confidence to Defend Against a Cloud Security Breach 11
- Confidence in Ability to Defend Against Cloud Vulnerabilities and Threats 11
- Barriers to Resolving Security Concerns 12
- Interdepartmental Alignment on Security Policies and Enforcement 13
- Measuring Security and Compliance Posture 14

Cloud Security Tools Being Used 15
- Solutions Used for Cloud Security 15
- Satisfaction with Cloud Service Provider's Security Solutions 15
- Use of Managed Service Providers 16

Cloud Security Posture Management 17
- Identification of Misconfigurations 17
  - Team Responsible for Detecting, Tracking, and Reporting Misconfigurations 17
  - Causes of Cloud Misconfigurations 18
  - Pipeline Delivery Stage Where Misconfigurations are Detected 18
  - Length of Time to Detect Misconfigurations 19
- Breaches and Incidents from Misconfigurations 20
  - Cloud Security Incident or Breach due to Misconfigurations in the Past Year 20
  - Barriers to Preventing or Fixing Cloud Misconfigurations 20
- Governance and Compliance 21
  - Designing Security and Compliance Standards for Managing Cloud Misconfigurations 21
  - Enforcing Standards Across Teams and Organizations 22
  - Balancing Security with Project Delivery 22
- Resolution of Misconfiguration Mistakes 23
  - Group Responsible for Correcting Misconfigurations 23
  - Pipeline Delivery Stage Where Misconfigurations are Remediated 24
  - Length of Time to Remediate a Misconfiguration 24
  - Methods for Improving Resolution of Security or Compliance Misconfigurations 25
  - Barriers to Using Auto-Remediation 25

Demographics 27
- Organization Public Cloud Spend 29
- Job Level 29
- Primary Department 30
- Organization Industry 28
- Organization Size 28
- Location 27

Survey Creation And Methodology

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

The Cloud Security Alliance (CSA) is a not-for-profit organization with a mission to widely promote best practices for ensuring cyber security in cloud computing and IT technologies. CSA is also tasked with educating various stakeholders within these industries about security concerns in all other forms of computing. CSA's membership is a broad coalition of industry practitioners, corporations, and professional associations. One of CSA's primary goals is to conduct surveys that assess information security trends. These surveys help gauge the maturity of information security technology at various points in the industry, as well as the rate of adoption of security best practices.

CloudHealth® by VMware commissioned CSA to develop a survey to add to the industry's knowledge about public cloud security and to prepare this report of the survey's findings. CloudHealth financed the project and co-developed the initiative by participating with CSA in the development of survey questions addressing cloud security. The survey was conducted online by CSA from May 2021 to June 2021 and received 1090 responses from IT and security professionals from a variety of organization sizes and locations. The data analysis was performed by CSA's research team.

Goals of the study

The goal of this survey is to assess organizational readiness for mitigating public cloud security and compliance risks due to configuration mistakes. Key research topics include:

- Current state of cloud security programs, including top risks and usage of security tools
- Cloud Security Posture Management (CSPM) challenges faced by organizations in mitigating misconfiguration vulnerabilities
- Organizational readiness, success KPIs, and teams responsible for different aspects of cloud security posture management

Executive Summary

Cloud misconfigurations consistently are a top concern for organizations utilizing public cloud. Such errors lead to data breaches, allow the deletion or modification of resources, cause service interruptions, and otherwise wreak havoc on business operations. With recent breaches due to misconfigurations making major headlines, this survey was conducted to better understand the current state of cloud security programs, tools utilized to mitigate security risks, organizations' cloud security posture, and barriers organizations face in reducing security risks.

Key Finding 1

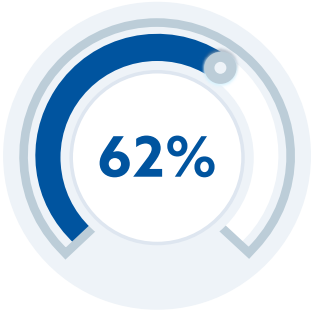
Lack of knowledge and expertise continue to plague security teams

Lack of knowledge and expertise are well-known issues within the information security industry. It is no surprise then, that lack of knowledge and expertise was consistently identified as:

- The primary barrier to general cloud security (59%)
- The primary cause of misconfigurations (62%)
- A barrier to proactively preventing or fixing misconfigurations (59%)
- The primary barrier to implementing auto-remediation (56%)

These findings highlight the trickle-down effect that lack of knowledge can have on security teams. It starts as a general barrier to implementing effective cloud security measures. This leads to misconfigurations, the primary cause of data breaches. But it's also preventing security teams from implementing a solution, such as auto-remediation, which could supplement this knowledge and skills deficit.

The primary barrier to general cloud security



The primary cause of misconfigurations

A barrier to proactively preventing or fixing misconfigurations

And the primary barrier to implementing auto-remediation

Key Finding 2

Information security and IT operations held responsible for reducing cloud misconfigurations

Each year data breaches due to misconfigurations make headlines, making it a top concern for many organizations.

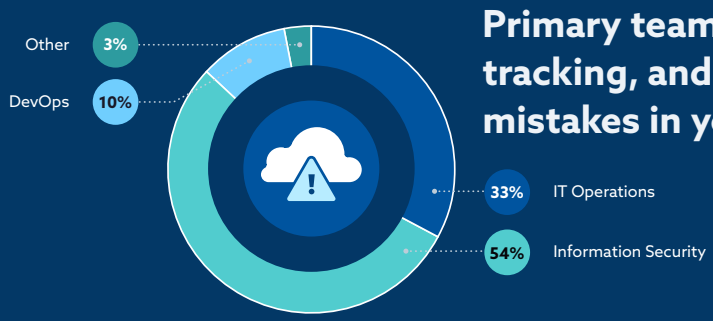
One likely reason why organizations struggle with management of misconfigurations is that they are holding their IT operations and information security teams primarily responsible for detecting, monitoring, and tracking potential misconfigurations (**information security 54%**, **IT operations 33%**) as well as remediating these misconfigurations (**information security 36%**, **IT operations 34%**), rather than distributing responsibilities across the DevOps or application engineering teams who may be accidentally causing such mistakes and are in a better position to directly fix these errors.

For this reason, it is important for organizations to shift left the remediation responsibilities to DevOps and application engineering teams in order to manage misconfiguration risk more effectively.

Also, the primary reason organizations state for having a security incident due to misconfigurations is "lack of visibility" (68%). It is equally as important for organizations to prioritize tooling that provides three primary things:

- Improved visibility
- Effective risk governance
- Automation

These functions will help improve the organization's ability to quickly identify and correct misconfigurations, regardless of the team responsible for them.



Primary team responsible for detecting, tracking, and reporting cloud misconfiguration mistakes in your organization.

Primary group responsible for ensuring cloud misconfiguration mistakes are corrected.

Key Finding 3

DevSecOps approach to security still out of reach

Departments are struggling to align on security policies and/or their enforcement

Topics like DevSecOps and shifting security left have become increasingly hot topics for the security industry. While these strategies result in harder, more secure, and more resilient applications, many organizations struggle to implement these approaches. They are struggling to even get interdepartmental agreement on security policies and the enforcement of those policies. Under a third of organizations have been successful in this regard.

This lack of alignment among departments could be due to cultural differences, namely differing priorities among managers. Typically, this issue starts with the managers and spreads to their team. Another explanation for this lack of alignment could tie back to a lack of knowledge noted in the previous key finding. If departments don't have sufficient knowledge of DevSecOps strategies and best practices, then it's incredibly difficult to start implementing them or to gain alignment on key issues.

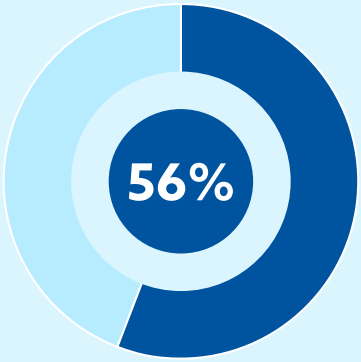
It's also worth noting that despite approximately 70% of organizations struggling to obtain interdepartmental alignment on security policies and/or enforcement, only 39% identified this as a primary barrier to resolving security concerns. So, it's likely that organizations are encountering more fundamental problems that are preventing them from moving toward a DevSecOps or shift left model.

Relationship between Security, IT Operations, and Developer teams regarding security policies and enforcement

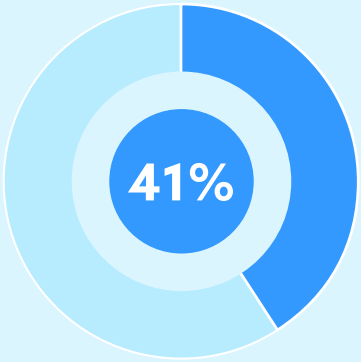
Interdepartmental alignment on security policies and enforcement is crucial for proactive security

Organizations who can gain alignment among their departments regarding security policies and enforcement strategies and are moving toward a DevSecOps approach are better equipped to deal with configuration errors. These organizations were more likely to detect a misconfiguration within a day of the error occurring (**full alignment – 56%**, **partial alignment – 41%**, **no alignment – 31%**). They are also more likely to remediate that error within a day of detecting the misconfiguration (**full alignment – 51%**, **partial alignment – 24%**, **no alignment – 19%**). Since misconfigurations are one of the leading causes of data breaches, the shorter the timeline to detecting and remediating these errors, the more secure an organization is overall. It's clear that this alignment and movement towards a DevSecOps approach is key for organizations addressing misconfigurations, but also reducing the risk of a data breach or other major security incident.

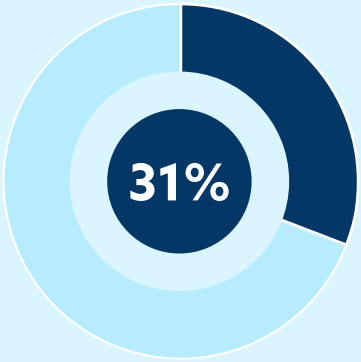
Detect Configuration Error within a Day



Aligned on security policies and enforcement

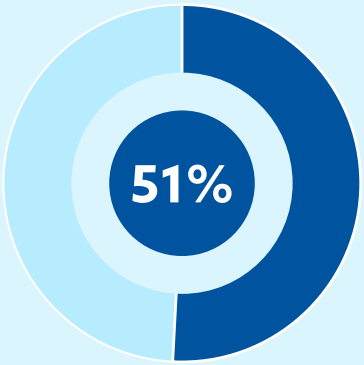


Aligned on security policies but not enforcement

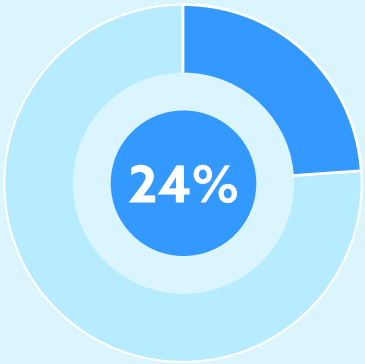


Not aligned on security policies or enforcement

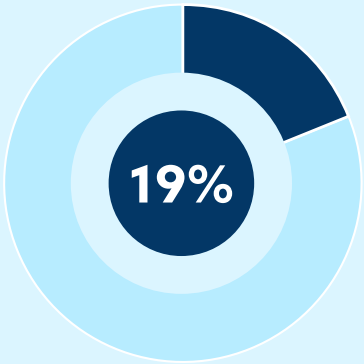
Remediate Configuration Error within a Day



Aligned on security policies and enforcement



Aligned on security policies but not enforcement

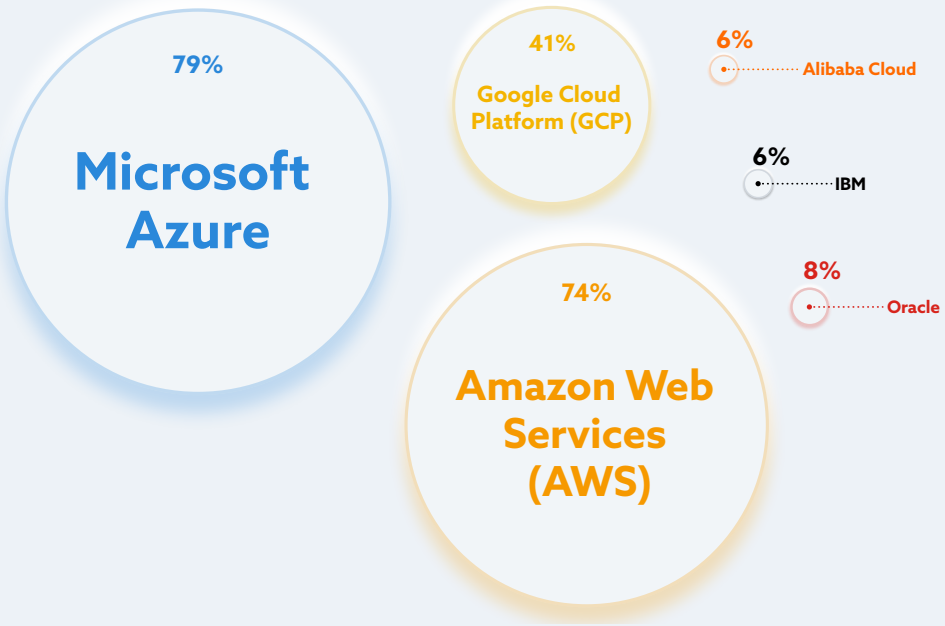


Not aligned on security policies or enforcement

Current State Of Cloud Security Programs

Public Cloud Providers Used

There is not one dominant public cloud platform in the market, but Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) continue to be the primary public cloud providers used. In this survey, **74% of respondents use AWS**, **79% use Azure**, and **41% use GCP**.

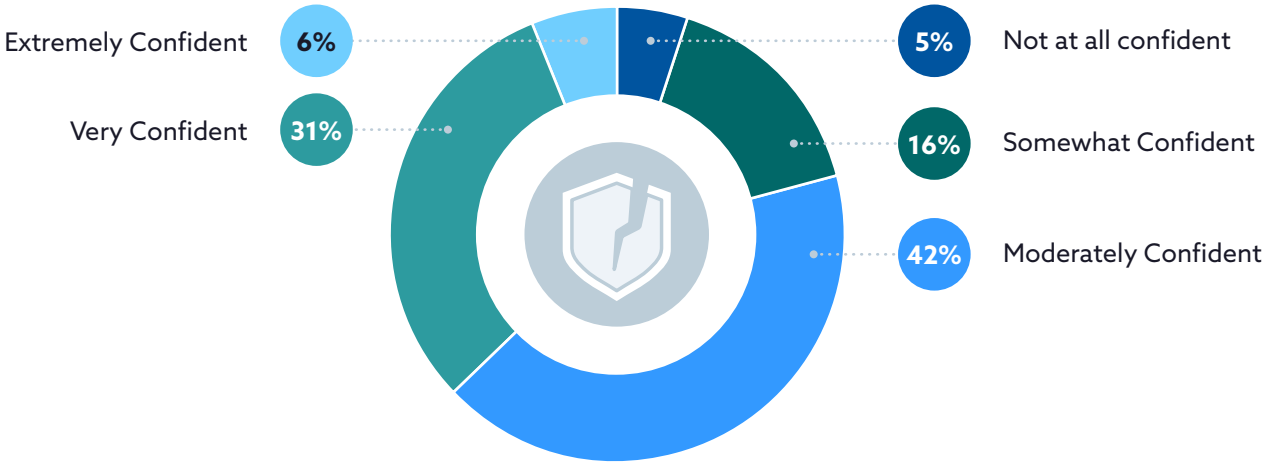


Annual Budget for Public Cloud

The budgets for public cloud spend varied greatly among participants. However, the top three most common responses were under $1,500,000 with **"$0-$250,000" at 22%**, **"$500,001-$1,500,000" at 15%** and **"$250,001-$500,000" at 13%**. There was also a notable percentage who were unsure (16%).

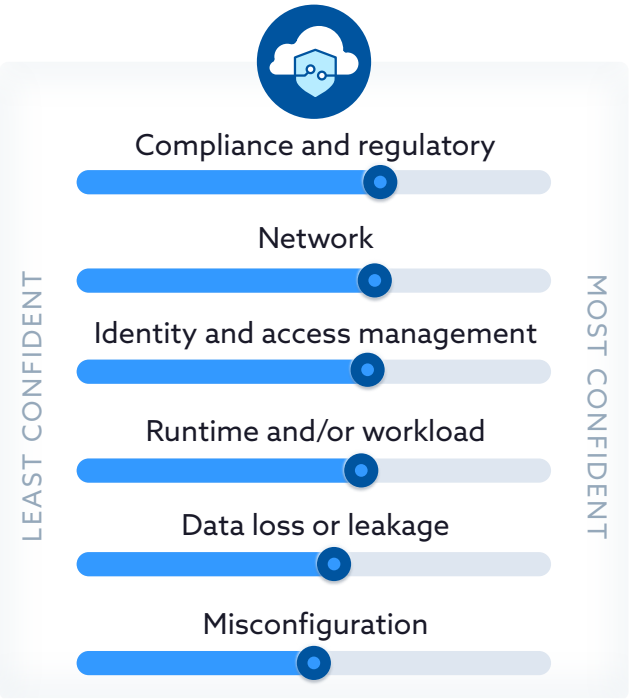
Overall Confidence to Defend Against a Cloud Security Breach

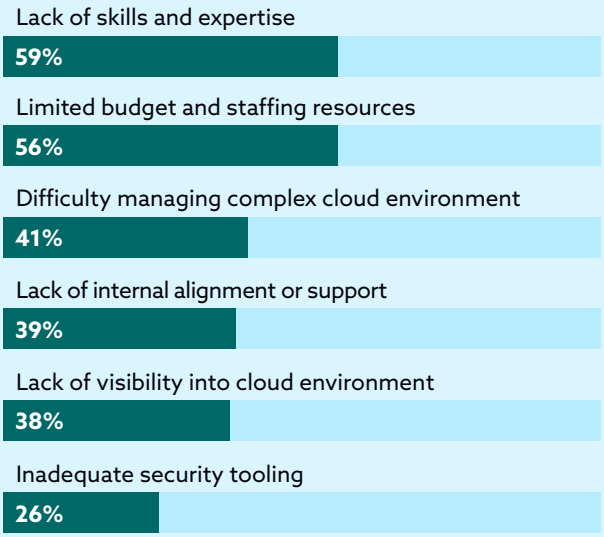
To assess respondents confidence in their organization's security program, they were asked to rate their general level of confidence in the organization's ability to defend against a cloud security breach. Most respondents reported being **"moderately confident" (42%)** or **"very confident" (31%)**.



Confidence in Ability to Defend Against Cloud Vulnerabilities and Threats

On average, respondents are **"moderately confident"** in their organization's ability to defend against threats and vulnerabilities in a variety of areas. There were minimal variations in the level of confidence among the various categories. The areas that inspired the most confidence, "compliance and regulatory" and "network," were only slightly higher than the lowest rated, "misconfiguration."





Barriers to Resolving Security Concerns

The primary barriers to resolving security concerns were unsurprisingly, **"lack of skills and expertise" (59%)** and **"limited budget and staffing resources" (56%)**. Both issues have plagued the industry for some time and tie in closely to the other options. This suggests that issues of budget, staffing, and expertise are perhaps obscuring other key issues such as "lack of visibility" and "inadequate security tooling."

Interdepartmental Alignment on Security Policies and Enforcement

DevSecOps and "shifting left" have become popular concepts within the security industry. However, it appears that the execution on these concepts remains elusive for many organizations. Only 31% report that their internal teams are aligned on both security policies and enforcement strategies. This lack of alignment between departments could be due to cultural differences, namely differing priorities. Another explanation could be a lack of knowledge, which is an issue noted in the previous question.

It's also worth noting that despite approximately 70% of organizations struggling to obtain interdepartmental alignment on security policies and enforcement, only 39% identified this as a primary barrier to resolving security concerns.

Additionally, respondents who have better interdepartmental alignment on security policy and/or enforcement policies are more likely to report they are "extremely confident" or "very confident" in their ability to defend against a security breach (Extremely confident: full alignment – 15%, partial alignment – 2%, no alignment – 1%; Very confident: full alignment – 49%, partial alignment - 27%, no alignment –16%). Evidently, we can gather that internal alignment is a key determining factor and baseline requirement for organizations looking to improve their cloud security posture.

12

Measuring Security and Compliance Posture

The indicators organizations are using to measure their security and compliance posture varies among organizations. Respondents were asked to select the top three indicators their organization uses. The most selected responses were **"% of unresolved high-risk misconfigurations or violations" (42%)**, **"number of failed security and compliance controls" (38%)**, and **"mean time to resolve misconfigurations or security and compliance violations" (32%).**

% of unresolved high risk misconfigurations or violations

Number of failed security and compliance controls

Mean time to resolve misconfigurations or security and compliance violations

Mean time to detect misconfigurations or security and compliance violations

% of cloud inventory covered by security or compliance controls

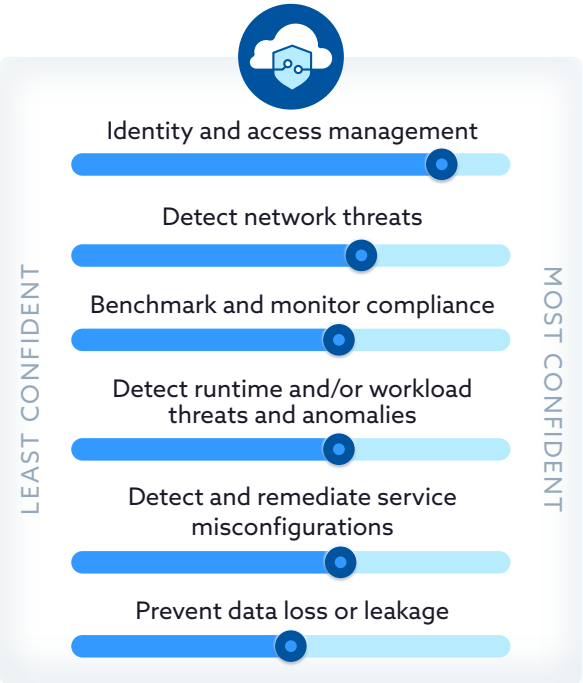
Cloud Security Tools Being Used

Solutions Used for Cloud Security

Generally, there is a relatively even split between organizations using cloud service provider's native tools and third-party solutions. However, a few categories of cloud security had a clear winner. Cloud service providers' native tools are the preferred solution for **"identity and access management" (47%)**, while third-party solutions are preferred for **"detect network threat" (46%)** and **"prevent data leakage" (35%)**.

A particularly concerning pattern to note is the percentage of organizations not using a data loss prevention tool (13%) which was much higher than for any other category. This could reflect the difficulty these types of solutions are to implement.

	Cloud Service Provider's Native Tools	Third Party Soultion	In-house Solution	N/A -No Solution	Unsure
Identity and access management	47%	31%	17%	2%	3%
Benchmark and monitor compliance	35%	34%	16%	9%	6%
Detect runtime and/or workload threats and anomalies	35%	38%	13%	7%	7%
Detect and remediate misconfigurations	34%	33%	17%	9%	7%
Detect network threats	31%	46%	13%	5%	5%
Prevent data loss or leakage	30%	35%	15%	13%	7%

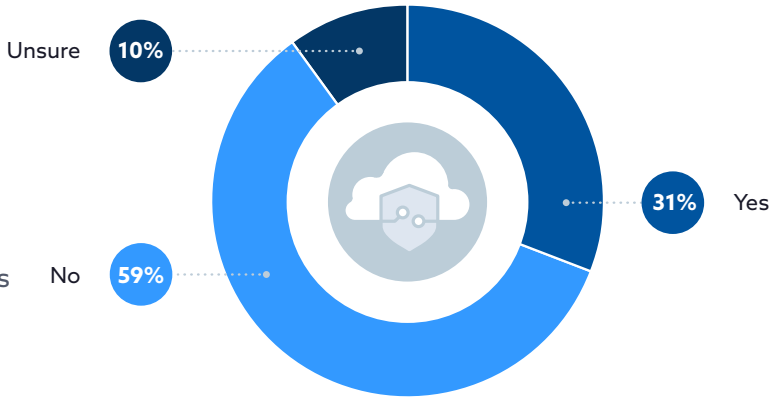


Satisfaction with Cloud Service Provider's Security Solutions

On average, respondents are **"moderately satisfied"** with their primary public cloud service provider's security solutions. There were minimal variations in the level of satisfaction among the various categories. The areas that had the highest average satisfaction, such as "identity and access management," were only slightly higher than the lowest rated, "prevent data loss or leakage."

Use of Managed Service Providers

Most organizations are not using a Managed Service Provider (**MSP, 59%**) to manage security and compliance of public cloud environments. Only **31% are using an MSP**. It should also be noted that small businesses with 1-50 employees were more likely to not use an MSP (72%) than organizations with 50 or more employees (57%).



Cloud Security Posture Management

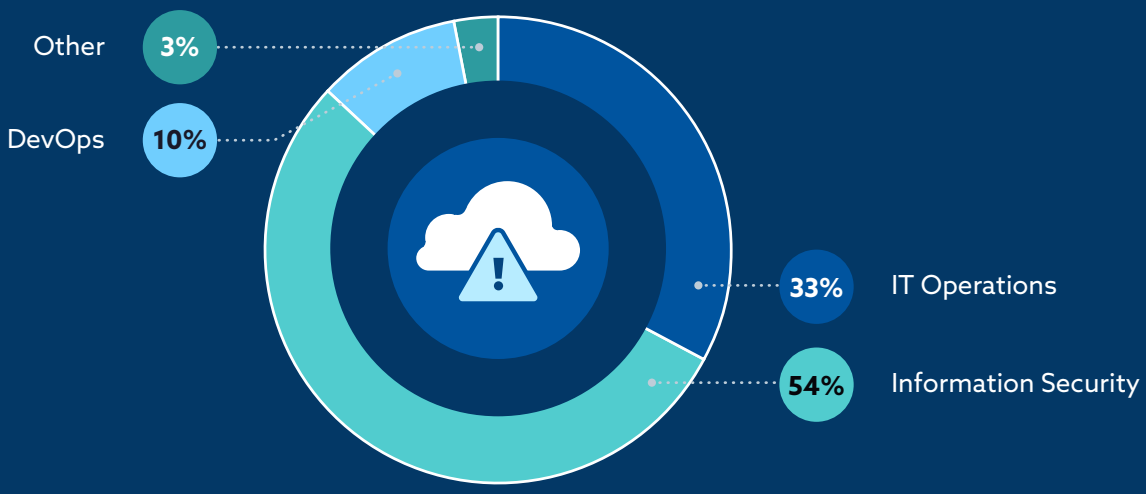
Identification of Misconfigurations

Team Responsible for Detecting, Tracking, and Reporting Misconfigurations

The primary team responsible for detecting, tracking, and reporting cloud misconfiguration mistakes is most often the **information security team (54%)**. IT Operations was the second most common response **(33%)**.

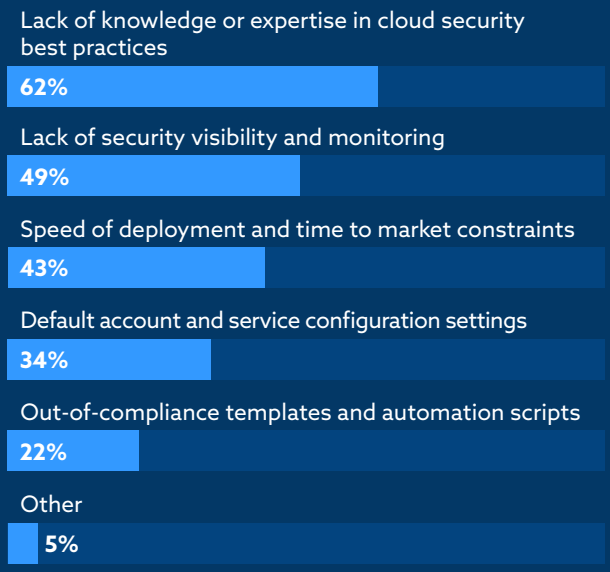
It is interesting that DevOps teams, who are usually the source of misconfigurations, and therefore more likely to be aware that a misconfiguration has occurred, are not identified as the group responsible for detecting, tracking, or reporting cloud misconfiguration mistakes. This highlights the importance of moving towards a DevSecOps approach to improve alignment and visibility across departments, that will ultimately result in faster detection and remediation of misconfigurations.

Equally important is ensuring the organization has the right tools that can enable all these departments across the organization. In particular, tools that enable effective risk governance, so organizations are better able to identify and manage risk and compliance. Automation is also key to quickly identify and remediate misconfigurations. This will require organizations to modernize their architecture towards cloud.



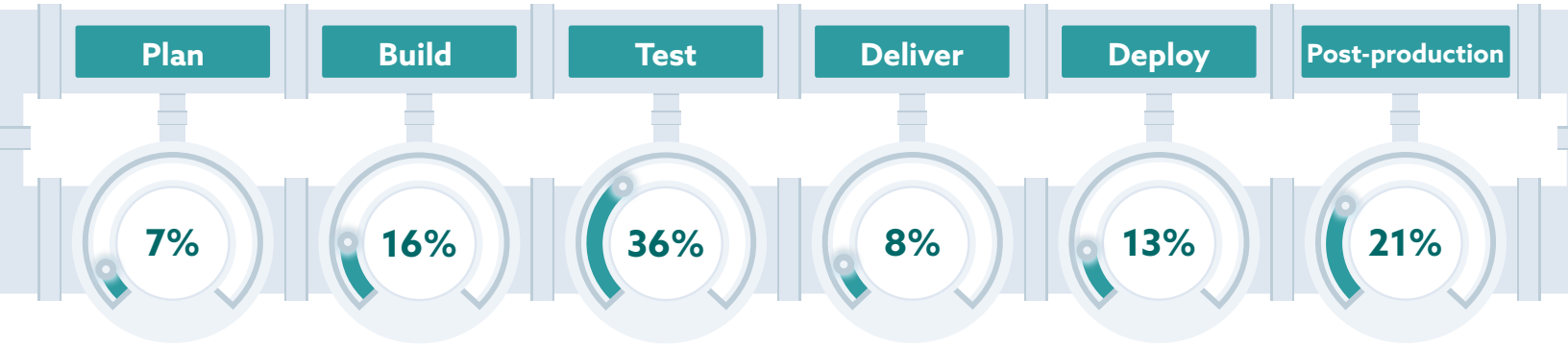
Causes of Cloud Misconfigurations

The primary cause of misconfigurations in organizations was **"lack of knowledge or expertise in cloud security best practices" (62%)**. This is unsurprising since this was noted as a major security barrier earlier. Somewhat more surprising was the second most selected response, **"lack of security visibility and monitoring" (49%)**, since visibility wasn't noted as a primary barrier for resolving security concerns previously in the survey. This could indicate that organizations are not prioritizing resolving challenges around visibility and as a result, visibility is a leading cause of misconfigurations.



Pipeline Delivery Stage Where Misconfigurations are Detected

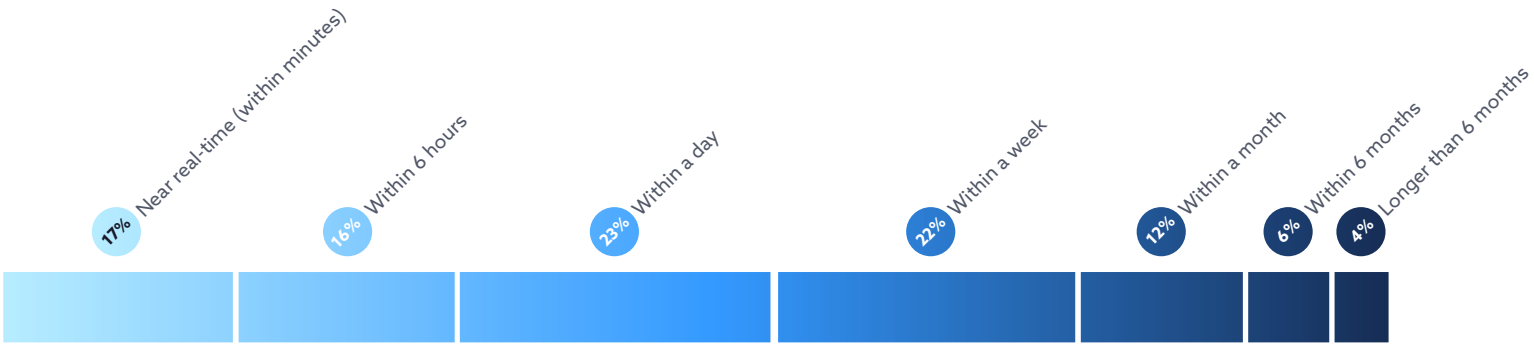
The most common stage in the delivery pipeline where cloud configuration errors are detected are in the **"test" phase (36%)** and the **"post-production" phase (21%)**. This means that most configuration errors are detected prior to deployment (67%) which would suggest in at least some ways organizations have been able to "shift left."



Length of Time to Detect Misconfigurations

The length of time organizations take to detect a cloud configuration mistake varies widely. Most commonly they are finding them **within a day (23%)** or **within a week (22%)**. More concerning however is that **22% of organizations are taking longer than one week** to even find the configuration errors, let alone resolve the misconfiguration.

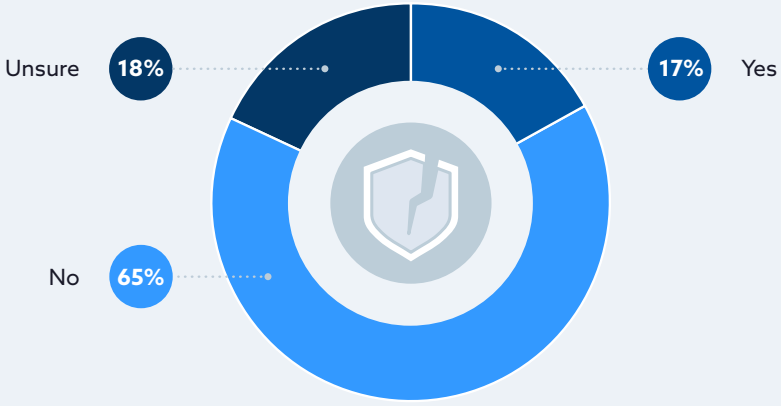
It is also important to note that organizations that reported interdepartmental alignment on policies and their enforcement were more likely to detect a misconfiguration within a day of the error occurring (full alignment - 56%, partial alignment - 41%, no alignment - 31%).



Breaches and Incidents from Misconfigurations

Cloud Security Incident or Breach due to Misconfigurations in the Past Year

Most organizations reported that they had not experienced a **public cloud security incident or breach in the past year (65%)**. About **17% said they had experienced such an incident**, leaving **18% unsure**. Given survey respondents are in job roles directly involved in their organization's cloud security posture, it's concerning that such a high percentage of respondents were not sure whether a security incident or breach had occurred.



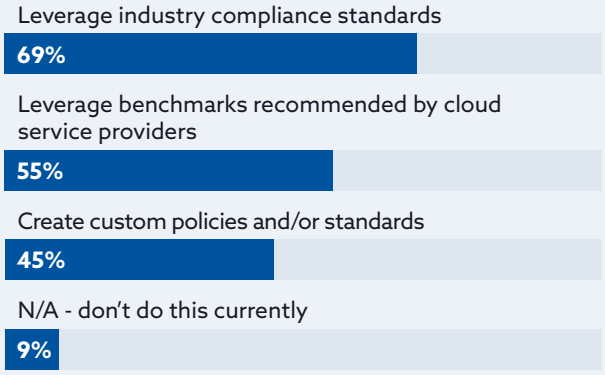
Barriers to Preventing or Fixing Cloud Misconfigurations

Of those 17% who had a cloud security incident or breach, the most common barrier to proactively preventing or fixing the cause was **"lack of security visibility and monitoring capabilities" (68%)** followed by **"lack of knowledge or expertise" (59%)**. Once again, knowledge and visibility are key barriers.

Governance and Compliance

Designing Security and Compliance Standards for Managing Cloud Misconfigurations

Organizations are primarily utilizing **"industry compliance standards" (69%)**, **"benchmarks recommended by cloud service providers" (55%)**, and **"custom policies and/or standards" (45%)**. This leaves only **9%** who reported that designing security compliance standards wasn't something they were currently doing.



Enforcing Standards Across Teams and Organizations

The level of enforcement of security and compliance standards differs among organizations. Roughly an even number of organizations reported **"fully enforced in all environments" (23%), "fully enforced in critical environments only" (26%)**, and **"subset of standards enforced in all environments" (24%)**. This is particularly interesting as 70% of companies reported struggling on interdepartmental alignment on security policies and/or their enforcement.

It should also be noted that organizations who had interdepartmental alignment on policies and their enforcement were more likely to report "fully enforced in all environments" (44%) when compared with those who were aligned on policy, but not enforcement (17%) and those who were not aligned on either (7%).

Balancing Security with Project Delivery

Organizations surveyed tend to **prioritize risk mitigation even if it resulted in some delay in speed of product delivery (41%)**. Another **29% prioritize speed of delivery with some delay in risk mitigation**. To ensure that these responses weren't skewed because of the large number of information security professionals who responded to the survey, the data was also analyzed with their responses omitted. No significant differences were found.

Another notable finding was that organizations who had interdepartmental alignment on policies and their enforcement were more likely to report that they "prioritize risk mitigation over speed of delivery" (35%) when compared with those who were aligned on policy, but not enforcement (12%) and those who were not aligned on either (12%).

Resolution of Misconfiguration Mistakes

Group Responsible for Correcting Misconfigurations

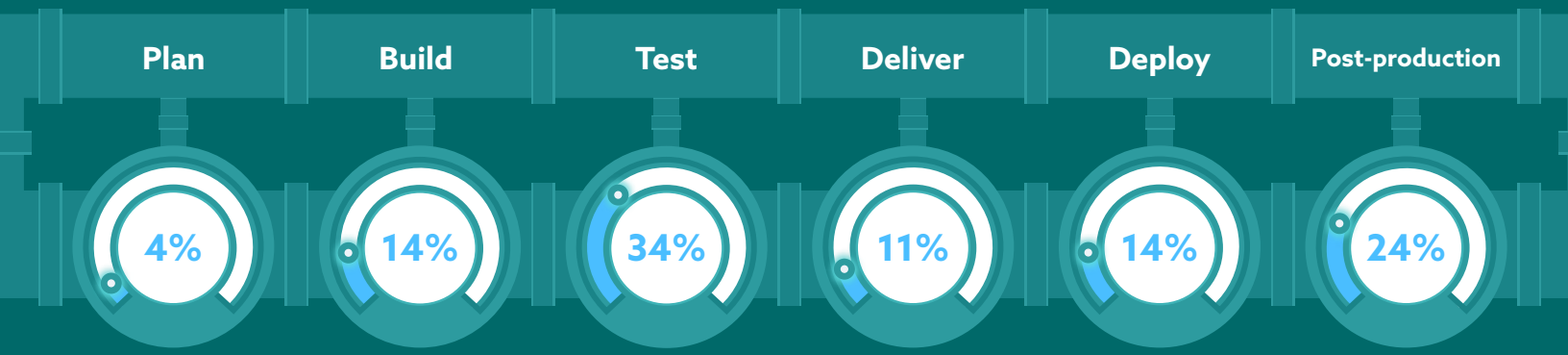
Earlier, we found that the primary group responsible for detecting, tracking, and reporting cloud misconfigurations is Information Security (54%), followed by IT Operations (33%). When it comes to resolving misconfigurations, Information Security and IT Operations are still the two primary groups responsible. However, the division of responsibility seems much more evenly split, with **36% of organizations reporting Information Security** is primarily responsible and **34% of organizations reporting IT Operations** is primarily responsible.

It is interesting that rather than the DevOps or Application engineer teams who are causing such mistakes and in a better position to directly fix these errors, IT operations and information security are held responsible. This once again emphasizes the importance of alignment among these departments. If organizations can gain this alignment and move toward a DevSecOps approach, they will have greater visibility into the activities of the other departments and can work together to more rapidly address misconfigurations and other errors that arise.

Pipeline Delivery Stage Where Misconfigurations are Remediated

The most common stage in the delivery pipeline where cloud configuration errors are remediated are in the **"test" phase (34%)** and the **"post-production" phase (24%)**. This means that most configuration errors are remediated prior to deployment (63%) which would again suggest in at least some ways organizations have been able to "shift left."

These findings are nearly identical to the stage in the delivery pipeline where cloud configuration errors are detected, which was discussed earlier (test, 36%; post-production, 21%; remediating prior to deployment, 67%).

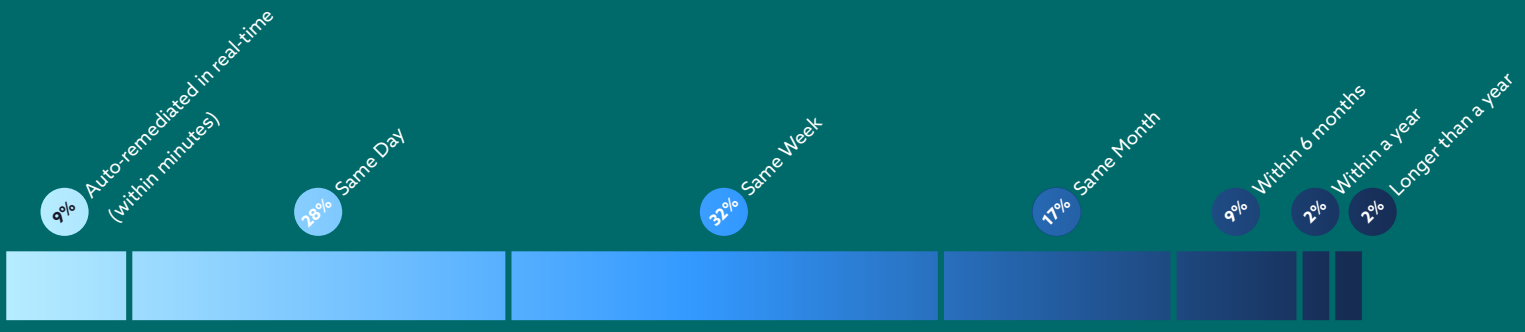


Length of Time to Remediate a Misconfiguration

Most organizations are remediating these cloud configuration mistakes **within the same week (32%) or the same day (28%)**. For approximately 30% of organizations however, it is taking longer than one week to remediate these misconfigurations.

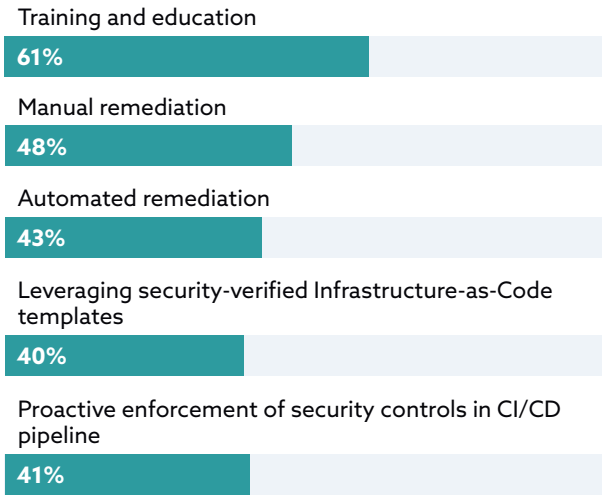
A similar question about the length of time to detect a configuration mistake, found that 78% of organizations were able to detect an error within one week. A similar trend was found with the length of time to remediate a configuration error, with 69% remediating within a week.

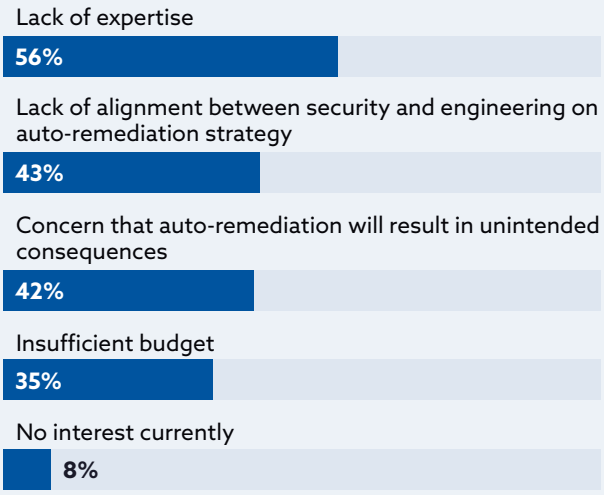
Another notable finding was that organizations that reported interdepartmental alignment on policies and their enforcement are also more likely to remediate that error within a day of detecting the misconfiguration (full alignment - 51%, partial alignment - 24%, not alignment - 19%).



Methods for Improving Resolution of Security or Compliance Misconfigurations

The most common method organizations use to improve the resolution of security and/or compliance misconfigurations in cloud environments is "training and education." This is unsurprising since lack of knowledge has repeatedly been indicated as a key barrier to security. The second and third most common responses were **"manual remediation" (48%)** and **"automated remediation" (43%)**. Although automation made the top three methods, it's clear that many organizations have yet to fully implement auto-remediation since it wasn't a commonly selected response when asked about the length of time it takes their organization to remediate misconfigurations in the previous question.





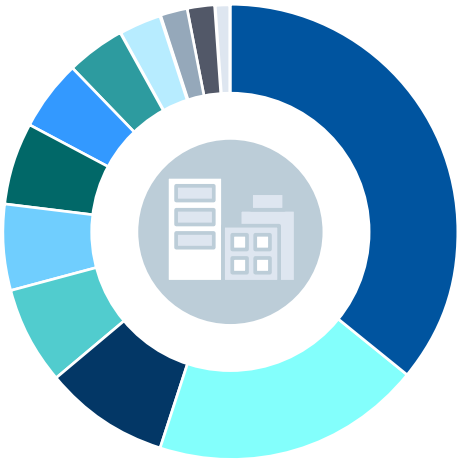
Barriers to Using Auto-Remediation

For those who don't utilize automated remediation, the most common reasons for not using this solution were once again, **lack of expertise (56%)**. The second most common reason cited was the **lack of alignment between departments on the auto-remediation strategy (43%)**. This is once again unsurprising since 70% of organizations are struggling to obtain interdepartmental alignment on security policies and/or policy enforcement. A close third reason was that there was **concern that auto-remediation could result in unintended consequences (42%)**. This could be tied back to the issue of lack of expertise and knowledge. If the teams don't know how to properly utilize the technology, there is a much higher likelihood that they could run into unintended consequences.

Demographics

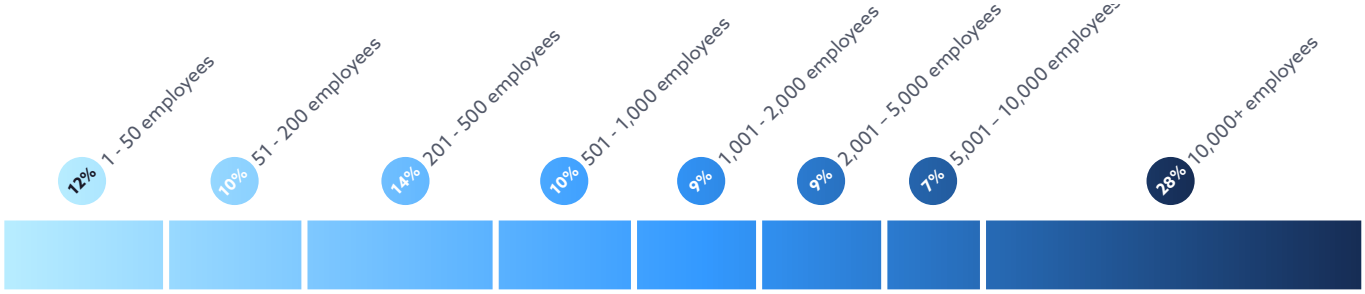
This survey was conducted from May 2021 to June 2021 and gathered 1090 responses from IT and security professionals from a variety of organization sizes, industries, locations, and roles.

Organization Industry

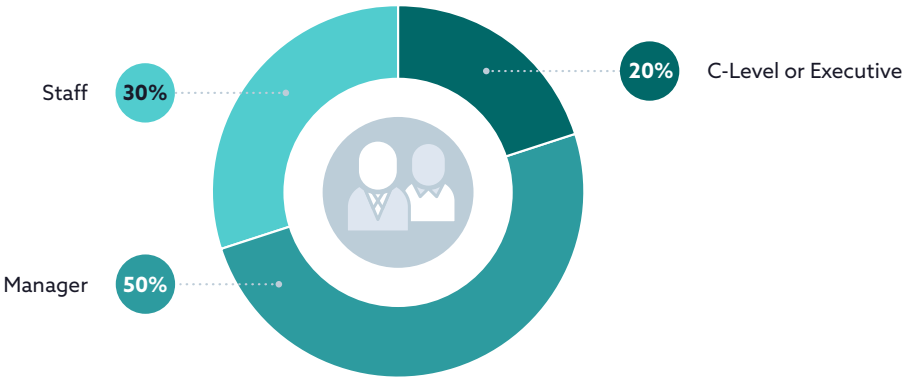


- **36%** IT and technology
- **19%** Financial services
- **16%** Public sector (government, education, etc.)
- **9%** Business and professional services
- **6%** Other
- **6%** Health, pharmaceuticals, and biotech
- **5%** Telecommunications
- **4%** Manufacturing and production
- **3%** Retail
- **2%** Energy, oil/gas, and utilities
- **2%** Travel and transportation
- **1%** Construction and property

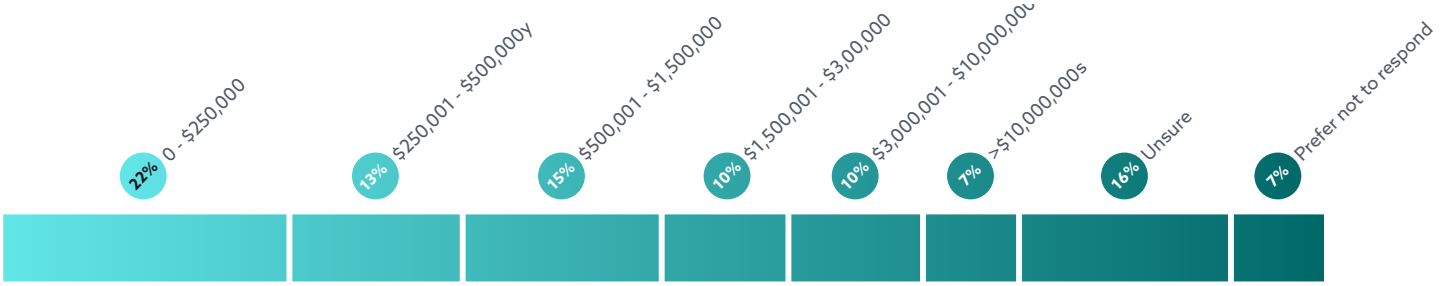
Organization Size



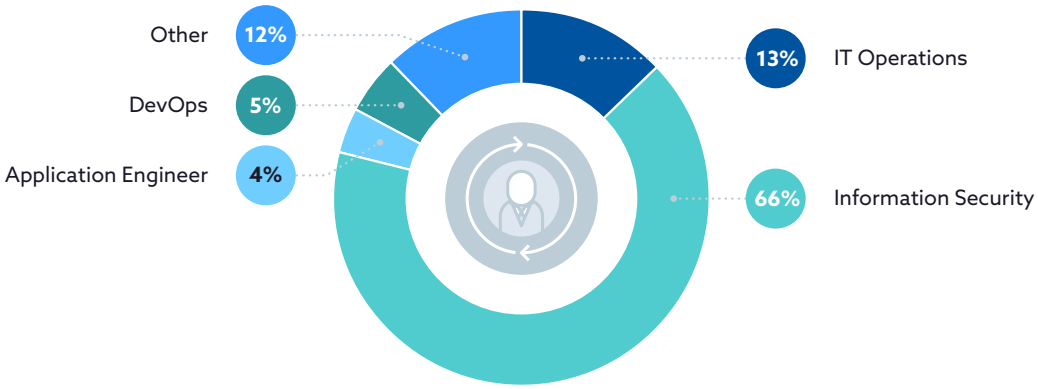
Job Level



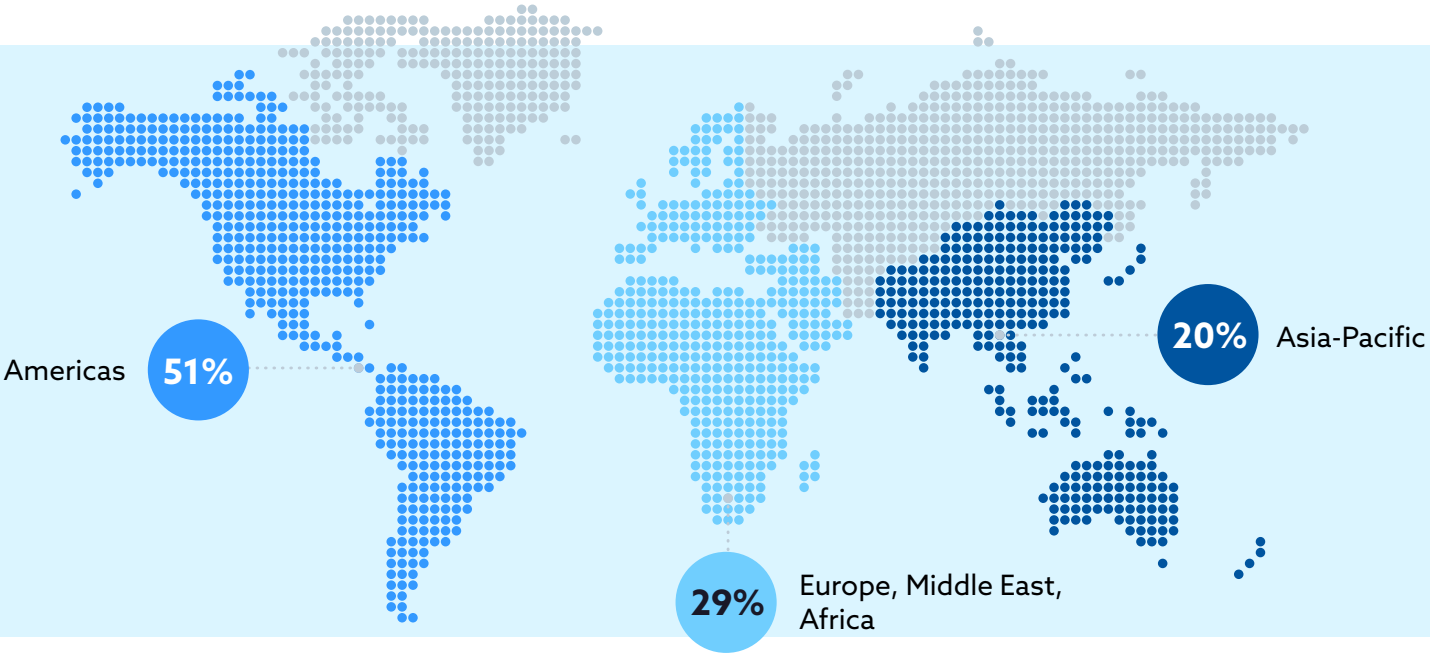
Organization Public Cloud Spend



Primary Job Department



Location



Top contributing countries include: United States of America, India, United Kingdom of Great Britain and Northern Ireland, Canada, Australia, Singapore, Germany, Switzerland, France

About the Sponsor

VMware is a leading innovator in enterprise software. We power the world's digital infrastructure. Our cloud, app modernization, networking, security, and digital workspace platforms form a flexible, consistent digital foundation. This foundation empowers businesses to build, run, manage, connect, and protect applications, anywhere–enabling technology-driven transformation without disruption. VMware acquired CloudHealth Technologies, Inc. in October of 2018.

CloudHealth by vmware®

Sponsors are CSA Corporate Members who support the findings of the research project but have no added influence on the content development or editing rights of CSA research.