DivvyCloud

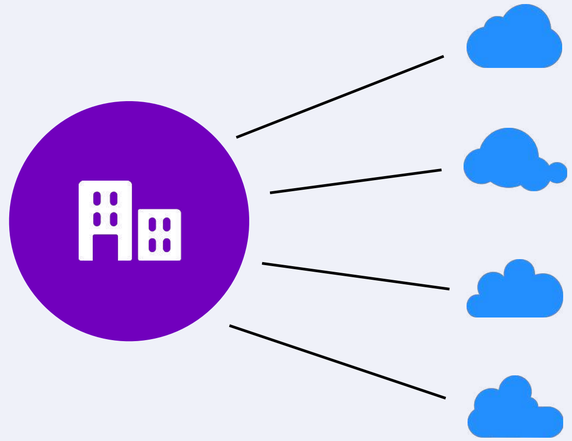
2020 State of Enterprise Cloud Adoption and Security

Enterprises Believe the Cloud Is Critical to Fuel Innovation, but Struggle with Security

Table of Contents

Executive Summary

Enterprise cloud adoption has been growing steadily in recent years, and as our survey demonstrates, it continues to accelerate. To better understand how enterprises are adopting public cloud, multi-cloud, containers, and other services, as well as the challenges they experience in maintaining security and compliance, we surveyed nearly 2,000 IT professionals throughout the 2019 calendar year. We then analyzed the data and compiled the results into this report. To illuminate trends over time, we have compared some of this year's results to the results of a similar survey conducted in 2018.



For some, the fear of suffering a data breach in the cloud is crippling and slows adoption to a crawl. For many others, they choose to circumvent security with hopes of gaining access to the agility and speed offered by cloud adoption. Too often, enterprises are making a false choice: either embrace cloud rapidly and carelessly, or approach it with such timidity that inhibits true cloud adoption. But the news isn't all bad. We observe in this report that some enterprises are finding a middle ground: the ability to adopt cloud at pace but doing so in a way that embraces friction-free, continuous security and compliance.

While most agree that taking advantage of this technology is good for business, it's clear from the onslaught of news headlines about data breaches caused by misconfigurations that companies are struggling to embrace the cloud in a secure, controlled manner. Our hope is that this report provides guidance to leaders and practitioners in how others are approaching their cloud strategy so you can better inform your path forward.

PART 1

Foreword

Running an IT shop today almost always means utilizing some form of cloud-based technology. This year's report validates what I see every day with clients of all sizes, across all stages of adoption maturity. Simply put, in almost all cases, legacy IT processes and policies have not kept pace with how cloud resources are being deployed.

With proper planning and the right people, processes, and tools, any enterprise can work efficiently, effectively, and securely in the cloud. Conversely, even as cloud adoption rates continue to grow, there is a troubling trend. Organizations are not implementing cloud security strategies at the time of cloud adoption.

This asynchronous approach to cloud adoption and the security that should go with it creates tremendous risk. Enterprises are accepting this risk, and they are doing so needlessly because security does not have to impede the power and efficiency that cloud offers.

This report offers valuable quantitative and qualitative perspectives on cloud, multi-cloud, and container adoption. It's helpful to know the rate at which enterprises are adopting cloud, but it's invaluable to know *how well* their cloud journeys are going. Together, the quantitative and qualitative information presented in this report indicates that cloud adoption remains strong, and while many enterprises are moving in the right direction, many are still struggling to achieve a comprehensive security and compliance posture.

PART 2

Foreword

Much progress has been made, but clearly we have much more work to do. It is my belief that ultimately people want to do the right thing, but working at the speed of cloud means that the supporting processes of the organization have to scale with that speed or individuals will go around the existing roadblocks. From both my experience at GE and ongoing work with existing clients, the only way to solve for scale is through automation.

The traditional role of security being a central controlling function has shifted, and it is everyone's responsibility in the organization to ensure that cloud resources are deployed and managed securely. The data outlined here is a call to action that we must educate, automate, and remediate. We must focus security efforts earlier in the development and deployment process and use automation to remediate nonconformance against policy, and we must also use automation to educate the organization and drive a shift in the culture.

Thomas Martin

Thomas Martin is the founder of **NephōSec**, where he and his team help startups to Fortune 500 multinational companies - spanning industries as diverse as consumer retail, travel, and financial services.

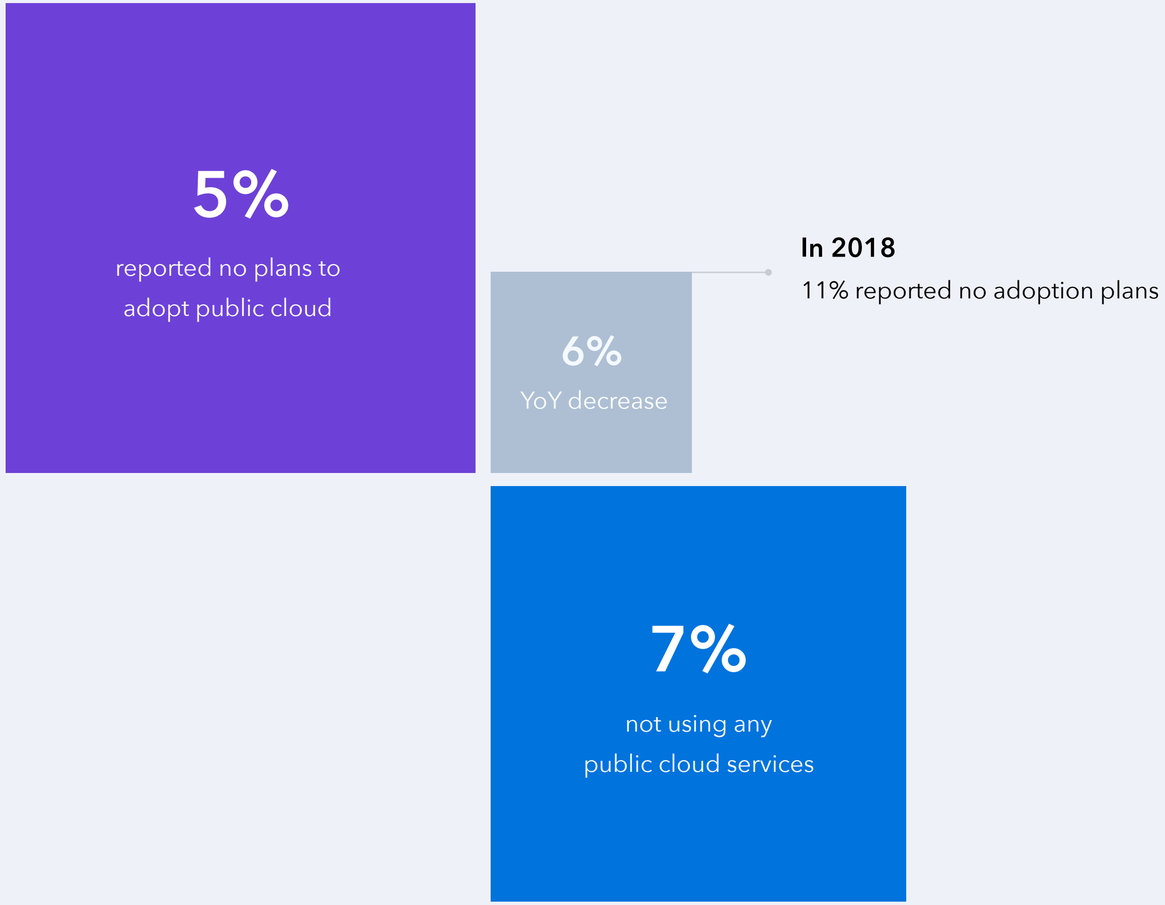
His team has pioneered automated remediation in thousands of cloud accounts under monitored management with individual resources in the millions. As a prior CIO and technologist at the **General Electric Company**, he has led the migration of 9,000 legacy workloads to public and private cloud infrastructure.

Trends in Cloud Adoption

Cloud Is Quickly Becoming Ubiquitous

Only 7% of organizations surveyed are not using any public cloud services, meaning the vast majority of enterprises have already embraced the cloud. What's more, only 5% reported no plans to adopt public cloud, a significant drop from the 11% who reported no adoption plans in 2018.

Despite popular opinion, larger enterprises may actually be struggling more than their smaller peers when it comes to cloud adoption. Of the respondents who confirmed their organizations are not using public cloud or have no plans to adopt public cloud, 30% are from organizations with 10,000 or more employees. This is followed by respondents from companies with 1 - 250 employees at 27%, while only 9% of respondents are from companies with 5,001-10,000 employees. The data suggests that mid-sized companies might be in the best position to adopt public cloud—large enough to have adequate resources to make the migration, but not too large so that the transition seems overly daunting, complex, or costly. However, large enterprises aren't always homogenous and often have multiple business units of varying sophistication. In these larger businesses, it is not uncommon for the more advanced business units to adopt cloud first with the smaller units following suit.



Trends in Cloud Adoption

Enterprises Continue to Race Through Cloud Adoption Lifecycle

When asked about the current state of public cloud adoption in their organization, respondents showed a positive progression across the board. A majority of respondents reported being in the final optimization stages of their cloud journey, with 59% indicating they are in the DevOps Optimization stage (an 11% increase from last year), and 36% indicating they are in the CloudOps Optimization stage.

On top of this, 47% of respondents are in the Application Migration Implementation phase, and 49% are aligning their cloud operations with their in-house policies and procedures, including security and governance. Just 28% are undergoing the Strategy and Economics Evaluation phase. Most enterprises report being in optimization stages of cloud adoption; however, this may not necessarily be a positive trend. Considering the lack of security policies and frameworks in place for cloud and container environments (included later in this report), it could be that enterprises are rushing through adoption without taking the proper assessment and evaluation steps to ensure their approach to cloud and containers is secure, compliant, and appropriate given their unique business operations needs.

Reported States of Public Cloud Adoption

59%
DevOps Optimization

36%
CloudOps Optimization

47%
Application Implementation

49%
Aligning Cloud Operations with Policies and Procedures

28%
Strategy and Economics Evaluation

Trends in Cloud Adoption

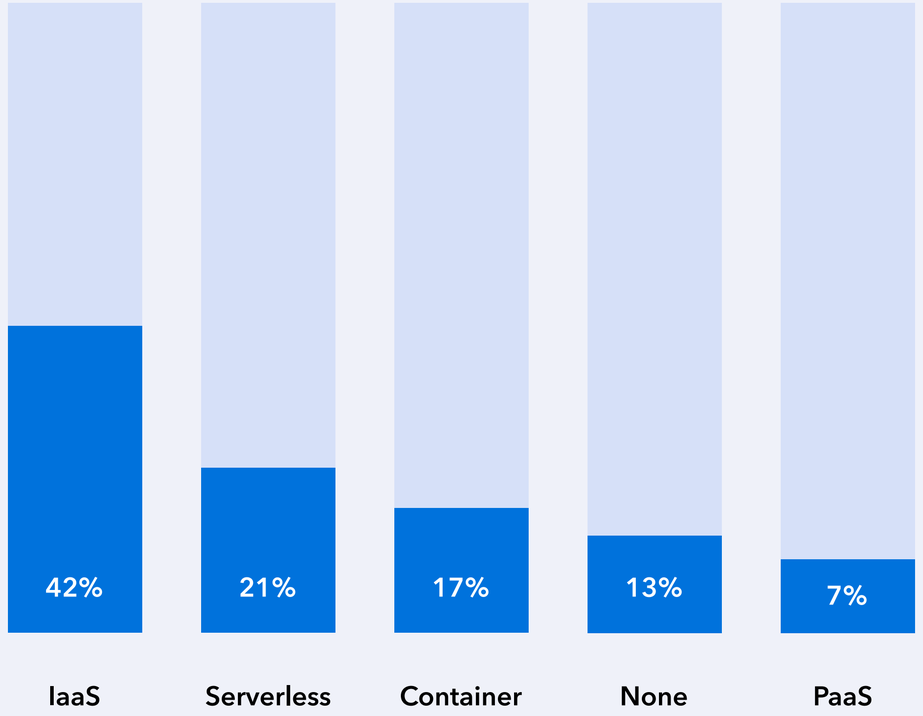
Multi-cloud Strategies Are Declining Among Enterprises?

Last year, 77% of respondents confirmed their organization was using two or more cloud services. This year, 64% reported using two or more cloud services, a 13% decline in just one year. This decline is likely due to companies struggling to implement effective multi-cloud strategies securely, given the additional complexity of using more than one cloud service provider. These companies who are scaling back to a single cloud effort from a multi-cloud strategy, need to be careful about abandoned resources. The resources in an orphaned provider presents high risk. However, as the rate at which enterprises adopt proper cloud security and compliance catches up to the rate of overall cloud adoption, DivvyCloud researchers expect an increase in multi-cloud use.

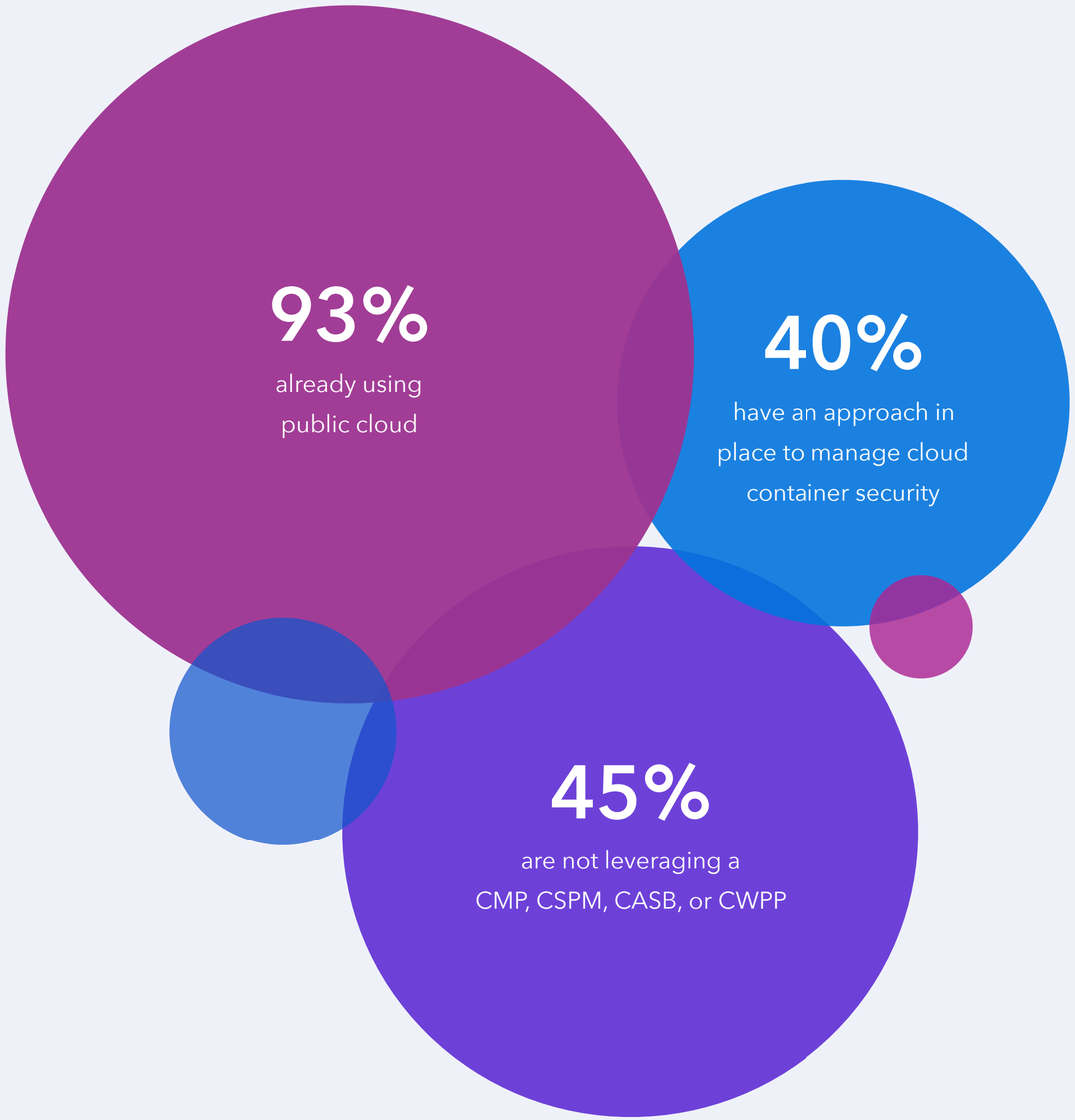
Infrastructure-as-a-Service Tops Advanced Architectures Employed by Enterprise

When asked to name the architectures their organizations currently use or plan to use within the next year to build apps, 42% said Infrastructure-as-a-Service (IaaS). While this is a 12% decrease from last year, it is still a strong indication that IaaS is particularly enticing to enterprise. Twenty-one percent of respondents selected serverless, 17% selected containers, and just 7% selected Platform-as-a-Service (PaaS).

Architecture Used or Planned for Use in the Next Year



Looking specifically at larger organizations, the interest in IaaS is even stronger. Of organizations surveyed with 10,000 or more employees, 53% either already use or plan to use IaaS to build apps in the next year.



IT Professionals Consider Cloud Adoption Critical to Innovation…

A full 85% of respondents believe that cloud adoption is necessary for their organization to drive innovation and remain competitive. The speed and agility of cloud services can make all the difference between stagnation and innovation, and enterprises know it. This understanding certainly contributes to the high rate of cloud adoption, but as the data in this report indicates, it's clear that proper cloud security is not keeping pace.

…but Are Not Equipped to Operate in the Cloud Securely

Among enterprises already using public cloud (93%), only 40% confirmed their organization has an approach to managing cloud and container security in place. Additionally, 45% confirmed their organization does not use any of the following cloud security services:

- Cloud Management Platform (CMP)
- Cloud Security Posture Management (CSPM)
- Cloud Access Security Broker (CASB)
- Cloud Workload Protection Platform (CWPP)

Cloud Security and Compliance

Rampant Data Breaches Caused by Misconfigurations

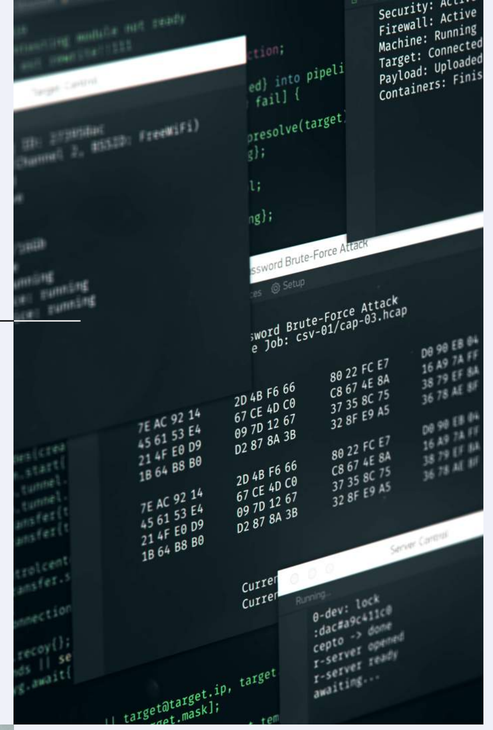
The huge discrepancy between the rate of cloud adoption and implementation of proper security is the reason data breaches caused by cloud misconfigurations continue to be rampant, costing enterprises an estimated $5 trillion in 2018 and 2019 alone. In fact, out of the respondents who confirmed their organization had suffered a cloud services data breach or other security incident within the last 12 months, 59% confirmed it was due to a misconfiguration, and another 15% weren't sure of the cause.

Understanding of Applicable Frameworks Is Low

Out of all IT professionals surveyed, 42% do not know which frameworks their company uses to maintain compliance with standards and regulations. These frameworks include GDPR, HIPAA, PCI DSS, SOC 2, CIS, FedRAMP CCM, and NIST CSF—just to name a few. Worse yet, the number of IT professionals unaware or unfamiliar with the standards and regulations to which their organization must comply actually increased 8% since last year. This trend could be an indication that because new regulations are emerging each year for both geographic regions (e.g. GDPR and CCPA) as well as industry verticals (e.g. HIPAA), it is getting more and more difficult for organizations to keep track of and ensure compliance with the various frameworks that apply to them.

59%

confirm data breach
caused by misconfiguration



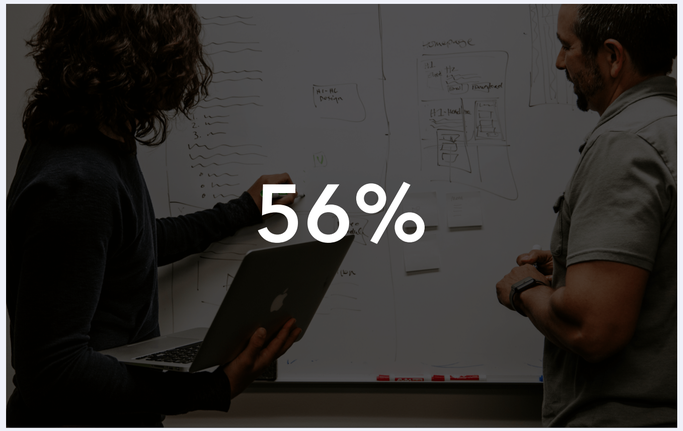
42%

don't know which
frameworks to use

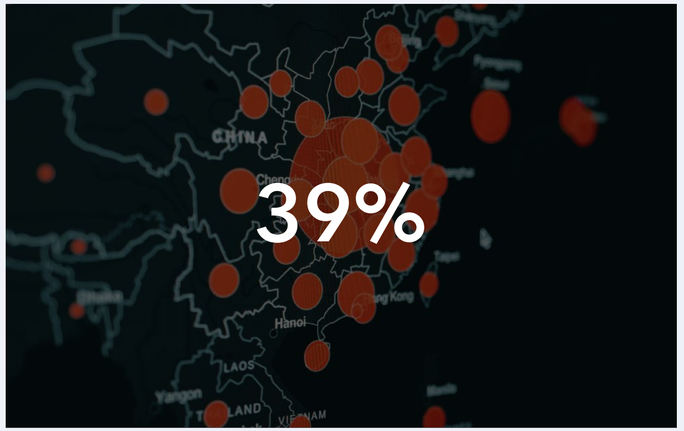
Cloud Security and Compliance

Primary Threats

When asked to name the top three biggest cybersecurity threats facing their organization, respondents chose misconfigurations (56%), data breaches (39%), and user permission and management (38%).

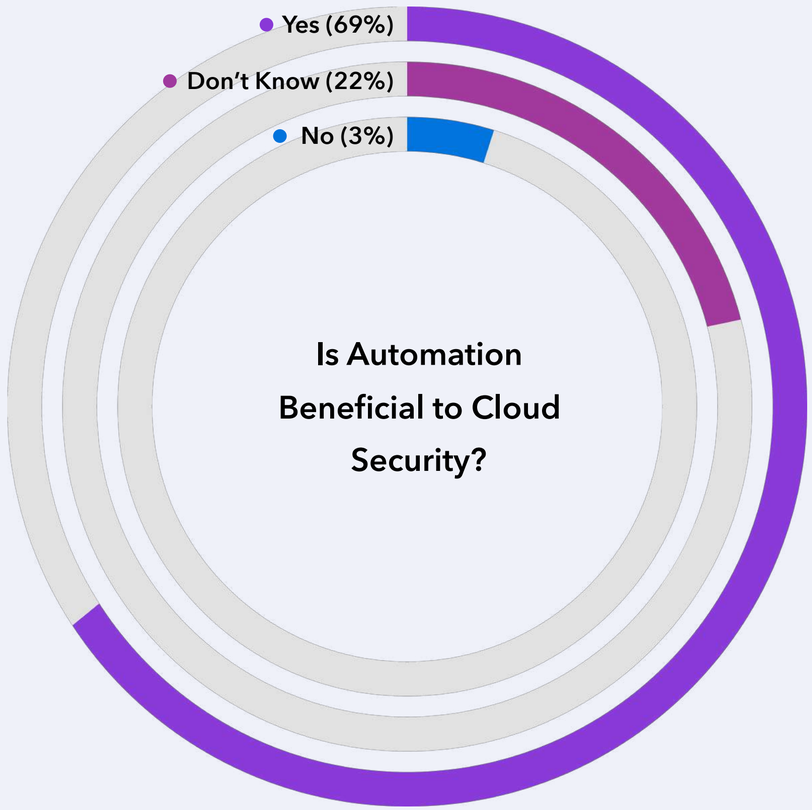


Misconfigurations



Data Breaches

User Permission & Management



Automation in Cloud and Container Security

Automation Is Coveted, but Not Leveraged...

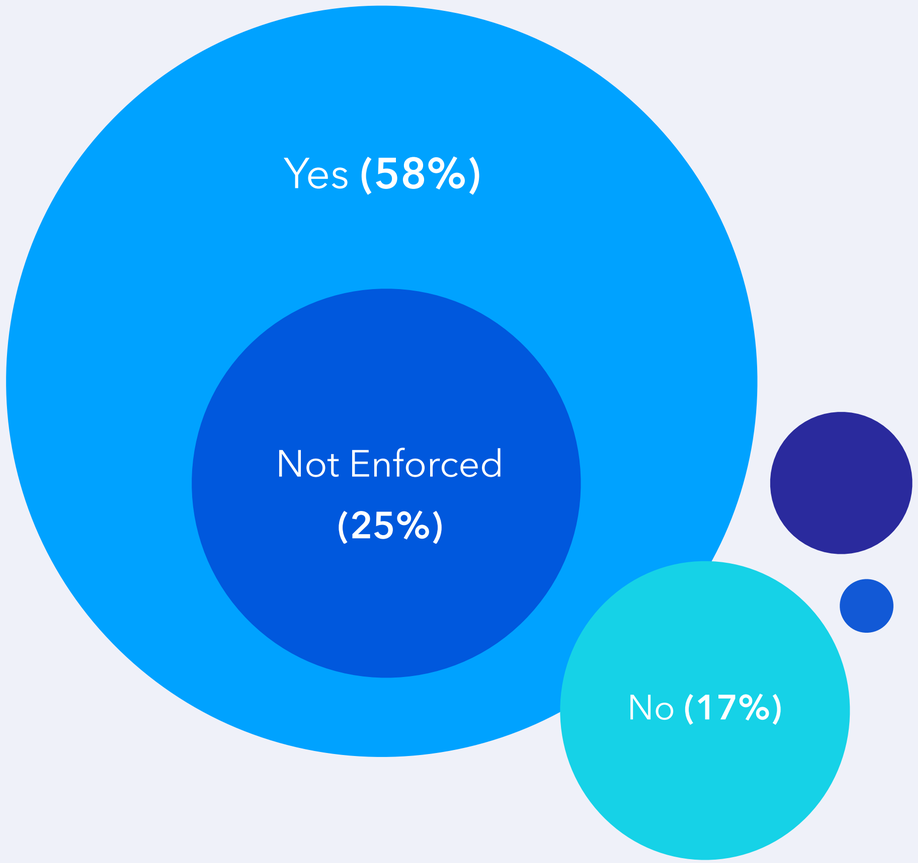
More than two-thirds of all respondents (69%) believe that automation can provide benefits to their organization’s cloud security strategy, but only 48% say their cloud security strategy currently relies on products that leverage automation. An additional 18% said they plan to adopt tools that leverage automation within the next 12 months. An overwhelming number of respondents (85%) trust automated security solutions more than or the same as human security professionals, and 43% specifically said they trust automated security solutions more than human security professionals. This is a clear indication that enterprises are realizing that humans are prone to error, and with the high rate of change in cloud and container environments, automation is critical to ensuring proper implementation and continuous enforcement of security and compliance.

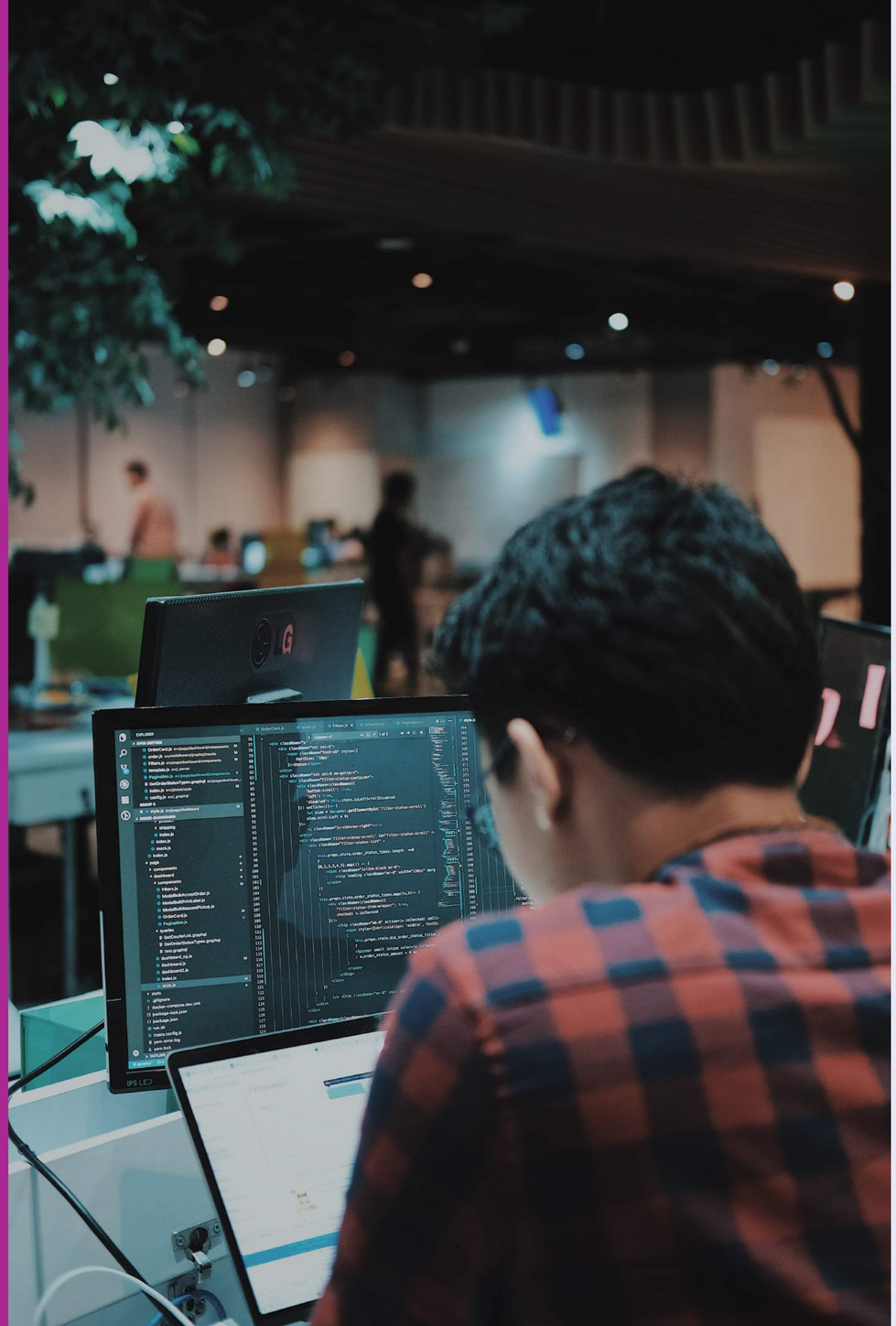
Developers and Security Still Misaligned

Clear Guidelines for Secure Cloud Operations Are Lacking...

The data is clear—organizations are adopting public cloud before establishing cloud-specific internal policies for security and compliance. Of the respondents who confirmed their organization is using public cloud, only a little more than half (58%) said their organization has clear guidelines and policies in place for developers building applications and operating in the public cloud. And of those, 25% said these policies are not enforced, while 17% confirmed their organization lacks clear guidelines entirely.

Do Organizations Have Guidelines/Policies for Developers Working in Public Cloud?





Developers and Security Still Misaligned

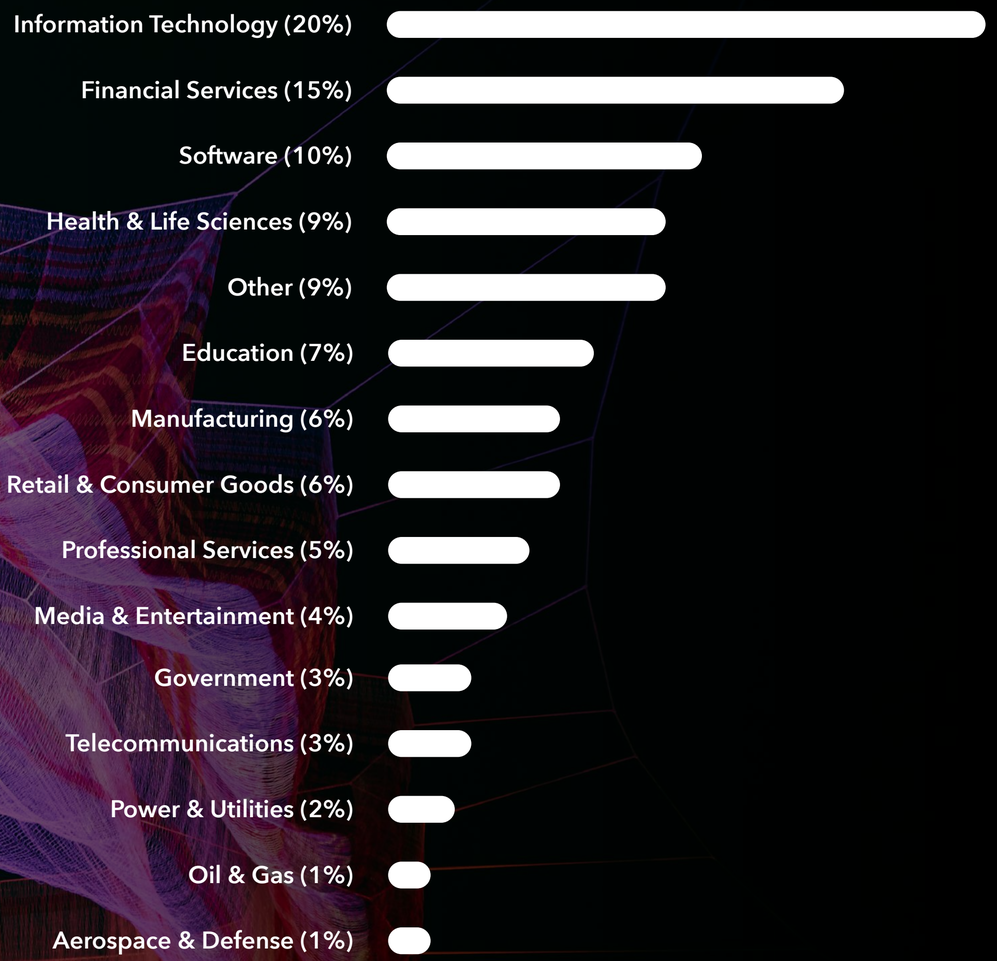
...and Many Developers and Engineers Ignore Security and Compliance Policies

Almost half (49%) of all respondents whose organizations use public cloud said that their developers and engineers, at times, ignore or circumvent cloud security and compliance policies. While this may seem like a shockingly high number, it supports the overall challenge identified in this report—that enterprises and their employees feel they must choose between security and innovation. Developers often feel that security and compliance policies limit their ability to build and deploy new services quickly and efficiently, so they choose to work around them.

Developers and Security Still Misaligned

IT and software companies are the worst offenders when it comes to circumventing cloud security.

Of the respondents who confirmed their developers/engineers ignore cloud security and compliance policies, 30% are from IT and software companies. Comparatively, 15% are from financial services companies, 9% are from health and life sciences, 7% are in education, 6% are in manufacturing, another 6% in retail, and 4% are in government. Similarly, only 35% of respondents do not believe security impedes developers' self-service access to best-in-class cloud services to drive innovation—meaning 65% believe they must choose between giving developers self-service access to tools that fuel innovation and remaining secure.

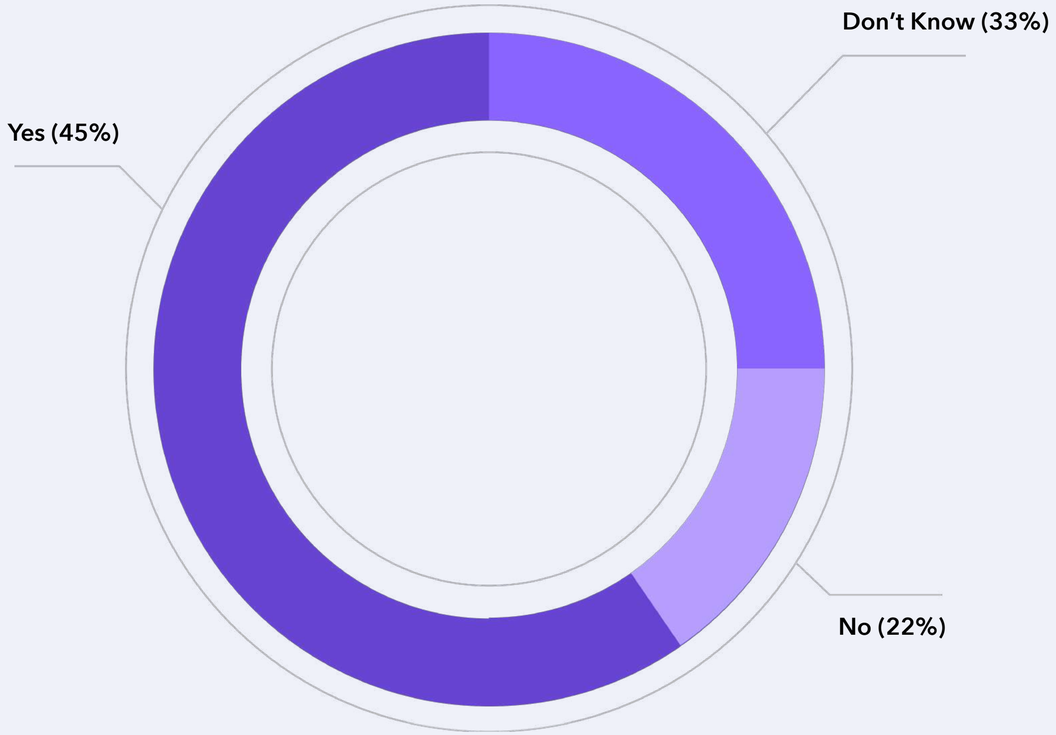


Developers and Security Still Misaligned

Developers/Engineers Are Not Held Responsible for Compliance and Security

In addition to circumventing compliance and security policies, DivvyCloud researchers found that less than half of organizations (45%) hold their engineers and developers responsible for remediating security and compliance issues within their projects. This is a significant challenge because if security and compliance guidelines aren't enforced among the developers and engineers, and they're not required to remediate issues within their projects, then they are not learning how to use new tools and resources securely and are all but doomed to repeat similar mistakes in the future.

Are Developers/Engineers Required to Remediate Security and Compliance Issues Within Their Projects?



Overcoming the False Choice Between Innovation and Security

The findings of this report clearly demonstrate that enterprise cloud adoption continues to outpace adoption of proper security and compliance, and that organizations believe they must choose between security and innovation. But this belief is simply not true. It is entirely possible to deliver advanced products and services while maintaining a secure cloud environment. Organizations must be able to trust that developers and engineers are provisioning and configuring cloud and container services properly; adhering to the necessary security, compliance, and governance policies; and using automation to enable this needed cultural shift.

Once security and remediation policies are clearly defined, enterprises can implement automated solutions that provide continuous enforcement and create a seamless and constant feedback loop for developers and engineers, thus removing any perceived barrier between innovation and security. These controls grant companies the ability to detect errors that typically arise from circumventing cloud security and compliance policies, and then either alert the appropriate personnel to remediate the issue or initiate an automated remediation in real-time. By employing the necessary people, processes, and systems concurrent with cloud adoption (not weeks, months, or years later), enterprises can ensure continuous security and compliance in the cloud.

Methodology

About this report

The data in this report is from a survey conducted throughout 2019, which generated responses from 1,833 participants. The survey respondents spanned all major industry verticals, organizational sizes, and job functions. Displayed to the right are detailed demographics on company size and industry. Due to rounding and questions for which multiple answers were allowed, not all percentage totals in this report equal 100%.

COMPANY SIZE	RESPONDENTS
1 - 250	24%
251 - 1,000	14%
1,000 - 5,000	19%
5,001 - 10,000	10%
10,000+	33%

INDUSTRY	RESPONDENTS
Information Technology	20%
Financial Services	14%
Software	14%
Health & Life Services	8%
Education	7%
Retail & Consumer Goods	5%
Media & Entertainment	5%
Manufacturing	4%
Professional Services	4%
Government (Local, State, & Federal)	4%
Telecommunications	2%
Power & Utilities	1%
Aerospace & Defense	1%
Oil & Gas	1%
Other	10%

About DivvyCloud

DivvyCloud protects cloud and container environments from misconfigurations, policy violations, threats, and IAM challenges. Our software combines prevention of risk during CI/CD with real-time detection and automated remediation, empowering customers to achieve full lifecycle, continuous security and compliance. With DivvyCloud, you can accelerate innovation using cloud and container technology without the loss of control.

Freedom is good. Chaos is bad.

To learn more about how to improve your cloud security, speak with DivvyCloud's experts today.