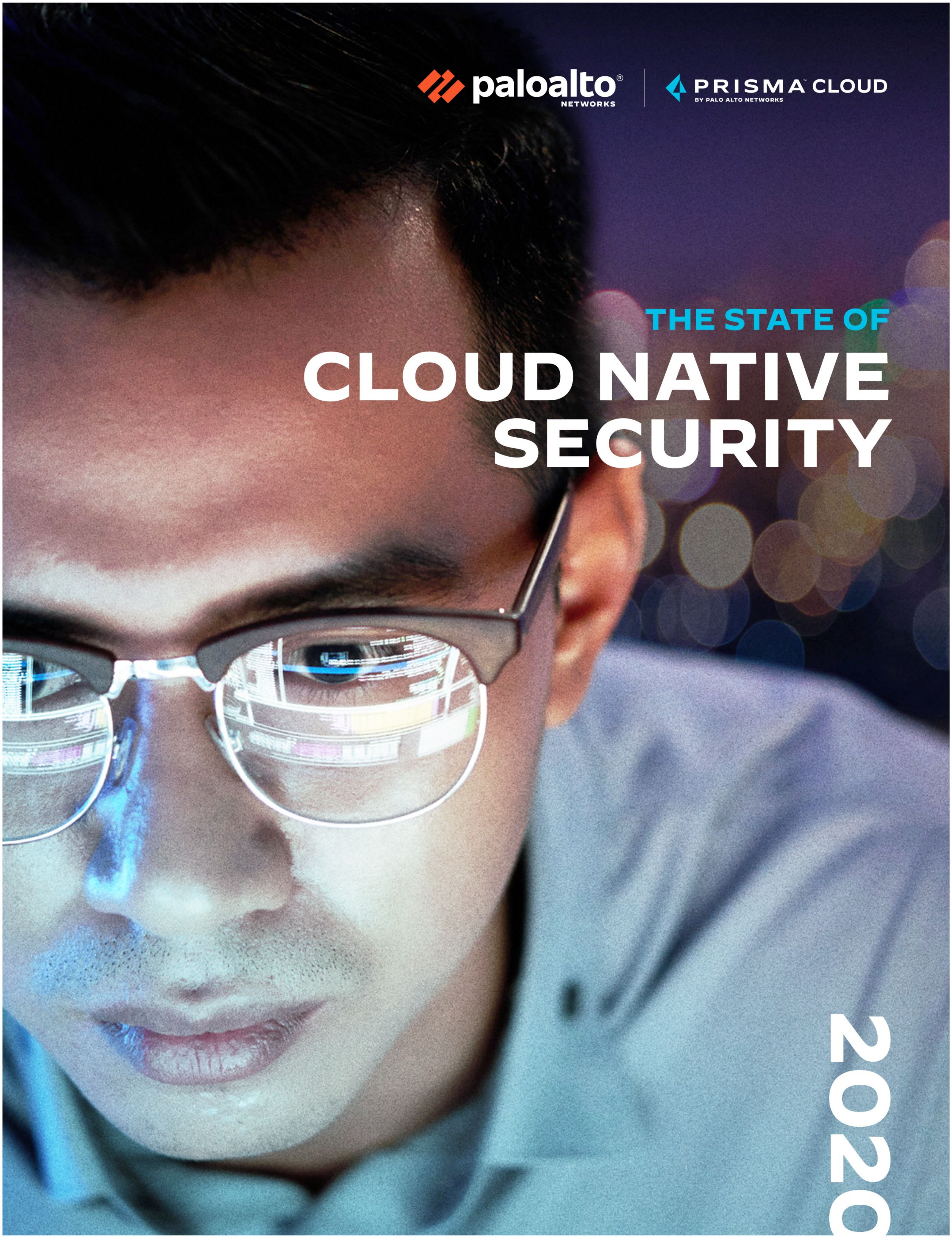


paloalto NETWORKS | PRISMA CLOUD BY PALO ALTO NETWORKS

THE STATE OF

CLOUD NATIVE SECURITY

2020

Table of Contents

Introduction

As the engine that powers business, science, education, government and so many other human endeavors, computing has evolved enormously over the past few decades – and that evolution is accelerating.

Today, the focus is less on the hardware underlying computing and more on the application itself – the thing that delivers actual value. We abstract computing away from the hardware as much as possible, in myriad ways: the concept of the cloud itself, as well as the specific technologies for operating in the cloud, such as virtual machines (VMs), infrastructure as a service (IaaS), platform as a service (PaaS), containers, managed container services such as Kubernetes and more.

As we adopt all these enabling technologies, we introduce a new responsibility: securing cloud systems and the data we're running on them. The need to address threats such as operating system and application vulnerabilities, cross-site scripting or SQL injection, and accessing data at rest has created an entire market for security tools and services. Today we have a whole new set of decisions to make, security plans and protocols to create, and processes to develop and implement.

That's why you now have this **STATE OF CLOUD NATIVE SECURITY** report in front of you. The companies behind this survey and research project all want to better understand the landscape our customers are operating in, so we can do a better job of helping them. We also want to share the knowledge we've gained with you, and everyone involved with securing the cloud, to keep our and our customers' information safe and secure.

About the report

The first **STATE OF CLOUD NATIVE SECURITY** report from Palo Alto Networks and Accenture outlines the practices, tools and technologies that companies around the world use to manage security for cloud native architecture.

Based on a survey of 3,000 professionals in cloud architecture, information security, DevOps and application development located across five countries and five industries, this report will help you make decisions about your own cloud transformation or cloud use, so you can realize the full potential of cloud. The information and recommendations we share are based on a proprietary set of recently gathered and rigorously analyzed data. To learn how we conducted our survey and analyzed the results, read the Methodology section of this report.

What we have learned from this survey – along with the feedback we hope to get from you and others in the IT and InfoSec communities – will help us create a new survey next year, and every year, that will enable us all to continually learn about and improve our industry.

Presented by:

Prisma Cloud by Palo Alto Networks offers the industry's broadest security and compliance coverage – for applications, data and the entire cloud native technology stack – throughout the development lifecycle and across multi- and hybrid cloud environments. The Prisma Cloud native security platform supports an integrated approach that enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud native application development and deployment securely.

Follow us @Prisma_Cloud on Twitter or learn more at https://www.paloaltonetworks.com/prisma/cloud.

Sponsored by:

accenture

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture helps organizations protect valuable assets end to end. With services that include strategy and risk management, cyber defense, digital identity, application security, and managed security, Accenture enables businesses around the world to defend against known sophisticated threats and the unknown.

Follow us [@AccentureSecure]() on Twitter or visit us at [www.accenture.com/security]().

Executive Summary

SECTION ONE

The State of the Cloud and Cloud Native Adoption

Cloud will become the dominant computing model over the next 24 months

- Enterprises using the cloud are close to the halfway point in their journey to the cloud. They now run 46% of their workloads in the cloud and expect to get to 64% in the next 24 months.

We are in a multicloud, multi-compute world

- 94% of organizations use more than 1 cloud platform
- 60% use between 2 and 5 platforms
- AWS is the most popular public cloud service provider

Diversity in application architectures is likely to continue, leading to growth in all forms of compute (IaaS, CaaS and PaaS) that power cloud applications

- No one compute dominates: Companies are spreading their workloads across all four computes (VMs 30%, containers 24%, CaaS 21%, PaaS 22%)
- 86% of companies expect their usage of all four computes to increase or stay the same over the next two years

Customers expect cloud to continue to evolve

- 80% of respondents say their company's cloud infrastructure is constantly evolving

SECTION TWO

The State of Securing the Cloud and Cloud Native Workloads

The top three challenges for moving workloads to the cloud

- Technical complexity (42%)
- Maintaining comprehensive security (39%)
- Ensuring compliance (32%)

Security cannot be addressed by solving for a single issue

- Respondents chose these top issues as being their biggest cloud threats:
  - ◊ Data security and malware
  - ◊ Application vulnerabilities
  - ◊ Weak and broken authentication
  - ◊ Insider threats
  - ◊ Credential leakage
  - ◊ Insecure APIs
  - ◊ Over-permissioned access
  - ◊ Misconfigurations

Challenges to providing comprehensive cloud security are often internal to a company's culture and organization

- The top four challenges identified by survey takers:
    - ◊ Lack of visibility of security vulnerabilities (15%)
    - ◊ Employee training on security tools (14%)
    - ◊ Employee training on safe practices (11%)
    - ◊ Evaluating the current state of security (11%)

Cloud security team structures are in transition. Most companies have a hybrid model comprising a center of cloud security excellence that works closely with security points of contact in decentralized development teams

- 77% of companies have more than 20 people on their cloud security teams
- 47% have both a centralized cloud security team and security experts embedded with delivery teams (cross-functional)
- 31% have a fully centralized cloud security structure
- 22% use a fully cross-functional cloud security structure

Organizations don't understand that cloud security responsibilities are shared

- 73% of companies struggle to clearly delineate between their cloud security provider's (CSP's) security responsibilities and their own

More security tools doesn't necessarily mean better security

- Companies investing more than $100 million in cloud are trimming the number of tools they use
    - ◊ 53% of this high-spending group use just 5 or fewer cloud security tools
- Acquiring more tools and vendors can create inefficiencies and make employee tool training more difficult
- Companies start to see overlaps between tools and vendor offerings, so they consolidate and rationalize tools and tool providers
- 71% of companies use third-party vendor tools, 65% use CSP-provided security tools and 62% use open source tools

Cloud security spend is rapidly catching up with cloud spend

- Cloud security spend is highest for companies with an annual cloud budget of $100 million or more
- 34% of these high spenders allocate 16% or more of their cloud budget to security

SECTION THREE

Measuring Security Preparedness

Keeping your cloud secure depends on a set of cloud security actions

- To determine how secure a company's cloud estate is, we developed a metric called *cloud security preparedness*
- This measure was derived from answers to questions about 19 specific security practices across cloud workloads
    - ◊ Two of the practices span the entire cloud infrastructure
    - ◊ The other 17 practices refer specifically to three types of cloud compute: VMs, containers and PaaS
- We identified three levels of security preparedness among surveyed organizations: low, medium and high
    - ◊ Only 18% of companies are highly prepared to keep their cloud estates secure
    - ◊ 29% of companies fall into the lowest-prepared category

Companies at the highest level of cloud security preparedness are embedding security into their DevOps process and integrating security into the software development lifecycle

- 45% of highly prepared companies have embedded security into DevOps processes, and 41% integrate security in at least four stages of the development lifecycle
- By contrast, 21% of the lowest-prepared companies have embedded security in DevOps, and just 12% involve security in at least four stages of the development lifecycle

As companies improve security preparedness and expand security practices, they recognize that using many security tools can actually hinder cloud security

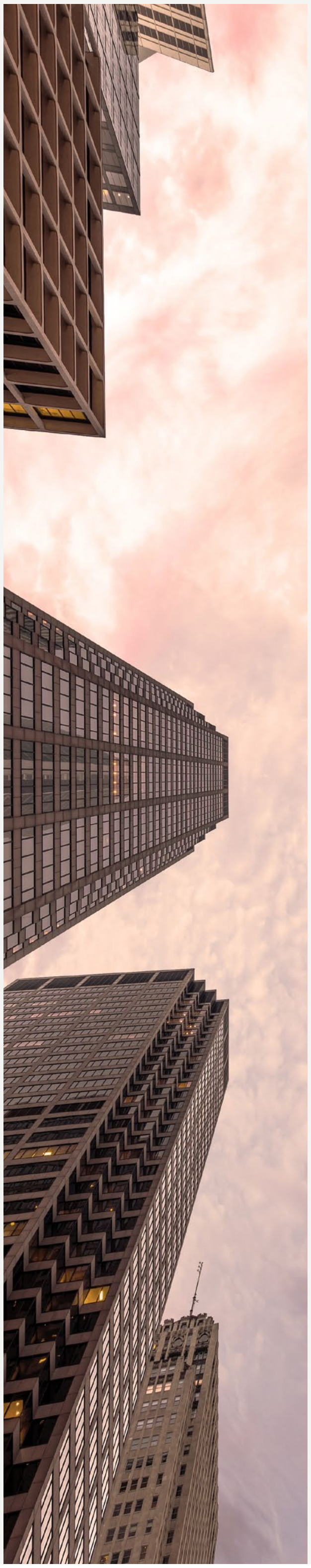
- 52% of employees at highly prepared companies with 11 or more security tools said a high number of tools made it more difficult to prioritize risks and prevent threats
- By contrast, just 16% at low-preparedness companies with 11 or more tools saw multiple tools as a problem

As companies improve their security preparedness, they agree that using a single, comprehensive security solution would improve their security

- For highly prepared companies using 11 or more security tools:
    - ◊ 50% say they're actively reducing the number of tools
    - ◊ 51% agreed that using a single, end-to-end cloud security solution would improve their cloud security posture

SECTION ONE

The State of the Cloud and Cloud Native Adoption



Organizations have moved to cloud over the past couple of decades to meet their need for faster, more flexible computing at a reasonable cost. For these same reasons, cloud adoption is accelerating – and so are the challenges that organizations face when moving workloads to the cloud and expanding their cloud estates.

In our survey of cloud professionals, we set out to discover the following:

- How quickly companies are adopting cloud
- How many cloud platforms they use
- Whether they choose public cloud services, private cloud or both
- Which computing technologies they use in their cloud environments
- How much they spend on cloud and on securing their cloud environments

We also wanted to learn what cloud professionals' biggest challenges are when it comes to cloud adoption and ensuring their cloud environments, applications and data are secure. In other words, what's keeping people up at night?

As you peruse this first section of the report, you'll see we analyzed characteristics of respondents' companies, such as revenue and degree of cloud adoption, against the choices these companies make for their cloud operations. In the second section, The State of Securing the Cloud and Cloud Native Workloads, you'll see our findings on cloud security practices and respondents' concerns around their own organizations' security. In the third section, Measuring Security Preparedness, we'll discuss our findings on security posture and the practices employed by the most highly prepared companies. It's our hope that these insights will provide guidance for safeguarding your data, applications and infrastructure as you adopt cloud technologies and expand your cloud estate.

Cloud adoption is high and growing

Cloud adoption is already high, and it's going to keep on growing. On average, organizations we surveyed currently host 46 percent of their workloads in the cloud, and 95 percent of them expect to grow their cloud use to 64 percent of workloads over the next two years.

By industry

It's no great surprise to see that companies in technology, media and telecom host the greatest proportion of their workloads in the cloud: 53 percent. Energy and resources companies host the lowest percentage of their workloads in the cloud at 42 percent. The other industry groups fall in between.

Across industries, all respondents expect to reach about the same level of cloud hosting two years from now, between 50 and 80 percent. This means the energy and resources sector will grow its cloud use faster than technology, media and telecom companies, which already use cloud for more of their workloads.

By company size

We asked survey respondents about their organizations' annual revenue as a measure of company size. We found that all companies expect, on average, to grow their cloud hosting between 15 and 20 percentage points over the next two years. For companies with less than US $1 billion in annual revenue, that means going from 47 percent of workload in the cloud to 64 percent. Companies over $1 billion, now averaging 45 percent of workloads in the cloud, think they'll grow to 66 percent.

By geography

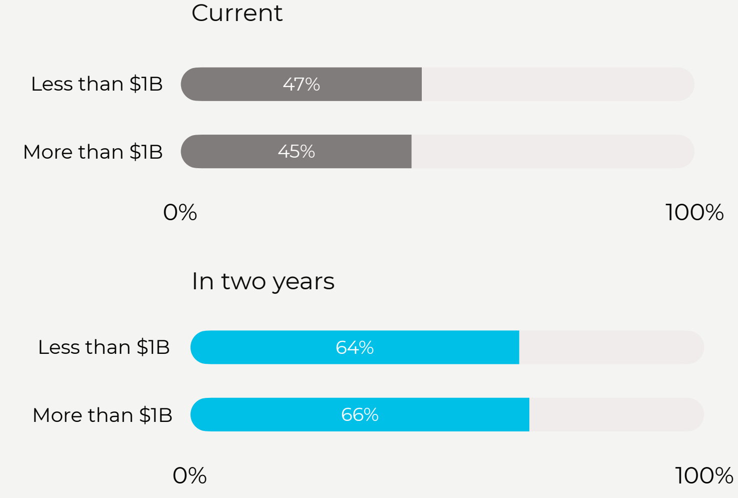
The United States and Germany showed slightly higher levels of cloud hosting than other countries. For U.S. companies, 48 percent of workloads are hosted in the cloud; for German companies, it's 47 percent.

Multicloud is the norm

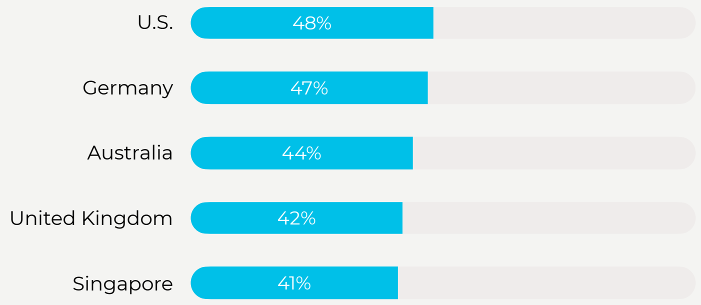
Overwhelmingly, our survey respondents manage multiple cloud environments: 94 percent of all organizations use more than one cloud platform. A majority – 60 percent – use between two and five.

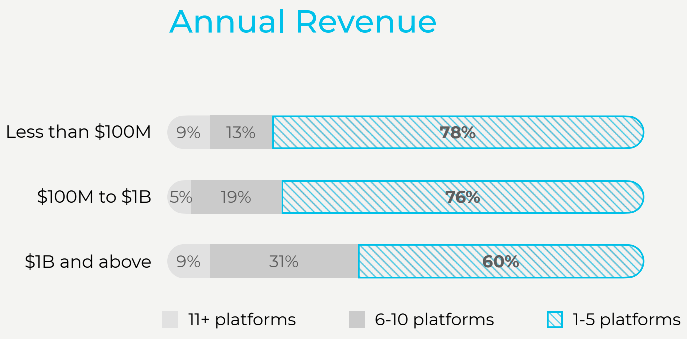
When we look at platform use by company size, those with revenue above US $1 billion tend to use more. For example, 40 percent of the over $1 billion companies use six or more platforms, and just 24 percent of the under $1 billion companies do.

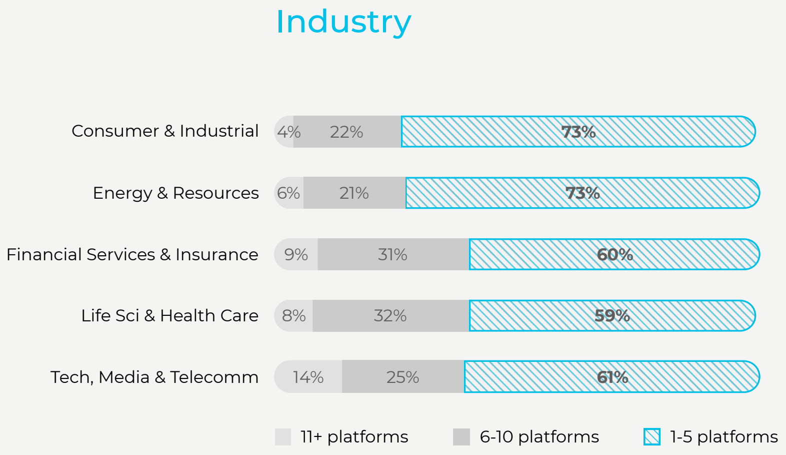
Cloud adoption by company size



Cloud adoption by country







The majority of high adopters – **61 percent** – use just one to five cloud platforms.

When we look at platform usage by industry, we see more platforms used by companies in technology, media and telecom; life sciences and healthcare; and financial services than by those in consumer and industrial products, or energy and resources.

Companies that are high cloud adopters – hosting 55 percent or more of their workloads in the cloud – might be expected to use more cloud platforms. As you can see in the chart on the next page, 13 percent of this group use 11 or more platforms. Among medium cloud adopters, 8 percent use this many, and only 4 percent of the low-adoption group use 11 or more platforms.

What's more striking is that the majority of high adopters – 61 percent – use just one to five cloud platforms. You'll see more interesting examples of this later in the report: Companies with high cloud adoption and big cloud budgets do not always use the most platforms.

Public cloud vs. private cloud: It's a wash

Our survey shows that organizations balance their use of public and private cloud services, with no real bias toward either option. For our full group of 3,000 respondents, 52 percent of cloud workloads are hosted on public cloud servers and 48 percent on private clouds.

Most respondents report that cloud workloads are hosted in a mix of public and private environments. A majority – 57 percent – have a pretty even mix, with 40 to 60 percent of workloads hosted in public cloud environments (and conversely, 60 to 40 percent in private clouds).

For those organizations hosting a majority (more than 55 percent) of their cloud workloads in either public or private environments, public is the more popular choice. Twenty-six percent of our respondents use public cloud services to host the majority of their cloud workloads, while 17 percent use private clouds for the majority of their hosting.

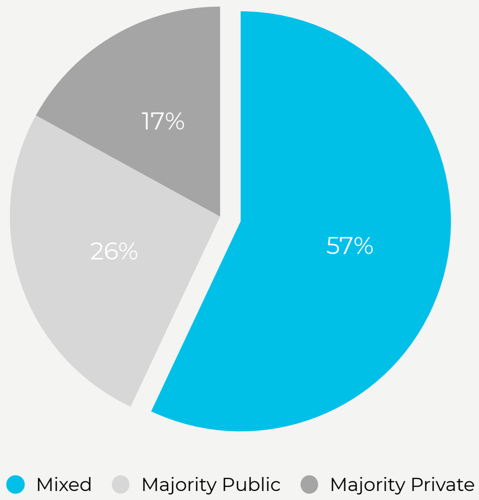
Looking at public and private cloud usage by annual revenue, you can see that, for all groups, mixing public and private cloud is the most popular option. Half of companies with less than $100 million in annual revenue use a mix, as do 45 percent of the largest companies, those with more than $100 million in annual revenue.

It may come as some surprise to note that the largest companies show the highest preference for public cloud. Among those over $100 million in revenue, 36 percent host the majority of their cloud workloads with public services. Just 25 percent of companies with less than $100 million in yearly revenue host the majority of their cloud workloads with public services.

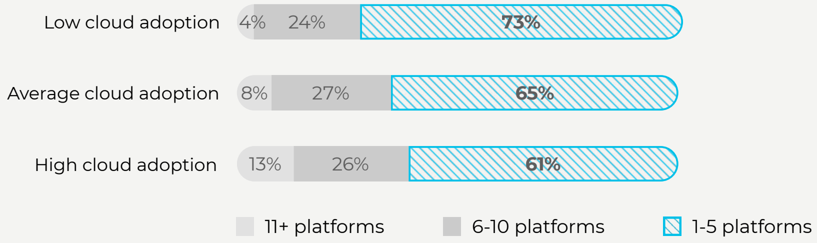
Companies at the highest level of cloud adoption – more than 55 percent of their workloads in the cloud – use private cloud more than companies at lower levels of adoption. A quarter of the high-adoption companies use private cloud for the majority of their workloads.

Companies at the lowest level of cloud adoption – less than 35 percent of their workloads in the cloud – use public cloud services the most. Of this group, 34 percent host the majority of their workloads in public clouds. It's not too surprising, as public hosting is the easiest first step to take when moving workloads to the cloud.

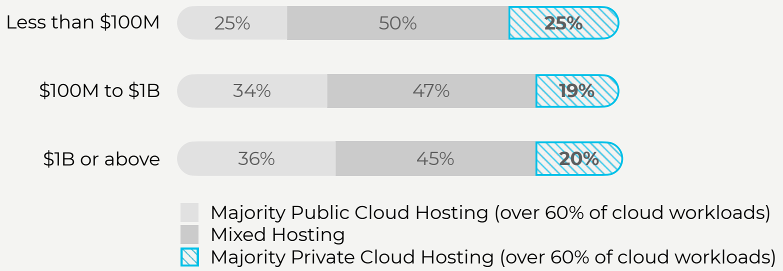
Cloud Hosting Composition



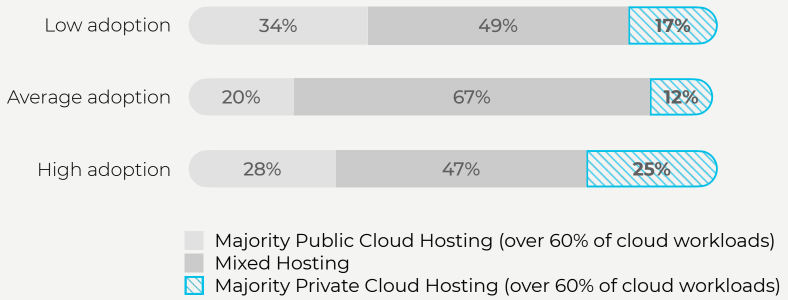
Cloud Usage



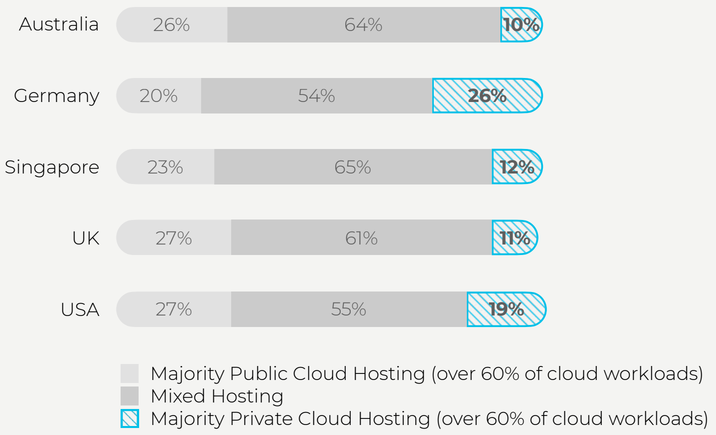
Annual Revenue

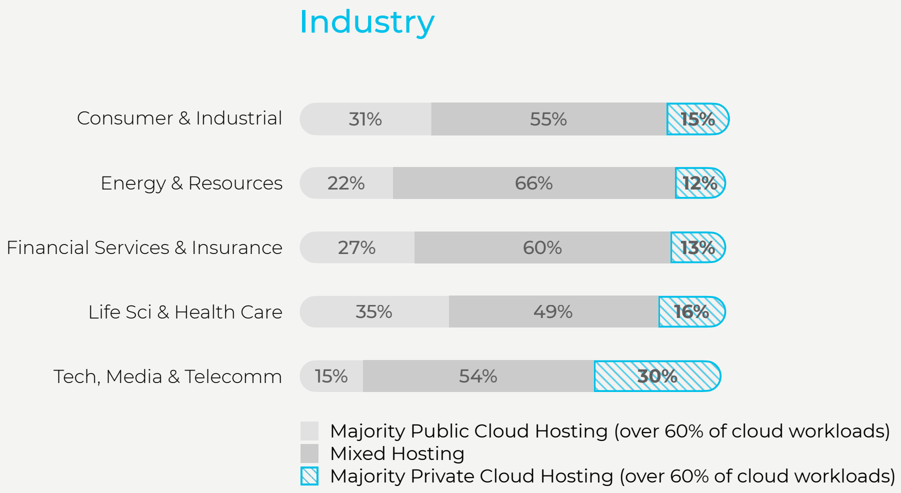


Cloud Adoption



Geography





Take a look at what happens to mixed hosting at low, medium and high levels of adoption, and you'll see an interesting shift. Of companies with a lower percentage of their workloads in the cloud, almost half use a pretty even mix of public and private cloud. Among medium adopters, 67 percent use an even mix of public and private. But then we see the usage of evenly mixed hosting drop back to 47 percent for the high-adoption companies.

You'll see this pattern – trying something out in low adoption, increasing it at the medium adoption level and dropping back at the high adoption level – in other areas of our findings, particularly companies' use of cloud tools and vendors.

Looking at public vs. private hosting by country, Australian respondents reported the least use of private cloud. Just 10 percent of Australians said their companies host 60 percent or more of workloads in private cloud environments.

German companies use private cloud the most: 26 percent host the majority of their workloads there. This may be due to the strength of European regulation around internet privacy – it's possible that German companies feel they can better control cloud security by using platforms they control themselves.

Among our industry groupings, the technology, media and telecom companies tend to use private cloud more than other groups; 30 percent of these companies host the majority of their workloads in private clouds, about double the level in other industries. This may be because tech and telecom companies have a higher level of understanding around internet security and how difficult it is to secure data and infrastructure.

Our survey respondents use seven different public cloud providers, with more in an undefined "other" category. By a wide margin, the top four services are the following:

1. Amazon Web Services
2. Google Cloud Platform
3. Microsoft Azure
4. IBM Cloud Services

Companies use a blend of compute technologies

As companies seek to host more of their workloads in the cloud and begin developing applications specifically to run in the cloud – that is, cloud native applications – they also adopt cloud native technologies. These technologies include abstracted models that are independent of computing hardware, often referred to as computes. Some examples are VMs; containers and container management services; and services such as IaaS, PaaS and containers as a service (CaaS).

These technologies allow product development teams to focus on the applications that provide value to their organizations, leaving to cloud service providers (or private cloud specialists within their companies) the tasks of managing infrastructure and computing resources.

We asked our survey takers about the compute technologies their organizations use. The choices:

- VMs, including hosts and IaaS
- Containers
- CaaS and managed container services such as Kubernetes
- PaaS or serverless, and technologies such as FarGate, Cloud Run or Pivotal Cloud Foundry

Almost all respondents – 93 percent – reported using all four types. Most respondents – 80 percent – balance their compute use fairly evenly, at 15 to 35 percent for each type.

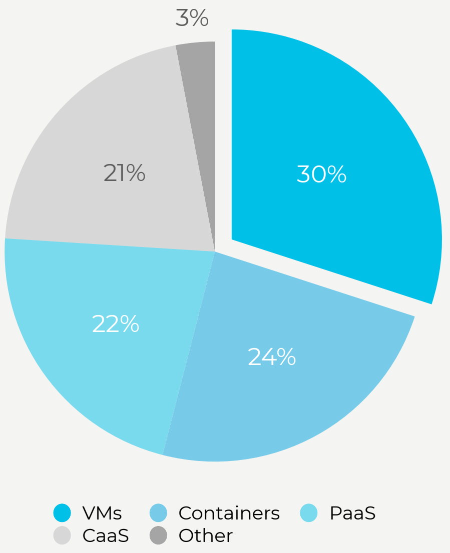
Overall, VMs, at 30 percent, are used more than other computes. Containers are the next most common at 24 percent, then PaaS at 22 percent and CaaS at 21 percent.

Choice of computes remains fairly consistent across such variables as the percentage of cloud hosting a company does, its degree of preference for public or private hosting, industry, annual revenue, and geographic location.

Use of all four computes will grow along with the growth of cloud hosting. Across our survey takers, 86 percent expect their usage to increase or remain stable over the next two years. The expected growth is evenly spread between VMs, containers and CaaS, with a tilt toward VMs for those respondents who expect a significant increase in compute use.

Companies that currently use cloud hosting the least expect their use of all four computes to grow the most over the next two years. The one exception: Companies at an average level of adoption have slightly higher expectations for increasing their use of CaaS.

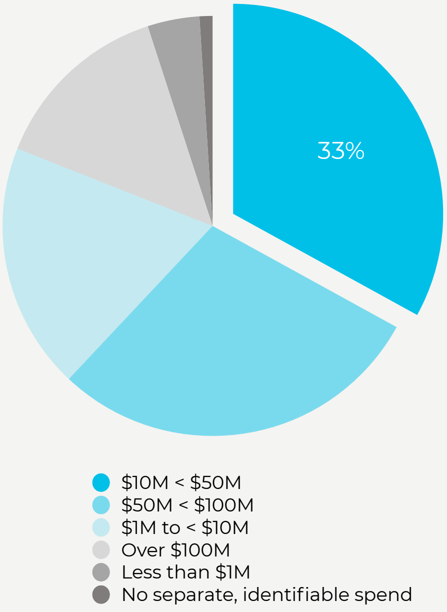
Companies use a blend of compute technologies



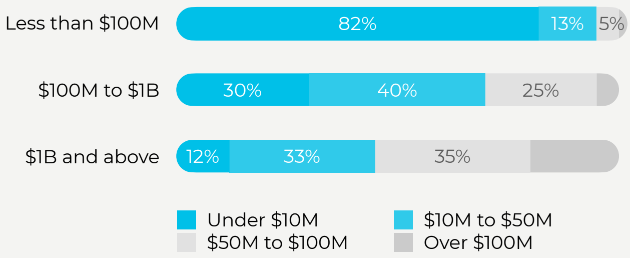
How do you expect your usage of compute options to change over the next 24 months?

	Consumer & Industrial Products	Energy & Resources	Financial Services & Insurance	Life Sciences & Health Care	Tech Media & Telecomm
VMs (e.g. Hosts, IaaS)	35%	42%	30%	39%	27%
Containers	31%	36%	25%	32%	16%
CaaS (e.g. Kubernetes)	30%	34%	27%	30%	20%
On demand containers, PaaS or serverless	33%	35%	29%	29%	28%

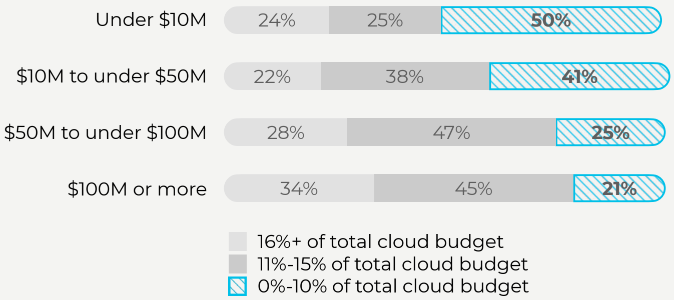
How much did your organization invest in cloud platforms (including CSPs, databases and containers platforms)



Annual Revenue



Cloud Spend



While companies in all industry groups expect to grow their use of the four computes over the next two years, companies in the tech, media and telecom group expect a higher degree of growth in VMs and PaaS than other companies, at the expense of containers and CaaS.

How much companies invest in cloud

More than half of the organizations we surveyed (56 percent) spent less than $50 million on their cloud platforms last year.

As you might expect, companies with higher revenue spend more on cloud. Among companies with more than $1 billion in annual revenue, 55 percent spent more than $50 million on cloud platforms last year. Of companies with $100 million to $1 billion in annual revenue, 30 percent spent that much.

It would be logical to expect that companies spending more on cloud hosting and technology also spend more on cloud security tools. That’s true, but we also observed that as cloud budgets increase, the proportion of spend on cloud security increases.

For example, among companies that spent more than $100 million on cloud in 2019, 79 percent dedicated more than 10 percent of that budget to cloud security. In this same group, 34 percent dedicated 16 percent or more of the cloud budget to security.

At the lowest end of the cloud budget scale, companies spending less than $10 million per year allocated a smaller proportion of their budgets to cloud security – just 49 percent dedicated more than 10 percent to security. And 24 percent allocated 16 percent or more of their cloud budget to security – 10 percentage points lower than those with the highest cloud budgets. See the chart below for a complete reckoning of cloud security spend among companies with different annual cloud budget ranges.

Perhaps the most interesting finding around cloud spending is that more investment does not necessarily correspond to using more cloud platforms. When you first glance at the chart below, it does look that way: Among companies that spent less than $10 million on cloud last year, 21 percent were using six or more cloud platforms. And at a spend of $10 million to $50 million, use of six or more platforms jumps to 40 percent.

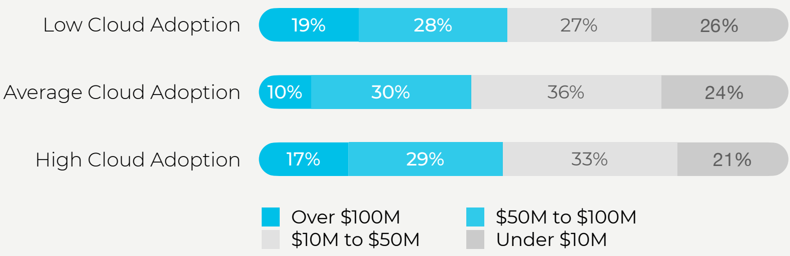
Among companies spending more than $50 million on cloud platforms though, the proportion using six or more platforms falls to 36 percent. It seems that while a smaller budget limits cloud spend, once the budget gets big enough, people see fewer reasons to add more platforms.

Note also that among companies with a cloud platform budget over $50 million, almost two-thirds (64 percent) are using five or fewer cloud platforms.

Number of cloud platforms by cloud expenditure

	Cloud Expenditure			
	Less than $10M	$10 to $50M	Over $50M	Total
1 to 5 platforms	80%	61%	64%	67%
6 to 10 platforms	16%	32%	25%	25%
11+ platforms	5%	8%	11%	8%
Total	100%	100%	100%	100%

Cloud Adoption



Another interesting, almost paradoxical observation: Higher adoption of cloud does not correspond to a higher level of cloud investment. Among the highest adopters of cloud hosting, just 17 percent invested more than $100 million in cloud in 2019. Even more interesting, these high spenders are 19 percent of the lowest-adoption group.

Challenges to cloud adoption

Businesses have been moving to the cloud over the past decade to gain advantages that only the cloud can deliver: greater flexibility for companies with growing or fluctuating computing needs, more flexibility for remote work, a better framework for disaster recovery, and a big reduction in capital expenditure.

With all that to gain, you'd think cloud adoption would be growing even faster than it is. So we set out to discover the challenges people are dealing with in moving workloads to the cloud.

Our survey respondents say the top challenges are the following:

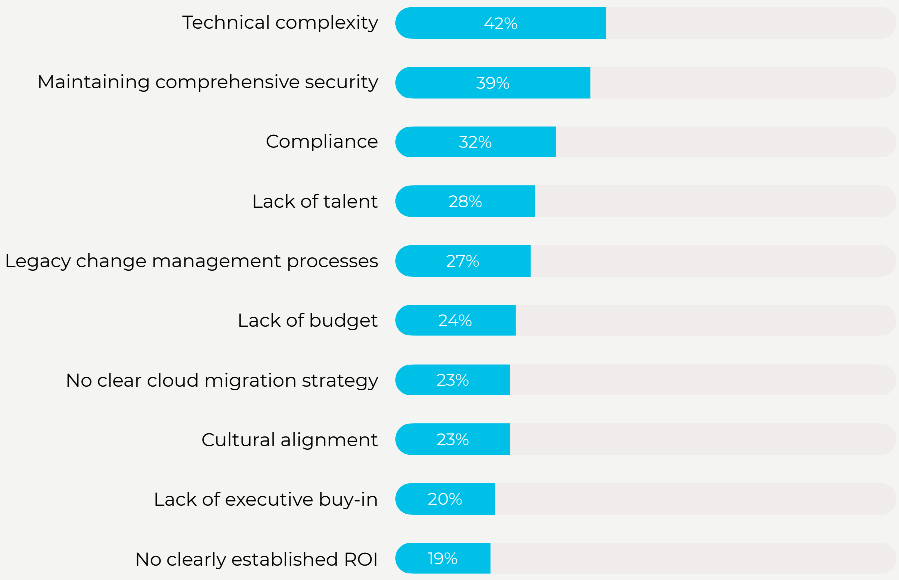
- Technical complexity
- Maintaining comprehensive security
- Compliance

Perhaps surprisingly, the ranking of these challenges remains consistent across all the variables we considered in our analysis: how many cloud platforms an organization uses, majority public or private cloud use, annual revenue, number of vendors used, degree of cloud adoption, and how much an organization invests in its cloud estate.

We did find that how much a company spends on cloud affects how intensely people experience the challenges. Survey respondents at companies spending more on the cloud feel the intensity of the top challenges less. This is particularly true for technical complexity and maintaining comprehensive security.

In the next section, we'll look at what our respondents told us about how their organizations handle cloud security, including how many security tools and security vendors they use, how large their security teams are and how they're organized, and how much of their cloud budget is invested in security.

Challenges in Moving to the Cloud



SECTION TWO

The State of Securing the Cloud and Cloud Native Workloads

The speed and flexibility that are so desirable in today's business world have led companies to adopt cloud technologies that require not just more security but new security approaches. In the cloud, you can have hundreds or even thousands of instances of an application, presenting exponentially greater opportunities for attack and data theft.

Public cloud service providers have done a great job of taking on the build, maintenance and updating of computing hardware, and providing VMs, data storage and databases to their customers, along with the baseline security to protect it all. But it's still up to you, the customer, to provide security for the data, hosts, containers and serverless instances in your rented or privately owned cloud. You also need to protect your networks, resource configurations, user data and credentials.

With so much at stake, organizations are hiring to expand their cloud security teams, buying more software tools and engaging with more cloud vendors. All these efforts – and all this money – aren't making cloud security folks feel particularly comfortable though. The sheer number of threats to cloud workloads is still keeping them up at night.

Cloud security is an ever-moving goalpost

Cloud is perpetually evolving, forcing teams to continually investigate, learn and apply new architectures and technologies that let them move as quickly as the business demands. In this environment of relentless change and persistent threat, security professionals struggle to keep their companies' cloud estates secure. Four out of five of our survey respondents told us their company's infrastructure is constantly evolving. And three-quarters of our survey respondents said that cloud security tools and solutions are outpaced by threats to their cloud systems.

These sentiments are driving companies to direct a greater proportion of their cloud budgets to security as their cloud investment grows. While you might think that companies with bigger cloud budgets would spend the same or a smaller proportion on cloud security, in fact, a bigger portion of the annual cloud budget goes to security. Cloud security spend is highest for the companies with over $100 million in revenue: 34 percent of them allocate 16 percent or more of their cloud budget to security. And 79 percent of these high spenders allocate over 10 percent of their cloud spend to security.

The threats and challenges to cloud security

We asked our survey respondents to identify the top three threats to their cloud security out of 10 possibilities. The gap between the top two threats – data exposure and malware – and those least identified as the top threat was narrow, around 5 percentage points.

These threat rankings were consistent across different characteristics relating to cloud security: the number of cloud vendors companies engage with, how many cloud security tools they use, the size of their cloud security team and how much they invest in cloud security. Threat rankings were also consistent across how much cloud hosting companies do, how much they spend on cloud and the number of cloud platforms they use.

The most intense threats to cloud security, as perceived by our survey respondents, are external, and all of them apart from "insider threats" are technical. But the greatest challenges respondents say they face arise from company culture: the organization's priorities and its common practices.

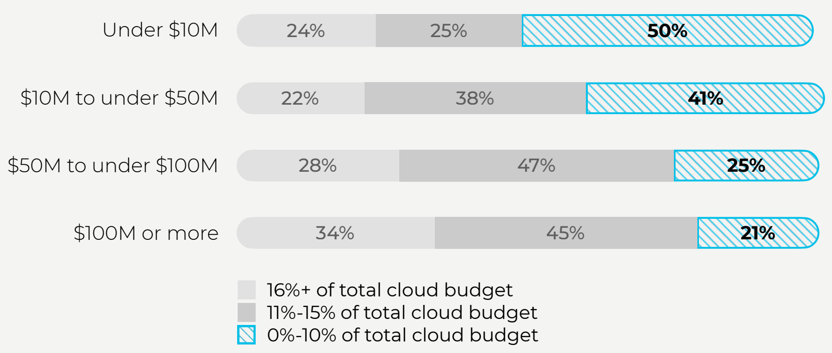
3/4

of our survey respondents said that cloud security tools and solutions are outpaced by threats to their cloud systems

4 out of 5

of our survey respondents told us their company's infrastructure is constantly evolving

Cloud Spend



What is your number 1 threat to cloud security?

Data exposure	13.2%
Malware	12.8%
Application vulnerabilities	10.9%
Weak and broken authentication	10.0%
Insider threats	9.7%
Credential leakage	9.1%
Insecure APIs	9%
Infrastructure misconfigurations	9%
Application misconfigurations	8.7%
Overprovisioned access	7.7%

Greatest challenge to providing comprehensive cloud security.

1	Lack of visibility	15%
2	Tool training	14%
3	Safe practice training	11%
4	Evaluating current state	11%
5	Integration of security tools	10%
6	Securing budget	10%
7	Security reporting tools	8%
8	Automation	6%
9	Executive buy-in	4%
10	Other	1%

Top organizational priorities for securing cloud native applications

Data protection	15.4%
Application security	11%
Network anomaly detection	8.5%
Vulnerability management	8.4%
Runtime security	8.3%
Compliance and governance	8%
User behavior analytics	7.3%
Asset inventory	7.0%
Machine identity	6.8%
IAM governance	6.6%
Network microsegmentation	6.5%
Incident response management	6.3%

Four items were most frequently chosen as the top challenges to cloud security from a list of 11 options:

- Lack of visibility of security vulnerabilities – 15 percent
- Employee training on security tools – 14 percent
- Employee training on safe practices – 11 percent
- Evaluating the current state of security – 11 percent

We know what our respondents see as their own and their organizations' top threats and challenges. Now let's look at what respondents say are their organizations' top three priorities for securing cloud native applications.

Out of 12 options presented in the survey, two priorities emerged as most important: data protection, at 15 percent, and application security, at 11 percent.

We discovered an additional issue that can certainly have an impact on cloud security: 73 percent of respondents say their organization struggles to clearly delineate between their own responsibility for cloud security and their CSP's responsibility for security.

The CSP is certainly responsible for securing the hardware, software and data that support and enable the cloud service, and the customer is certainly responsible for configuring resources properly, protecting applications and securing their own data. However, with CSPs offering different levels of services, it can be unclear to the customer exactly where the CSP's security responsibility ends and the customer's begins.

Investing in cloud security

With multiple threats and challenges to the security of their cloud-hosted applications and data, we asked how much companies are investing in cloud security. Almost two-thirds of surveyed organizations invested more than 10 percent of their 2019 cloud budget in securing their cloud estates.

How are companies employing their cloud budgets to deal with the wide range of threats and address their security priorities? They're buying tools, signing up for services and hiring people.

More than three-quarters of surveyed companies – 77 percent – have more than 20 people working on their cloud security teams.

Well over half of companies are engaged with more than five security vendors (58 percent) and more than five security tools (57 percent). This means most companies are buying just one security tool per vendor.

We asked about three types of security tools: those provided by cloud service providers, tools from third-party vendors and open source tools. Three-quarters of our respondents use more than one type.

65%

of survey organization's invested more than 10% of their 2019 cloud budget in securing their cloud estates.

58%

use 6 or more cloud security vendors.

57%

use 6 or more cloud security tools.

77%

of companies have cloud security teams bigger than 20 people.

While 65 percent of surveyed companies use security tools provided by their CSP, 71 percent use tools provided by third-party vendors. Use of open source tools is slightly lower than CSP tools at 62 percent.

Security team structure

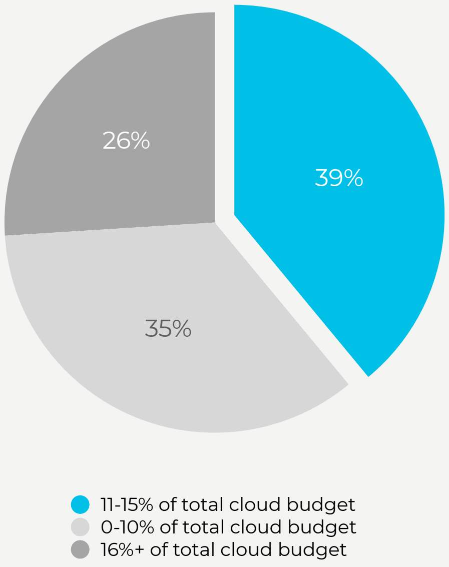
Companies vary in how they approach cloud security team structure. Two models are common: a centralized cloud security team that supports delivery teams as needed and a cross-functional structure wherein security experts are embedded with development and infrastructure teams.

Nearly half the companies our survey respondents work for mix these two models: They have a centralized cloud security team as well as security experts working within delivery teams. Less than a third employ the fully centralized model, and just 22 percent use the fully cross-functional model.

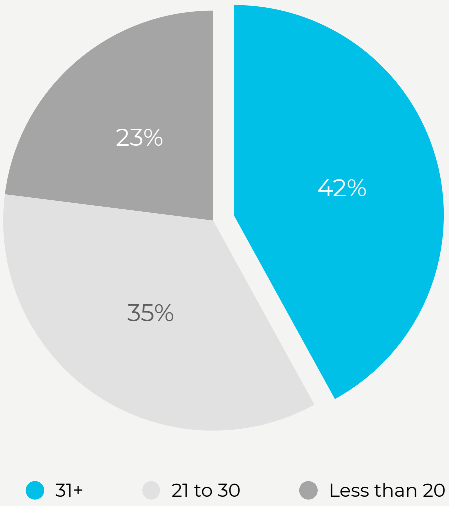
Security tools and vendors: More does not always equal better

As companies increase their cloud spend, they tend to acquire more cloud security tools and engage with more cloud security vendors. However, an interesting pattern has emerged from our data, where we see that companies investing more than $100 million in cloud reduce the number of vendors and tools they use.

Total Cloud Budget

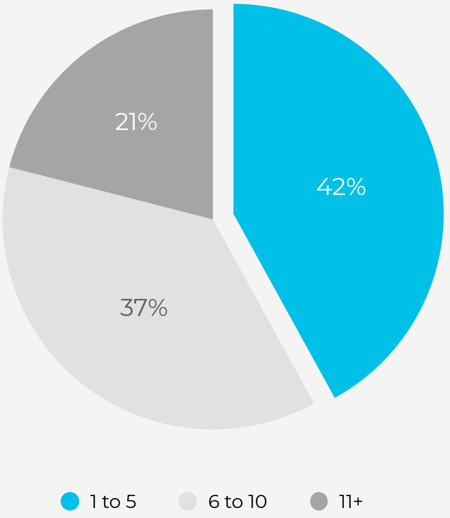


Cloud Security Team Size

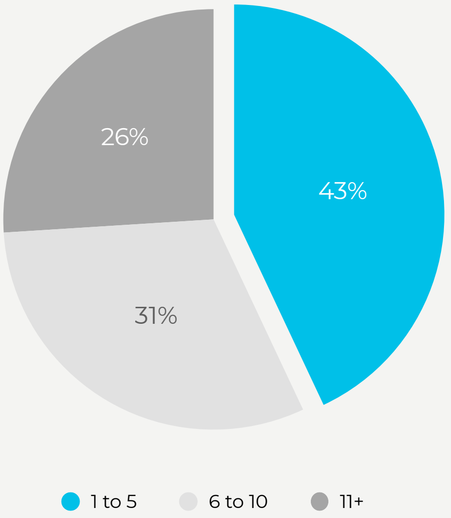


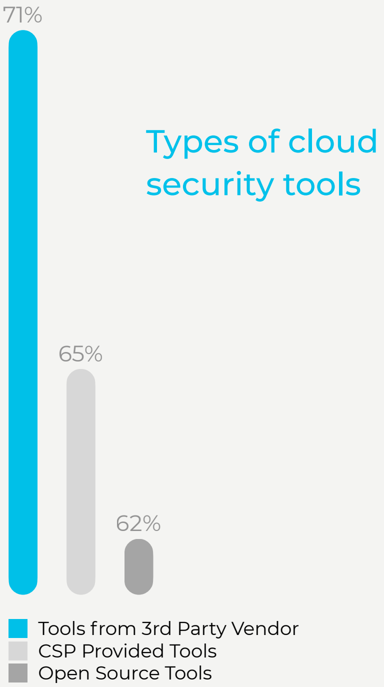
75 percent of companies use more than one type of cloud security tool, and third-party tools are more popular than either open source or CSP tools.

Number of cloud security vendors

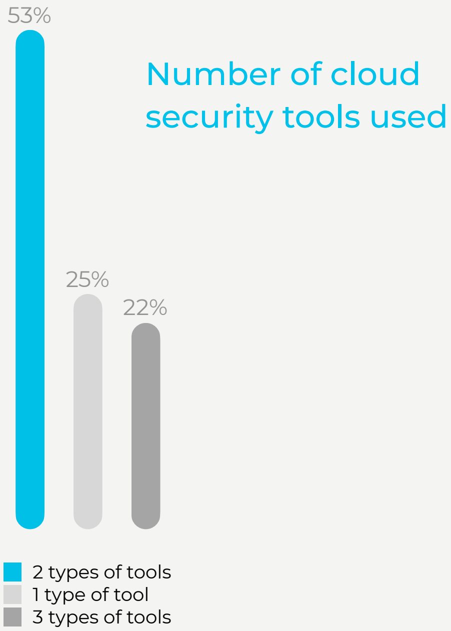


Number of cloud tools



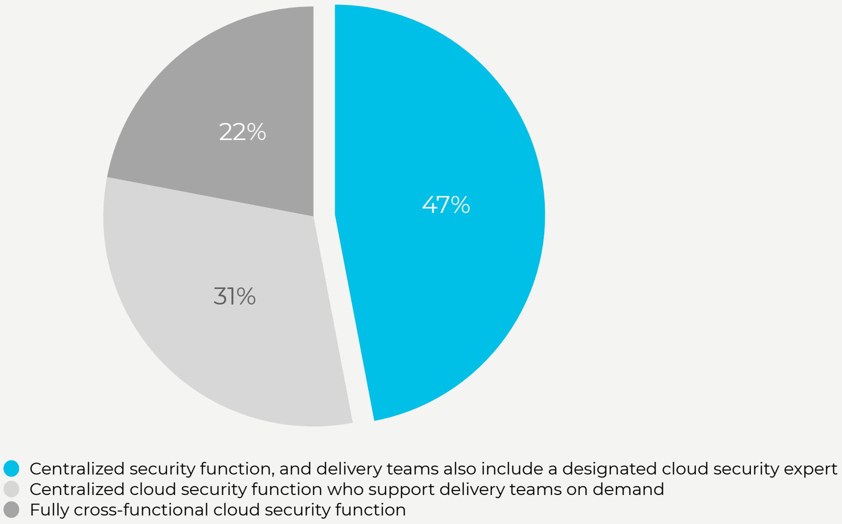


Types of cloud security tools

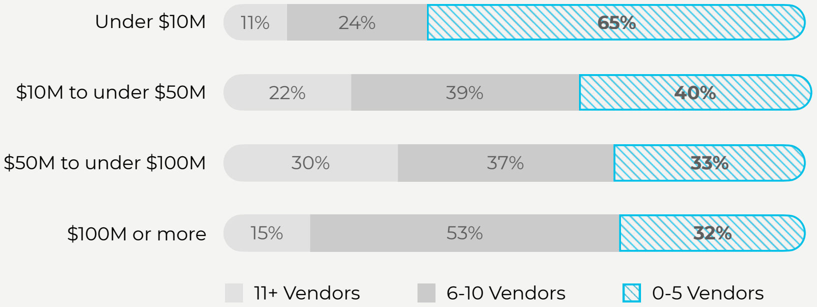


Number of cloud security tools used

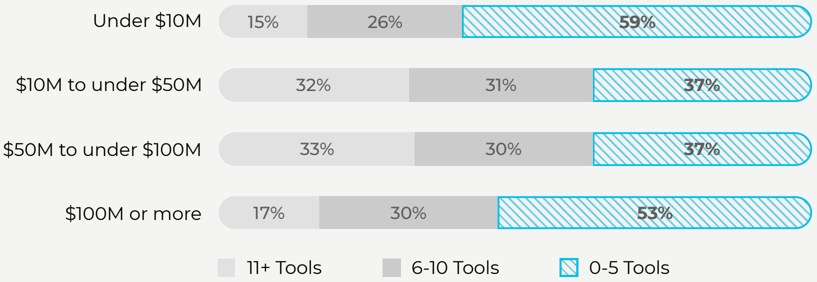
Organization of Cloud Security



Security vendor engagement by cloud investment



Tool usage by cloud investment



For example, two-thirds of companies investing less than $10 million in cloud security used five or fewer security vendors. And just 11 percent of these companies used 11 or more vendors. This seems natural for a company with a smaller budget.

As cloud investment bumps up toward $50 million and then $100 million, we see companies using more vendors. Among companies in the $50-million-to-$100-million group, 30 percent use 11 or more cloud security vendors.

Though we might expect another increase in security vendors for companies investing more than $100 million in cloud, we actually see fewer using 11 or more vendors – just 15 percent. The majority of these high spenders – 53 percent – use 6 to 10 security vendors.

This same pattern can be seen for the number of security tools used, with slightly different percentages. The main difference here is that, among companies investing more than $100 million per year in cloud, most – 53 percent – are using five or fewer security tools. Interestingly, that's the same proportion of the high spenders that use 6 to 10 security vendors.

We believe that as companies go through stages of cloud adoption and development, they identify new threats to their cloud security, so they acquire more tools and engage more vendors. But at a certain point, there are just too many tools and vendors.

Training employees on security tools is one of the top challenges to providing comprehensive cloud security, as seen above. In fact, as companies achieve a higher level of security preparedness (discussed in the subsection below), the top challenge to cloud security becomes training employees on tools, so rationalizing the use of fewer tools makes sense. As teams gain more experience, they can identify overlaps between tools and vendor offerings and judge which ones best answer their particular needs.

In the next section, we'll look at the practices companies engage in to secure their cloud estates. We'll also discuss how we evaluated which companies are doing a better job with cloud security and identify the things that the most secure companies have in common.

SECTION THREE

Measuring Security Preparedness

We asked respondents to rate their organization's overall security posture for cloud workloads. Eighty-four percent said their organization's cloud security posture was "strong" or "very strong." Given how many concerns respondents shared, this seemed odd and contradictory. So we dug into our survey results to see if we could uncover a more nuanced picture of people's feelings and perceptions around cloud security.

A new measurement framework: Security preparedness

To understand how well any given company is guarding its cloud infrastructure, applications and data, we asked about 19 specific security actions. Seventeen of these actions are at the compute level, and two span the entire cloud infrastructure.

Cloud security actions

Organizational practices

- Automating security processes for cloud workloads
- Actively integrating security into the development lifecycle

For workloads on PaaS and serverless

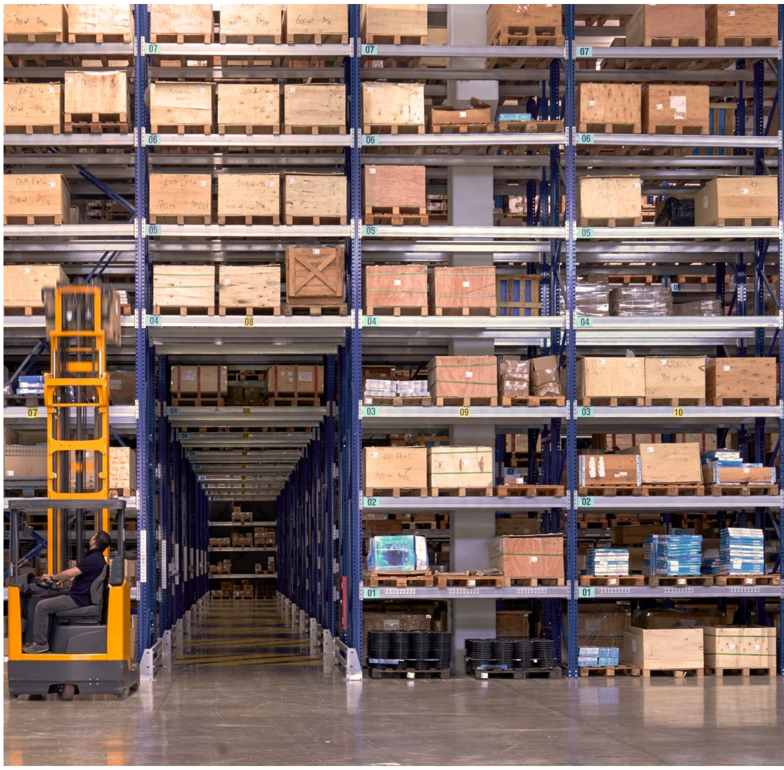
- Runtime protection from unauthorized access
- Vulnerability scanning/management
- Automatic configuration of security policies for hardening systems
- Network protection

For workloads on containers, CaaS and managed Kubernetes

- Integration of CI/CD scanning
- Hardening and compliance checks
- Runtime protection
- Container-to-container microsegmentation
- Access controls, incident response and forensic analysis

For workloads on VMs, hosts and IaaS

- Automated auditing and monitoring of configurations
- Identity access management tools
- Data protection
- Automated vulnerability management
- File integrity monitoring
- Microsegmentation to secure priority systems
- Automated vulnerability scanning of third-party platforms
- Automated compliance modeling



From the answers about security actions, we developed a measure for *security preparedness* or how ready a company is to address threats to its cloud workloads. We calculated separate scores for security actions at the compute level and for actions at the organizational level. Compute-level scores accounted for 75 percent of the total security preparedness score, and organization-level actions contributed 25 percent.

To score a company as low, medium or highly prepared, we considered both how many practices it uses and how deeply these practices have been implemented across its cloud workloads.

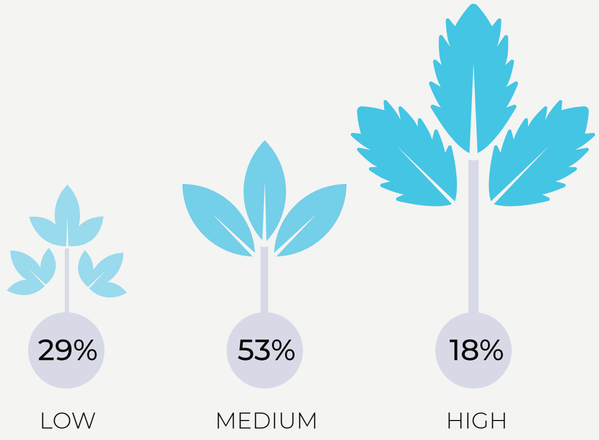
We identified three levels of security preparedness among the surveyed organizations: low, medium and high.

- **LOW PREPAREDNESS.** These companies are taking few security actions across a small proportion of their cloud workloads.
- **MEDIUM PREPAREDNESS.** These companies are taking more security actions across more of their workloads than the low group, but they lag behind the leaders in the high group.
- **HIGH PREPAREDNESS.** These companies are taking the most security actions and across a high proportion of their cloud workloads.

The majority of our respondents – 53 percent – are in the medium group. Just 18 percent are in the high group, which

Just **18 percent** of surveyed companies are at a high level of security preparedness.

Cloud security preparedness



shows how rare it is for companies to do all they should to secure their cloud applications, data and infrastructure. Nearly a third are in the lowest-prepared group.

In addition to asking about specific security tools and practices, we also asked survey respondents how effective they feel these tools and practices are for protecting their company's cloud workloads. Their answers gave us a good proxy for the strength of each organization's cloud security posture, since we had no way to directly evaluate that.

We combined our analysis of security preparedness with our evaluation of security posture. This allowed us to understand which practices and tools are used by companies at each level of security preparedness and to what degree.

While we evaluated responses from the low, medium and high groups, we are most interested in what the high-preparedness group does. Their practice patterns are the ones that other companies should consider when looking to improve their own cloud security.

Practices common to organizations with high preparedness levels

Here are our observations of the practices common to organizations at the highest level of security preparedness.

As companies improve and expand their security practices, they do a better job of embedding security into their DevOps process and build more security touchpoints into the software development lifecycle.

Our survey results show that companies at a low level of security preparedness struggle with both embedding security into DevOps and introducing security touchpoints into the development lifecycle. Just 21 percent have been able to embed security in DevOps, and an even lower number – 12 percent – involve security in at least four stages of the development lifecycle.

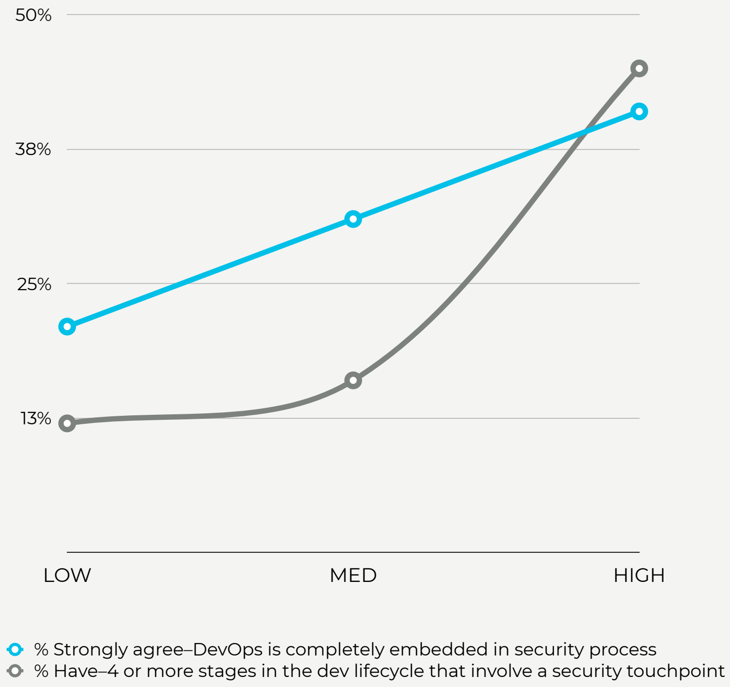
Things improve at the middle level of security preparedness. At this stage, 31 percent of companies embed security in DevOps. But only 16 percent have been able to add security touchpoints to at least four stages of the development lifecycle.

There's a big jump in security integration for companies at the highest level of security preparedness. At this level, 45 percent of companies have embedded security into DevOps processes, and 41 percent integrate security in at least four stages of the development lifecycle.

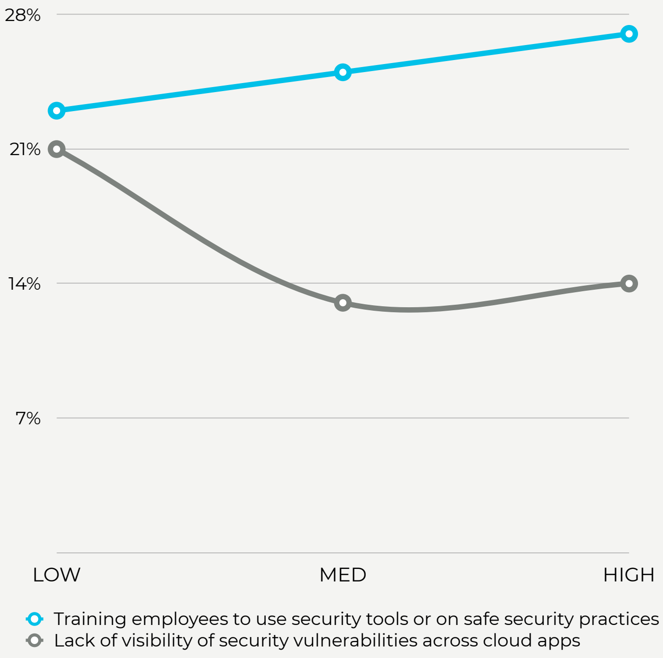
As companies increase their level of security preparedness, training employees on security emerges as the biggest challenge.

As we discussed above, the top two challenges to providing comprehensive security are lack of visibility of security vulnerabilities across cloud applications, and training employees on security tools and safe practices.

Security Integration into DevOps and the development lifecycle



Training and Visibility are the top two challenges in providing comprehensive cloud security



These two challenges are most acutely felt by people whose companies are at the lowest level of security preparedness. In this group, lack of visibility is a top concern for 21 percent of respondents, and training is the focus for 23 percent.

But as companies employ more security practices and become better prepared to meet security threats, concern about visibility declines and training emerges as the top challenge. For people at highly prepared companies, training is reported as a top challenge by 27 percent of respondents – twice as often as visibility.

As companies improve security preparedness and expand security practices, they recognize that using many security tools can actually hinder cloud security.

We asked survey takers whether the number of security tools or vendors they use detracts from their ability to prioritize risk and prevent threats. We were most struck by the results from organizations that use 11 or more tools and those using 11 or more vendors.

Among respondents from companies at the highest level of security preparedness, about half said that the high number of tools in use does make it harder to prioritize risks and prevent threats. By contrast, only about 15 percent of those in the least-prepared group felt that way.

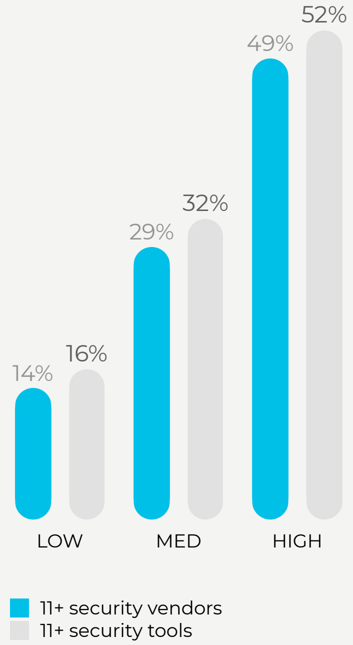
We conclude that using too many tools not only doesn't help cloud security – it can actually make things worse.

As companies increase their security actions and preparedness, they reduce the number of security tools they're using and say that a single, comprehensive cloud native security solution would improve their security.

As we've noted above, within organizations at the highest level of security practice and preparedness, a majority of survey respondents feel that using too many tools makes it harder to ensure their cloud systems are secure.

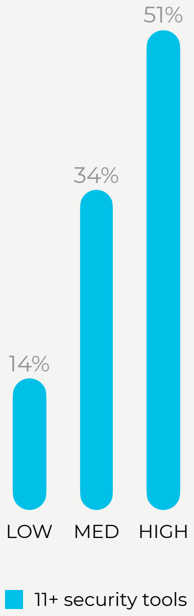
These feelings were especially acute for respondents in high-preparedness companies using 11 or more security tools. Within this group, 50 percent said they were reducing the number of cloud security tools, and 51 percent felt a single, comprehensive solution would improve their security posture.

By contrast, just 15 percent of respondents in the low-preparedness group (using 11 or more tools) said their organizations are reducing the number of security tools they use. Only 14 percent believe a single, comprehensive cloud security solution would help them improve their security posture.

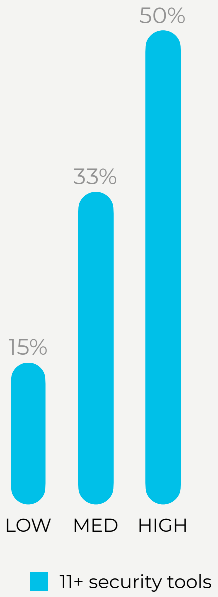


I believe the number of point solutions that we use to secure our cloud-native workloads creates blind spots that detract from our ability to prioritize risk and prevent threat

I believe a single, end-to-end comprehensive solution to cloud native security would improve our security posture across the cloud and compute options



My organization is actively reducing the number of security solutions that we can use across our cloud-native workloads



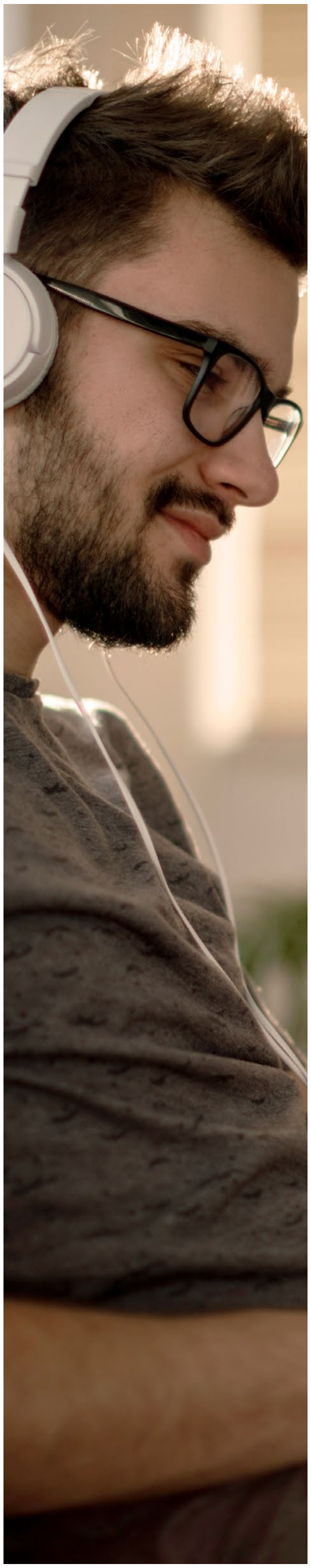
You’ve reached the end of our first annual **The State of Cloud Native Security Report**.

We hope you’ve learned something valuable from these findings and recommendations, and that you now feel you can take a refreshed look at your organization’s cloud security – and improve it.

We would love to have your feedback on this report. Since we plan to repeat it next year, and into the future, we want to make it relevant and valuable. Let us know what you’d like us to investigate next time – what we left out this time around that you would have liked to know, which issues are going to be important for you in the near future and anything else you think will help us help you more.

Tell us what you think: CNSsurveyfeedback@paloaltonetworks.com

Who Took the Survey



For our inaugural State of Cloud Native Security survey, we collected perspectives from a group of carefully selected IT professionals working with infrastructure, applications and security in the cloud. Our respondents live in five countries and work in five different industries in a variety of jobs and teams in companies of different sizes.

We were delighted to get completed surveys from 3,000 people. Thanks to all who participated!

Location

Half our respondents were in the United States, with the rest split evenly between Germany, the United Kingdom, Singapore and Australia. We purposely focused on North America and Europe based on data from the Cloud Native Computing Foundation 2020 survey, The State of Cloud Native Development, which found that out of 4.7 million cloud native developers around the globe, the largest percentage reside in North America and Europe. However, we chose to add two important Asia Pacific countries because this region is a significant and fast-growing contributor to the global economy, and cloud use is growing there, too. We felt it would be interesting to uncover any similarities to and differences from our North American and European respondents.

Industry

Almost three-quarters of our respondents were fairly evenly spread between three industry categories. These are financial services and insurance, consumer and industrial products, and energy and resources. The remainder of our respondents work in either technology, media and telecommunications or life sciences and healthcare.

Annual revenue

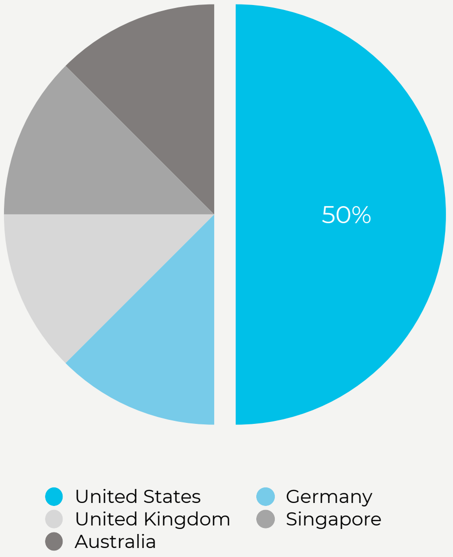
Nearly two-thirds of our respondents work for companies with annual revenue above US $1 billion. Of this group, the vast majority are at organizations with revenue between $1 billion and $5 billion. Just over a quarter of our respondents work at companies with revenue between $100 million and $1 billion.

The dominance of larger companies in our responses isn't surprising, as larger companies have bigger workloads, hence more reason to make use of the efficiencies cloud services can provide.

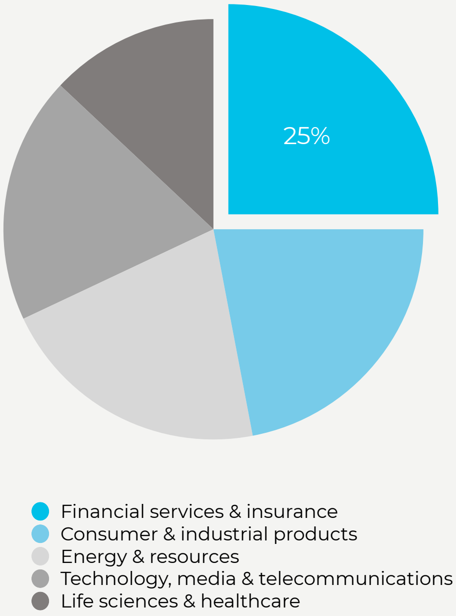
Knowledge of cloud use and cloud security

Two-thirds of our respondents felt they were "very knowledgeable" about their company's cloud operations and cloud security, while one-third said they were "somewhat knowledgeable." We were careful to screen out respondents who had little to no knowledge of their organization's cloud use.

Survey respondents' home country

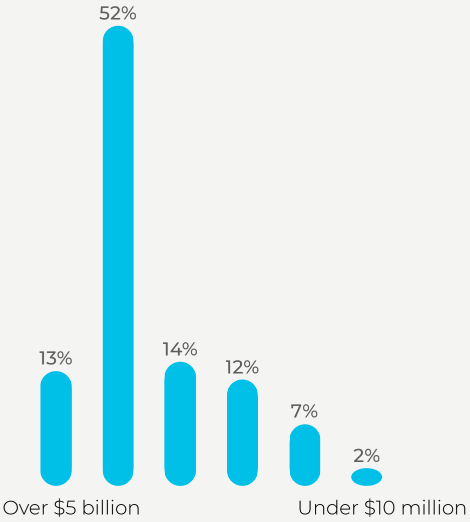


Survey respondents' industry groups

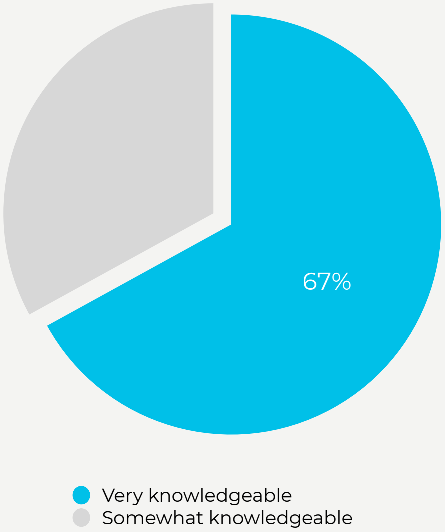


Revenue of survey respondents' organization

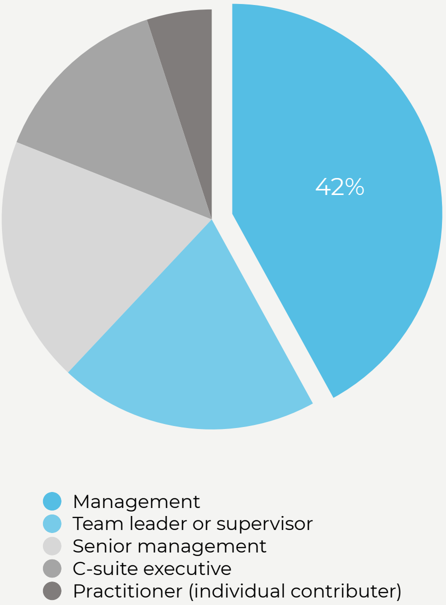
All revenue expressed in U.S. dollars



Survey respondents' knowledge of their company's cloud operations and security



Survey respondents' position in hierarchy



Position in organizational hierarchy

Almost two-thirds of our respondents work in senior and middle management, with more than 40 percent of respondents working in middle management.

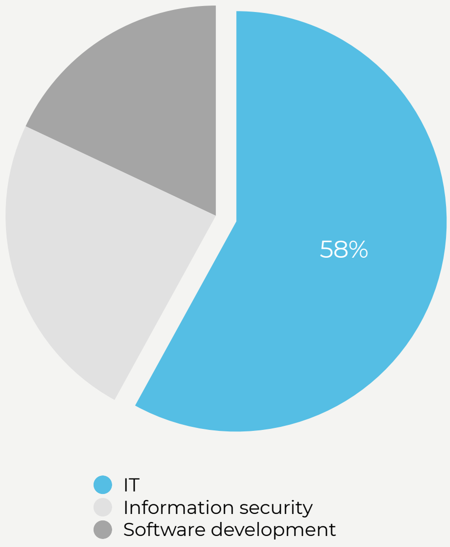
We were glad to see so many people in this type of role respond to the survey. Standing between top management and hands-on practitioners, managers should have a good understanding of both how security is integrated into infrastructure or development and the company's overall strategy and business goals, including the strategic employment of cloud technology.

Departments and teams

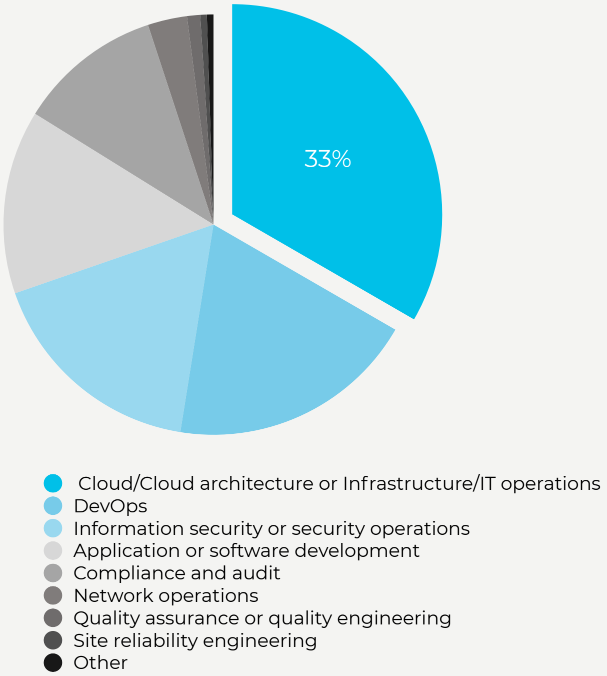
Our survey included only people working in departments and teams that directly deal with cloud infrastructure and security. You'll notice that there's not a direct mapping between departments and teams; this may be because organizations make different choices about which department a given team belongs in.

For example, 24 percent of our respondents work in information security departments, yet 17 percent work in teams respondents identify as "information security or security operations," and 11 percent work in teams they identify as "compliance and audit."

Survey respondents’ departments



Survey respondents’ teams

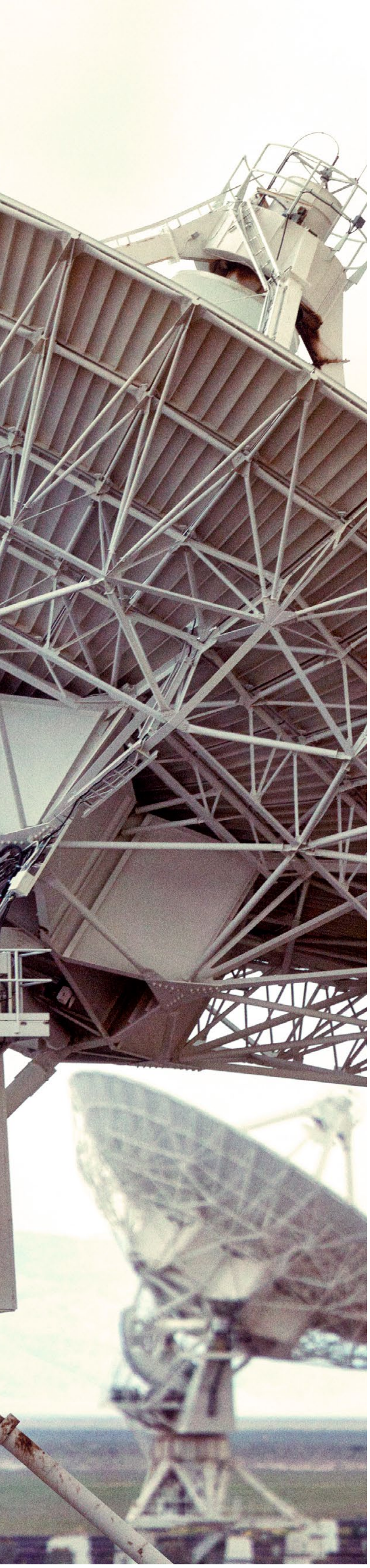


We noticed that nearly 60 percent of respondents are in IT departments, while just 24 percent work in information security departments.

For teams, the single largest bucket was cloud/cloud architecture or infrastructure/IT operations at 33 percent. DevOps came in next at 19 percent, just ahead of information security/security operations at 17 percent.

For the past couple of years, the Puppet State of DevOps Report has found that successful DevOps teams do a good job of integrating security into the software development process. This may explain why we had good representation from DevOps teams; people working in them often have a good understanding of security and its role in IT and software development.

Methodology



RESEARCH SCOPE

Survey questions covered the following topics:

- Overall risk assessment of the organization's cloud estate
- Degree of cloud adoption
- Level of investment in cloud platforms and cloud security
- Tools, technologies and platforms used for cloud computing and for cloud security
- Cloud security implementation at the compute level
- Greatest challenges and threats to providing comprehensive cloud security
- The organization's most important priorities for securing cloud native applications
- Attitudes toward cloud security practices
- Assessment of the organization's approach to cloud security
- Respondent's confidence in various aspects of their organization's cloud security

We used a number of statistical techniques, including Shapley regression, linear regression, correlation, factor analysis and cross-tabulations to understand the relationships between different aspects of cloud use: level adoption, technology, organizational behavior and attitudes toward security. We examined quite a few pairings, including the following:

- **Differences in organizational behaviors based on level of cloud adoption.** We looked at whether organizations with lower levels of cloud adoption behave differently from those with higher levels of cloud adoption – for example, spending, number of tools, and platforms and vendors used.
- **How cloud expenditure influences technology choice.** For example, we explored whether the level of investment in cloud corresponds to using more or fewer tools, more or fewer platforms, or whether they prefer public or private cloud.
- **How security practices affect confidence in security posture.** We investigated whether people working for companies that have taken more security measures feel more confident about their company's security posture.
- **How specific cloud investments influence an organization's level of security preparedness.** For example, does the number of vendors or tools a company uses influence its level of security preparedness?
- **Whether organizations at different levels of security preparedness face different challenges or threats.**

Based on these interrelationships, we uncovered a number of key insights:

- How to best support security through a balance of tools, vendors and employees
- The key challenges organizations face as they scale their security actions
- The practices that help companies address and overcome these key challenges
- How developing key security capabilities drives a strong security posture

To understand security preparedness – how well a company is guarding its cloud infrastructure, applications and data – we analyzed 19 specific security actions that survey respondents told us their companies were taking and over how much of its cloud infrastructure. One example: We asked each respondent whether their company had implemented runtime protection for containers and Kubernetes, and if so, over how large a proportion of its cloud workloads.

We used multiple linear regression modeling to better understand how the 19 security actions drive overall confidence in cloud security, which became our proxy for security posture. Building on the multiple regression model, we used Shapley analysis to understand the relative importance of each action and how much each variable was responsible for the predictive power of the model.

Working with the security preparedness measure and our analysis of respondents' confidence in their organizations' cloud security posture, we were able to determine whether taking more security actions – and which actions – contribute to a strong cloud security posture.

For more information about the research firm that did the fieldwork and provided the advanced analytics for this survey, visit www.OnRcx.com.