PRISMA® CLOUD | paloalto® NETWORKS | FLOW the smart choice

THE STATE OF CLOUD NATIVE SECURITY REPORT 2022

Find Your Path to Successful Cloud Expansion

Table of Contents

Introduction

In these yearly State of Cloud Native Security Reports, more than 3,000 respondents around the world are surveyed about their cloud adoption strategies, budgets, experiences, and plans. Their responses shed light on the practices, tools, and technologies used to implement cloud workloads and manage security for cloud native architectures. As in the 2020 report, we aim to highlight the behaviors and correlated outcomes of organizations who succeeded in their cloud initiatives, as well as those who fell short. A clear differentiator appeared in how organizations addressed cloud security. This includes differences in how they implemented technologies and processes to support both high security posture, defined as the effectiveness of their cloud security efforts, and low security friction, defined as the degree to which cloud security is limiting their operations.

Perhaps unsurprisingly, the COVID-19 pandemic influenced both cloud expansion and results (see "The Ongoing Impact of COVID-19"). While organizations moved quickly during the pandemic to respond to increased cloud demands, many still struggled to automate cloud security and mitigate cloud risks. Yet, the move to the cloud continues for companies at all stages, from those newly taking advantage of cloud capabilities to the well-established, born-in-the-cloud organizations.

The report identified patterns in approaches and outcomes that led to three representative groups known as Moderate Adopters, Rapid Expanders, and Established Users. These groups emerged based on traits such as cloud footprint, transformation goals, and operational strategies. We present these groups along with rigorous data and analysis of their behaviors to help readers find their organization's peer group and identify common challenges and strategies that impact outcomes. Regardless of your organization's cloud maturity level, industry, region, or cloud-migration goals, the research outlined in this report provides the essential insights you need to plan your cloud adoption path.

Executive Summary

As the cloud's unique capabilities continue to evolve, so have the ways in which we employ it to drive business forward. As such, this report includes research that pays special attention to the latest top-of-mind concerns and narratives in the cloud native security community, including automation, DevSecOps, security posture, the use of open source and more. Our goal each year in the production of this report remains the same: for you to come away with valuable insights that help guide your cloud adoption and security journey in 2022 and beyond.

Cloud Expansion and Strategy

- Organizations rapidly **expanded their use of clouds during the pandemic by more than 25% overall** but struggled with comprehensive security, compliance, and technical complexity.
- Organizations expanded with less budget, with **39% of organizations spending less than $10M on their cloud** (up 16% from 2020) and **only 26% spending more than $50M** (down 17% from 2020).
- While organizations continue to use diverse compute options, **platform as a service (PaaS) and serverless approaches rose 20%**, likely supporting the rapid transition to the cloud, while the use of containers and containers as a service (CaaS) saw more moderate growth.

Security Posture and Friction

- **Organizations with a strong security posture are more than 2X more likely to have low levels of security friction**—the degree to which organizations believe cloud security supports or limits their operations. This highlights the need for a two-pronged approach to cloud security, with effective security capabilities that don't disrupt teams outside of security.
- Organizations with best-in-class security operations see the greatest benefits to their workforce in terms of productivity and satisfaction. **Eighty percent of those with strong security posture and 85% of those with low security friction reported increased workforce productivity**.
- A majority of organizations **(55%) report a weak security posture** and believe they need to improve their underlying activities—such as gaining multicloud visibility, applying more consistent governance across accounts, or streamlining incident response and investigation—to achieve a stronger posture.
- **Eighty percent of organizations that primarily use open source security tools have weak or very weak security posture**, compared to 26% of those who primarily leverage their cloud services provider and 52% of those who depend on third parties, highlighting that piecing together a platform using disparate tools leaves an organization less secure.

Security Drivers

- Organizations are consolidating their security approach. **Nearly three-quarters use 10 or fewer security tools**, and we see a **27% increase from the 2020 data in the number of organizations using just one to five security vendors**, suggesting that they are looking to fewer security vendors for more capabilities.
- **Organizations that have implemented a high level of security automation are 2X more likely to have low friction and strong posture** than their counterparts with low levels of security automation.
- How well organizations adopted and implemented DevSecOps methodologies is the primary indicator of best-in-class security. **Organizations that tightly integrate DevSecOps principles are over 7X more likely to have strong or very strong security posture and are 9X more likely to have low levels of security friction**.

The Ongoing Impact of COVID-19

"Rapid cloud scale and complexity without automated security controls embedded across the entire development pipeline are a toxic combination."

This year's survey was conducted during May 2021—a little over a year after the COVID-19 pandemic sent entire countries into shelter-at-home restrictions. Our survey respondents reported on business decisions made over their previous 12 months, from June 2020 through June 2021, a period that represents the most profound worldwide social and economic upheavals since World War II. The decisions these organizations made were in response to dramatic and unexpected changes in demand for cloud-delivered services, which occurred almost simultaneously around the globe and impacted every industry segment:

- The rapid shift to remote work, school, and healthcare driving a surge in the use of online collaboration and meeting tools.
- A sudden, acute demand for business-critical applications delivered in the cloud.
- A broad consumer shift to low-contact online shopping and takeout dining.
- Intensified demands for cloud infrastructure support for everything from social services to supply chain management.

And as companies raced to meet new and unexpected demands, they found themselves facing another kind of global threat: cyberattacks. A Palo Alto Networks Unit 42 Cloud Threat Report on COVID noted "an explosion of security incidents" that correlated to increased cloud spending by organizations beginning in the first six months of the pandemic. The conclusion was that "rapid cloud scale and complexity without automated security controls embedded across the entire development pipeline are a toxic combination." At the time of writing, the pandemic stretches on. Organizations continue to move workloads to the cloud while still struggling to automate cloud security and mitigate cloud risks.

The Global State of Cloud and Cloud Native Security

In the first section of this report, we review the broad trends in cloud adoption and cloud security activities as reported by organizations around the world. (See the Methodology and Demographics section for more detail on who we surveyed.)

Cloud Growth Through the Pandemic

Throughout the pandemic, there were significant expansions of cloud workloads overall, jumping to **an average of 59% of workloads hosted on the clou**d, up from an average of 46% in 2020. **In addition, 69% of organizations host more than half of their workloads in the cloud**, up from just 31% of respondents in 2020.

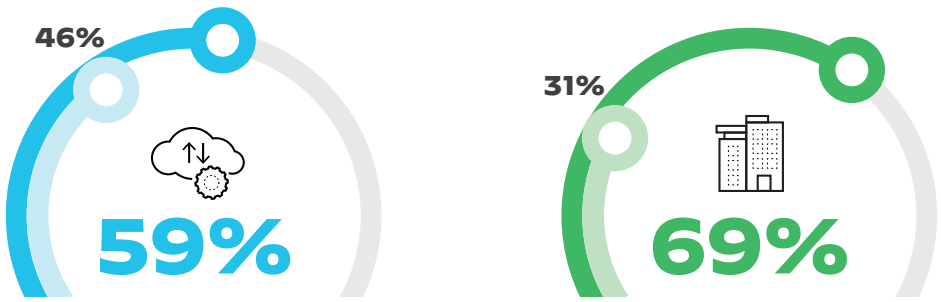


Figure 1: Percent change in cloud workload volumes since 2020

Looking ahead, organizations have not significantly changed their expectations for leveraging the cloud since last year. On average, organizations expect to host 68% of their workloads in the cloud within two years, which is consistent with last year's expectation of 65%. Despite a faster shift during the pandemic than many organizations expected, this suggests that the upper limit of organizations' cloud transformation has not significantly grown.

Cloud composition also evolved this year, as organizations shifted toward private hosting of their cloud workloads, with an average of 55% of cloud workloads on private clouds, up seven percentage points from 2020. While organizations continue to use diverse compute options, **PaaS and serverless approaches rose 20 percentage points, while the use of containers and CaaS saw more moderate growth**. PaaS and serverless strategies, which allow development teams to put applications in the cloud without necessarily having to build and scale infrastructure at the same time, likely helped support the rapid transition to the cloud seen in the past year. This is a trend we expect to continue and plan to closely monitor.

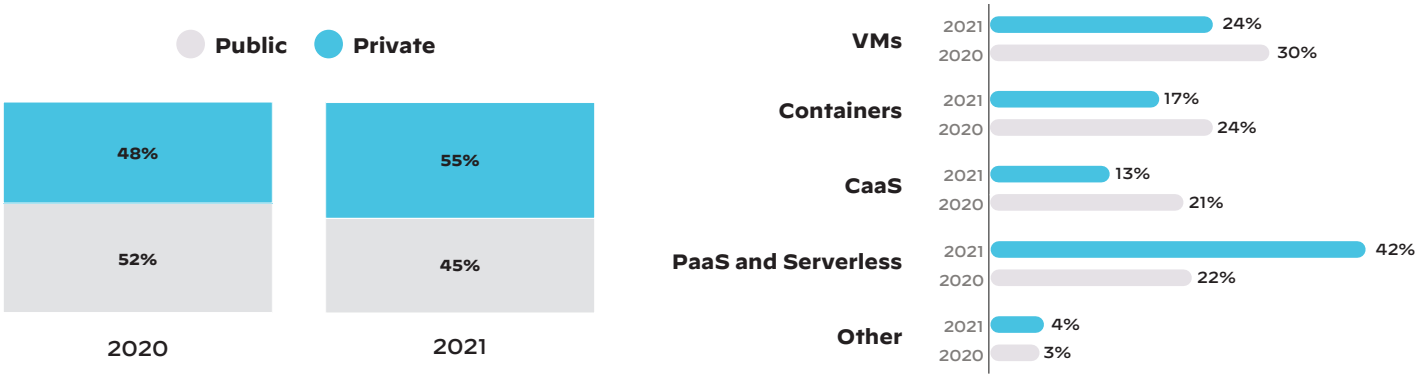


Figure 2: Share of workloads hosted in public vs. private clouds (left); share of workloads by compute type (right)

When examining the reasons why organizations expanded their cloud capabilities, the growth was fueled by strategic business drivers—application modernization, maintaining competitiveness, and controlling infrastructure overhead. While the pandemic was surely a contributing factor in this year's report, these reasons remain paramount for why organizations choose to utilize the cloud in general. The flexibility and agility that the cloud provides to organizations allow them to keep businesses moving forward at an ever-increasing pace.

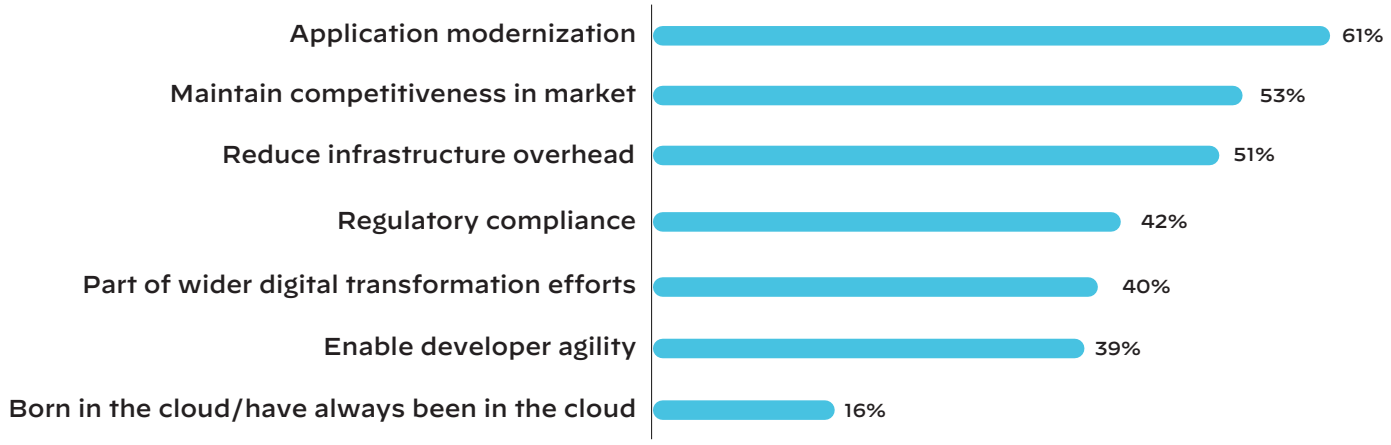


Figure 3: Reasons for expanding cloud capabilities

Despite the push to move more workloads to the cloud, organizations did so with less budget than the previous year. **In 2021, 39% of organizations spent less than $10 million on their cloud**, an increase of 16% from 2020, **while only 26% spent more than $50 million**, a drop of 17% from 2020. This drop in cloud spending may be the result of across-the-board budget cuts or reallocation of funds due to the pandemic, or it may simply reflect a "normalization" of cloud activities, with budgets falling naturally as teams gain confidence and efficiencies with experience.

In 2020, 21% of organizations dedicated less than **$10M** toward their cloud.

In 2021, 39% of respondents fall in that category.

Orgs with cloud budgets over **$50M** dropped from **46% to 26%**.

Figure 4: Changes to cloud budgets

While we see slight differences in cloud adoption approaches by industry, geography, and revenue, the data indicates that these variations do not play a significant role in overall results. That said, the figure below highlights some of the more notable regional variations.

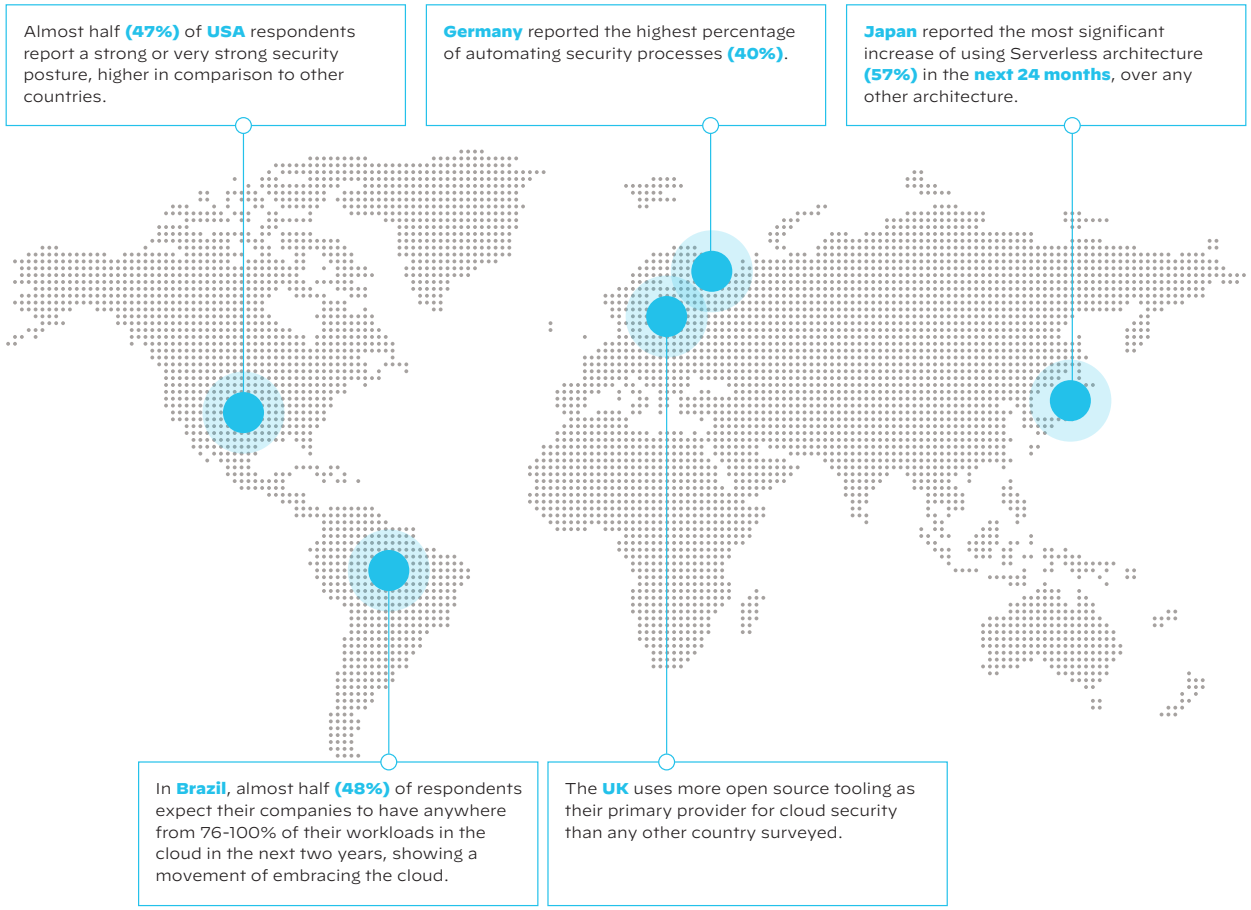


Figure 5: Cloud trends by global region

Security Challenges in Moving to the Cloud

As organizations rapidly expanded their use of the cloud over the past year, they reported the same top challenges as last year's respondents: comprehensive security and compliance, along with technical complexity.

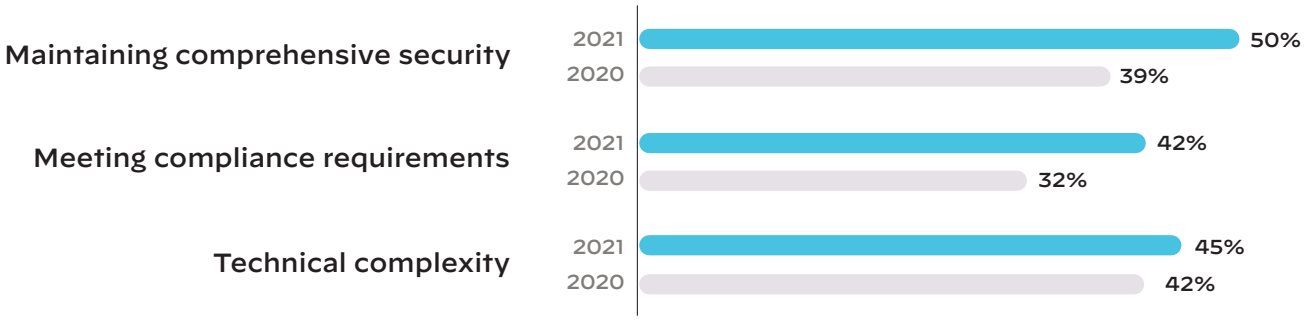


Figure 6: Challenges in moving to the cloud

While top-line cloud budgets fell, cloud security budgets remained steady. We interpret that to mean that while organizations spent less money on the cloud overall, they did not let their security budgets waver. This highlights that companies understand the value of securing the cloud in order to take the most advantage of it.

We saw this year that **companies expanded their cloud security teams during the pandemic, with 53% of organizations reporting a security team of over 30 people, up from 41% last year**. Companies also consolidated their cloud security vendors as they expanded their cloud environments. The data shows a 27% increase in the number of organizations using just one to five security vendors, while those using six to ten vendors is down 19% since last year.

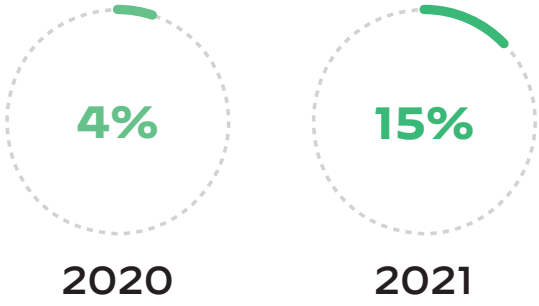


Figure 7: Respondents spending more than 20% of cloud budget on security

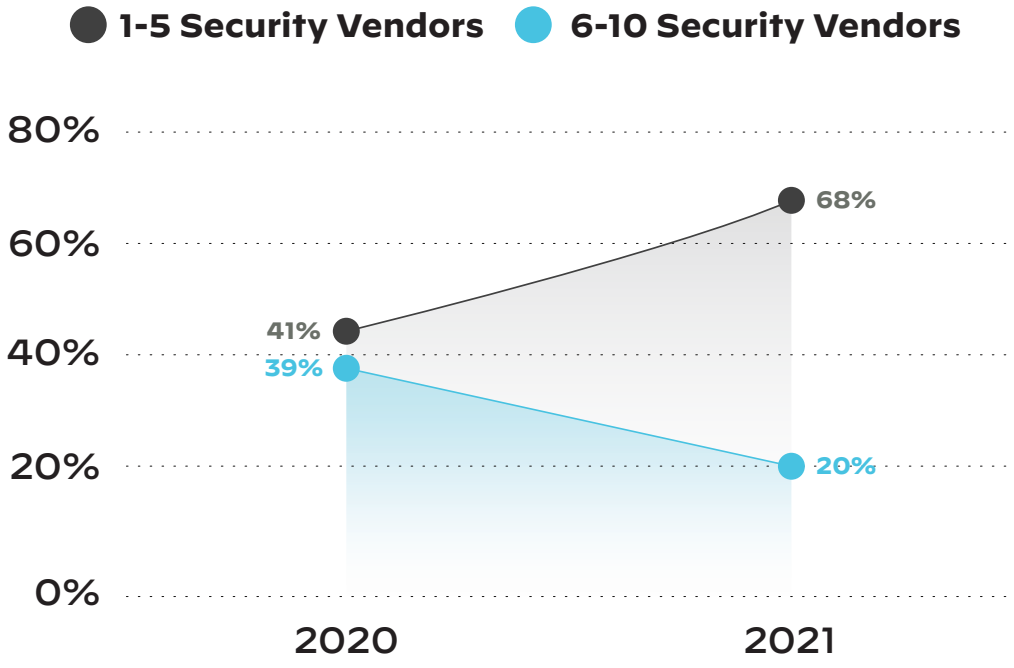


Figure 8: Changes to number of security vendors

While companies reduced the number of security *vendors* they engage, they made minimal year-over-year changes in the number of security *tools* they are leveraging. We define cloud security vendors as any company that organizations employ to secure their clouds and security tools as the number of capabilities and/or features those cybersecurity companies offer. **Nearly three-quarters of organizations use 10 or fewer security tools**, suggesting that they are looking to fewer security vendors to satisfy the need for a wide range of capabilities. This consolidation supports observations that organizations who depend on disparate tools from multiple vendors can experience blind spots that increase risk and force additional efforts to close those gaps. For the 28% of organizations who are still using large numbers of tools—including the 8% using 21 to more than 50 tools—we raise a cautionary flag.

Of those organizations that used 21 or more security tools, almost all (91%) used six or more vendors to supply them. To manage so many tools simultaneously, these organizations had larger teams managing and supporting cloud workload security; nearly half (49%) of them employed more than 50 employees to manage cloud security. Perhaps not surprisingly, then, higher tool usage is more likely to be taken on by companies with higher revenues. Of respondents working at companies with revenues of $1 billion, 11% indicated using 21 or more tools, versus only 3% of those working for companies with revenues less than $1 billion.

Organizational Attributes of High Performance

Beyond the varying use of security vendors and tools, we also examined the organizational security attributes that underlie successful cloud expansion. The research highlights the key elements of cloud native security, drivers for best-in-class security, and the impact of security on wider organizational success.

To reach a conclusion that allowed us to compare otherwise disparate organizations, we studied two opposing security attributes:

- Security posture is how organizations rate the effectiveness of their cloud security efforts.
- Security friction is the degree to which organizations believe cloud security supports or limits their operations.

To measure cloud security posture, we asked respondents about their agreement with six statements. The more strongly a respondent agreed with the statements, the stronger the overall perception of the organization's cloud security posture. We found that a slight majority of organizations (55%) have a weak security posture. More specifically, this majority believes their underlying activities—such as gaining multicloud visibility, applying more consistent governance across accounts, or streamlining incident response and investigation—need to be more effective.

Security Posture and Spending

Organizations with strong security postures tend to spend more on security. Over two-thirds of those with strong or very strong security posture invested 16% or more of their cloud budget on security. For those with weak or very weak security posture, under a fifth spent the same percentage of their cloud budget on security. The "strong security posture" group also appears to have plans to increase its security spending. Nearly three-quarters (71%) of organizations with strong or very strong security posture plan to spend 16% or more of their cloud budget on security over the next 12 months, versus only 46% of the weak or very weak security posture group.

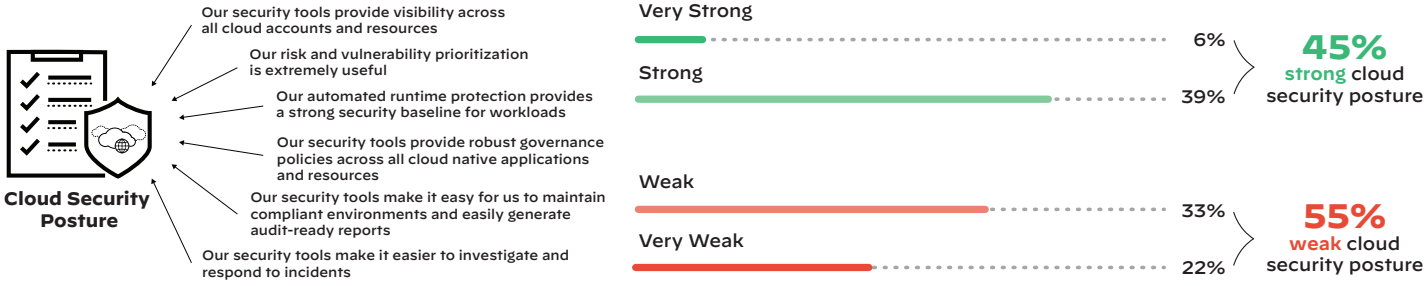


Figure 9: Factors contributing to security posture (left); percentage of organizations with strong or weak security posture (right)

To analyze cloud security friction, we asked respondents whether they agree with two statements about business outcomes as a result of cloud adoption and security. The more strongly a respondent agreed with the statements, the higher the respondent's overall perception of their company's cloud security friction. Here we find that **just under half (48%) of organizations believe they have low security friction**.

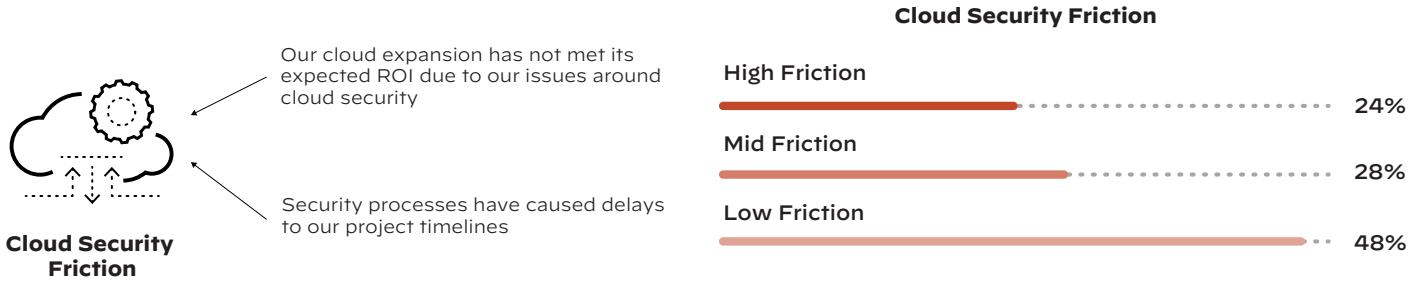


Figure 10: Factors contributing to organizational friction (left); Percentage of organizations with high, medium, or low friction (right)

By combining these two metrics, we see that achieving low security friction is essential to driving a stronger security posture. **Organizations with a strong security posture are more than two times more likely to have low levels of security friction**. This highlights the need to take a two-pronged approach to cloud security: organizations should strive for the most effective security capabilities, but they need to ensure those tools and processes do not interfere with the flow of business operations.

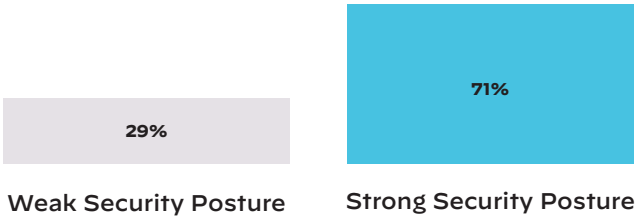


Figure 11: Percent of "low-friction" organizations with weak or strong posture

Beyond operational excellence, we also see additional advantages to achieving these best-in-class security outcomes. Organizations that enable high security posture and low friction see the greatest benefits to their workforce in terms of increased productivity and higher employee satisfaction with **over 80% of organizations with low levels of security friction reporting increased or significantly increased levels of employee satisfaction**.

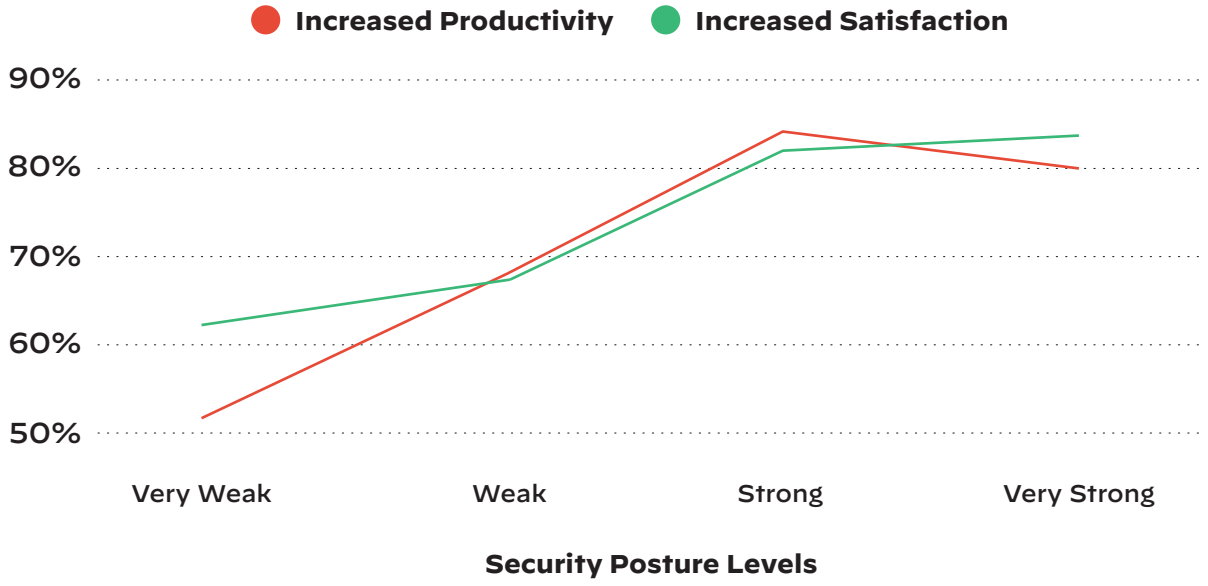


Figure 12: Comparing organization outcomes to overall security posture

How Organizations Achieve Stronger Security Posture

Next, we examine the approaches taken by top-performing organizations to reduce organizational friction and improve overall posture. The organizations that achieve this balanced, best-in-class security excel in two related disciplines:

- DevSecOps integration—the degree to which cloud security touchpoints have been integrated into the full development lifecycle, from build to runtime.
- Cloud security automation—the degree to which cloud security has been automated.

We asked respondents to rate the degree of their organization's DevSecOps integration on a scale of "never" to "always" in response to four questions.

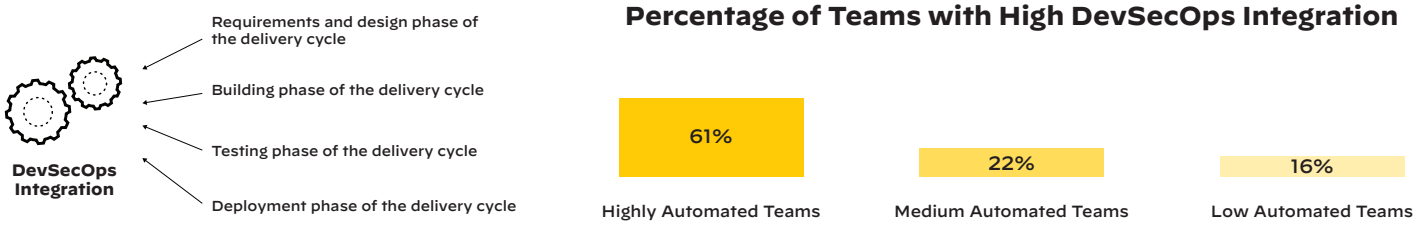


Figure 13: Factors that contribute to DevSecOps integration measurement (left); comparing DevSecOps integration to automation levels (right)

How well organizations adopted and implemented DevSecOps methodologies was the primary indicator of best-in-class security. **Organizations that tightly integrate DevSecOps principles into their development lifecycle are over seven times more likely to have strong or very strong security posture and are nine times more likely to have low levels of security friction.**

To measure automation, we asked respondents to rate how deeply their organization has automated five security practices, on a scale of "completely manual" to "completely automated."

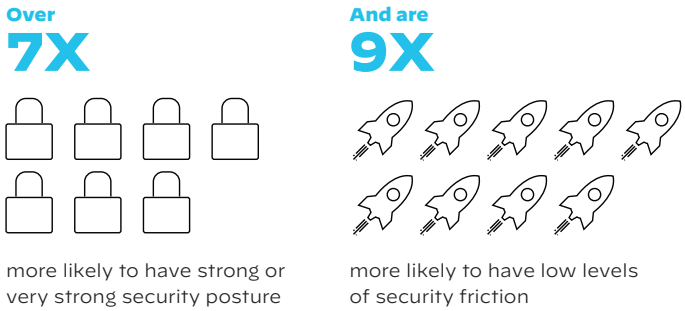


Figure 14: Outcomes for organization that tightly integrate DevSecOps principles

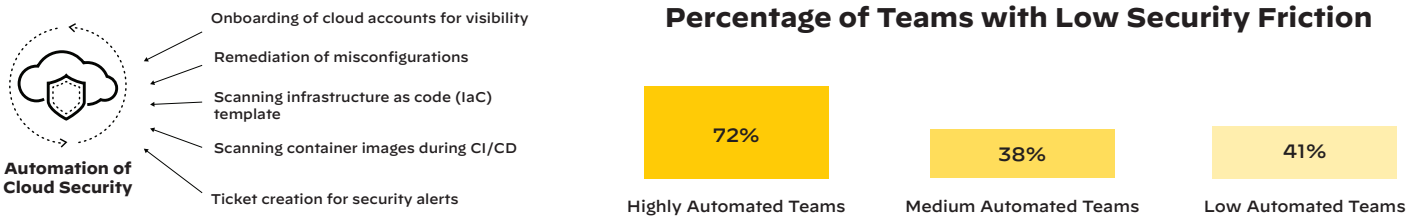


Figure 15: Factors that contribute to automation measurement (left); comparing security friction to automation levels (right)

We find that **organizations that have implemented a high level of security automation are roughly two times more likely to have low friction and strong posture than their counterparts with low levels of security automation**. Specifically, pushing past "average" levels of automation leads to a significant increase in security outcomes.

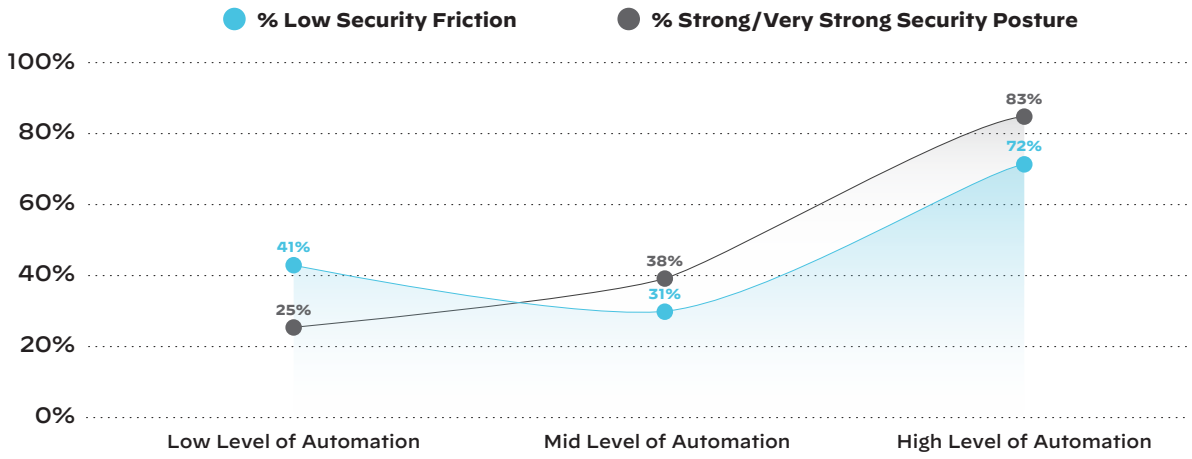


Figure 16: Automation as a driver of security outcomes

The Impact of Open Source Security Tools

Organizations took a wide variety of approaches to the providers of their security tools, leveraging cloud service providers (CSPs), third parties, and open source security tools. However, the data reveals consistent challenges for organizations that rely primarily on open source tools.

This group tends to have smaller budgets than their counterparts who are leveraging third-party or CSP methods, but perhaps counter-intuitively, these teams are larger than those using tools from third-party or CSP providers, with **70% of organizations that rely primarily on open source tools reporting security teams of 30 or more**.

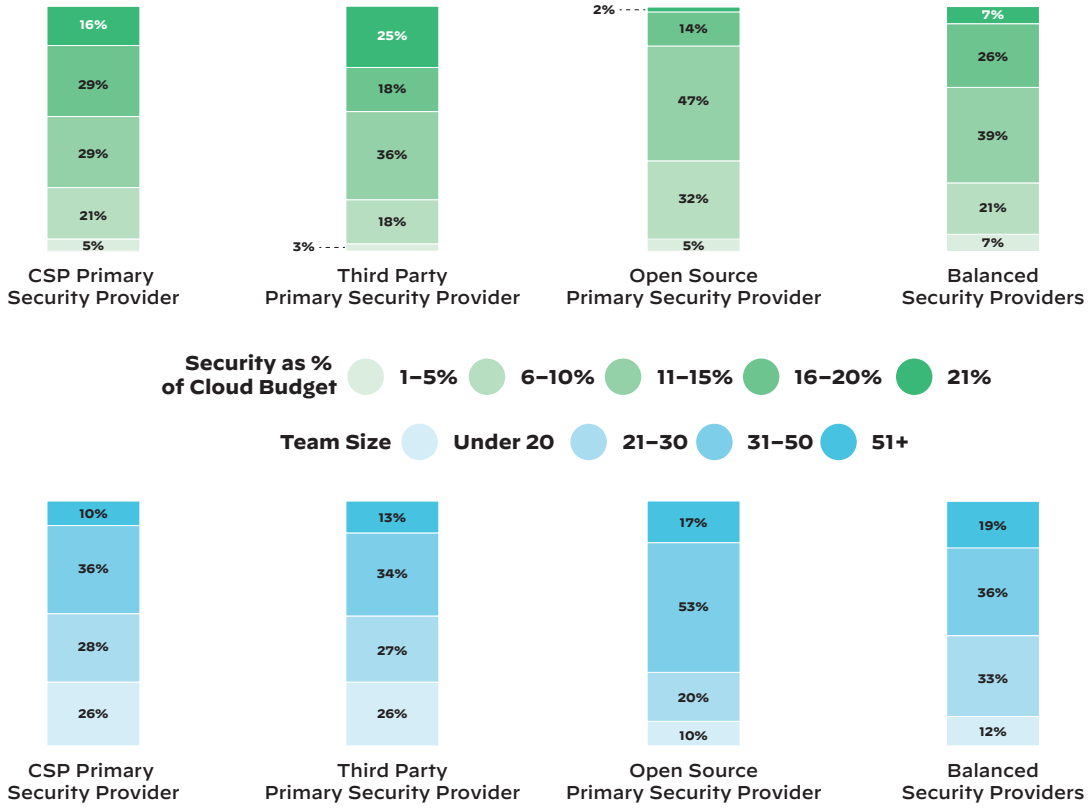


Figure 17: Security provider and team budget (top) and size (bottom)

Furthermore, of those who are using primarily open source security tools, 80% have weak or very weak security posture.

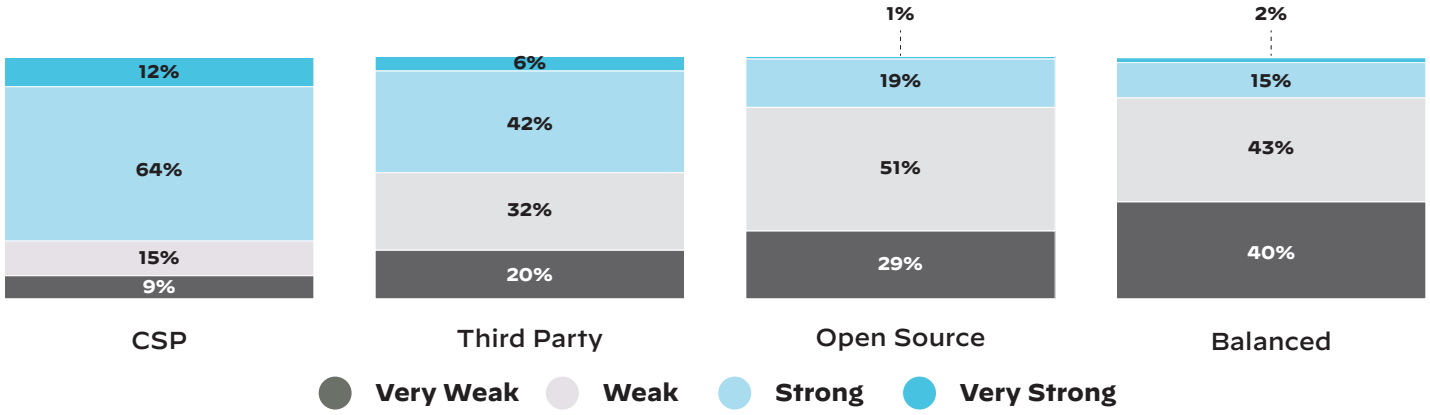


Figure 18: Security provider and security posture

In aggregate, the data suggests that open source security tools do not offer an integrated, comprehensive approach that satisfies the full range of capabilities and features organizations are looking for. Organizations successfully utilizing open source security tools seem to merely shift budget costs to labor in order to support their efforts. Organizations that are looking to adopt open source tools should be prepared to trade a highly customized implementation with ongoing investments for internal support that would otherwise come from designated solution providers.

Identify and Learn from Your Cloud Group

To determine if certain frameworks can drive best-in-class security outside of DevSecOps methodologies and automated security, as noted above, we looked for patterns in the paths that organizations took to develop their cloud environments and cloud security during the pandemic. This period provided something of a natural experiment, where we were able to compare different approaches and see their impact on a significantly condensed timeline. Rather than waiting for several years, this concentrated move to the cloud produced rapid results in just months.

From the data, we discovered three representative groups based on organizational behaviors and approaches to cloud security. Note that our **findings from these groups remain consistent regardless of geography, industry, or revenue**. This gives us a unique look at cloud success factors—and paths to failure—based on how organizations approach their cloud and cloud security initiatives rather than who they are.

> "This gives us a unique look at cloud success factors—and paths to failure—based on how organizations approach their cloud and cloud security initiatives rather than who they are."

The first group is the **Moderate Adopters**, comprising organizations with a lower focus on cloud adoption both before and during the pandemic. The second group is **Rapid Expanders**, made up of organizations that had small cloud footprints before the pandemic but engaged in rapid, widespread cloud adoption during the pandemic. Finally, **Established Users** are organizations that already had large cloud footprints before the pandemic and continued moderate expansion during this time.

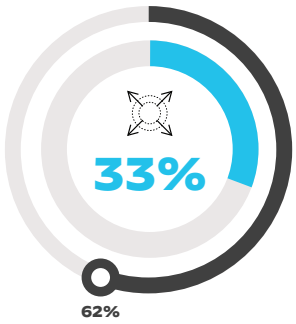
We encourage you to explore the traits and experiences of each group to identify which most closely matches your organization. You can use the data to benchmark your organization against your peers, validate experiences, and explore differences. This analysis also allows you to identify a group that most closely matches your future cloud aspirations and explore the decisions and behaviors the group exhibits to inform your ongoing strategies for long-term success.

Which Group Best Describes Your Organization?

Moderate Adopters: 39% of total
More likely to have lower revenue
Before pandemic: Small cloud footprint

During pandemic:
Steady cloud expansion
Expansion driven by tactical value
Low investment and priority for cloud

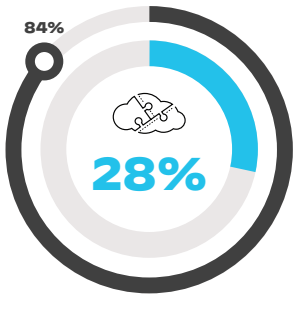
Currently: Leveraging serverless architectures
Planning: Average target for total cloud usage (62%)



Rapid Expanders: 33% of total
Tend to have higher revenue
Before pandemic: Small cloud footprint

During pandemic:
Rapid cloud expansion
Expansion driven by strategic and tactical value
Average investment and priority for cloud

Currently: Leveraging PaaS architectures
Planning: Average target for total cloud usage (62%)



Established Users: 28% of total
Mostly large organizations (by revenue)
Before pandemic: Large cloud footprint

During pandemic:
Steady cloud expansion
Expansion driven by tactical value
High investment and priority for cloud

Currently: Balanced use of compute environments
Planning: High target for total cloud usage (84%)

Figure 19: Characteristics of each cloud adoption group

The State of Cloud Adoption Groups

As stated earlier, the cloud traits and behaviors of these groups are generally consistent regardless of geography, industry, or size of the organization.

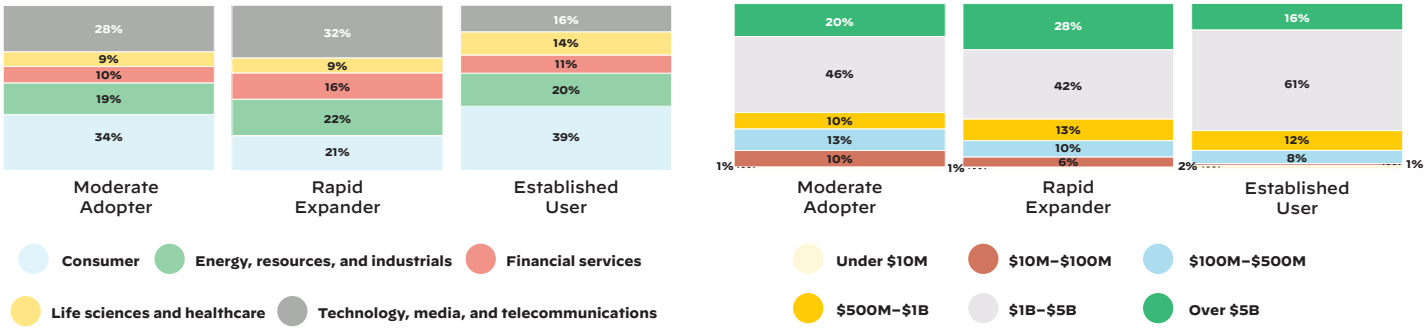


Figure 20: Cloud adoption groups by industry (left); cloud adoption groups by income (right)

Cloud Footprints

Moderate Adopters came into the pandemic with a fairly small cloud footprint and expanded minimally over the following 12 months. Rapid Expanders entered the pandemic with a similar small cloud estate but with much faster expansion. In contrast, Established Users show a significant existing cloud footprint but with slower growth, similar to the Moderate Adopters.

Future Cloud Plans

When asked about future plans, both groups with small, pre-pandemic footprints—Moderate Adopters and Rapid Expanders—expect to have 62% of workloads moving to the cloud over the next two years. In contrast, Established Users expect to continue their heavy adoption, putting an average of 84% of workloads in the cloud in the next two years.

	2020	2021	Current Total	2022 Target
Moderate Adopter	35%	14%	49%	62%
Rapid Expander	26%	33%	59%	62%
Established User	61%	13%	74%	84%

Figure 21: Percent of workloads in the cloud by adoption group

Cloud Spending

Across all groups, cloud spend varied significantly. Only 42% of Moderate Adopters spent more than $10M on the cloud, compared to 69% of Rapid Expanders and 70% of Established Users. Established Users also have the highest cloud budgets, with 10% spending over $100M, compared to just 2% of Moderate Adopters and 1% of Rapid Expanders.

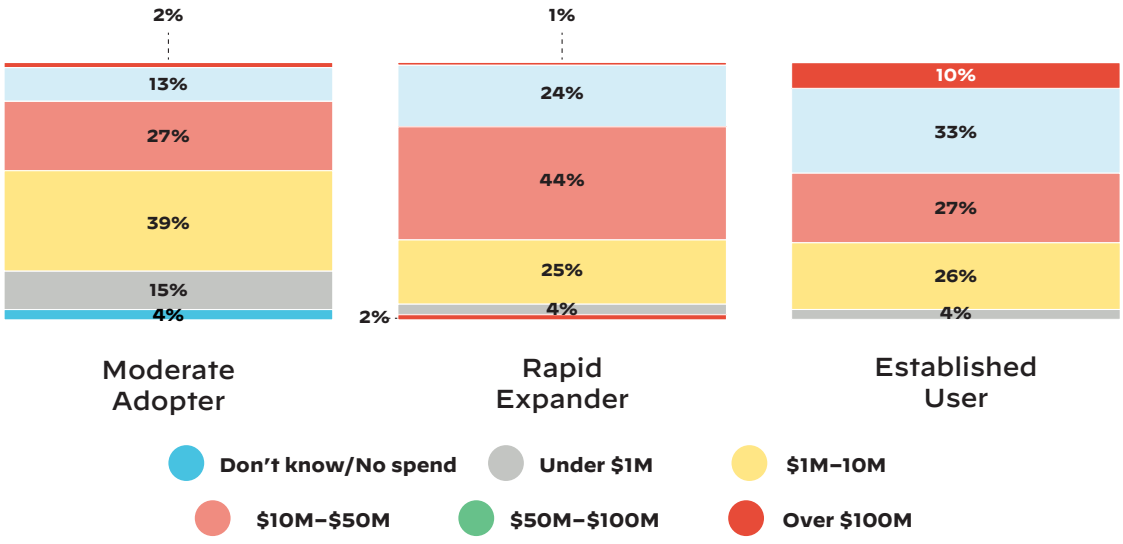


Figure 22: Total cloud spend by adoption group

Approach to Compute Environment

We also see differences in approaches to cloud architectures. Established Users are far more likely to use a blend of compute environments, including virtual machines (VMs), containers/CaaS, PaaS, and serverless, with 65% of this group using all four equally. **Rapid Expanders also show a mostly balanced approach (48%), but with twice the use of PaaS compared to Established Users (28% versus 14%)**. This decision to avoid infrastructure management may have enabled some of Rapid Expanders' fast growth.

Our analysis is that Moderate Adopters, with smaller cloud footprints and slower growth plans, may not be "cloud-first" organizations; rather, their cloud efforts are designed to support other organizational strategies. This group's compute decisions (47% primarily use serverless, and 32% have a balanced stack) may reflect this, with an approach that favors lower overhead and is focused on the development of application code rather than building and maintaining cloud infrastructure.

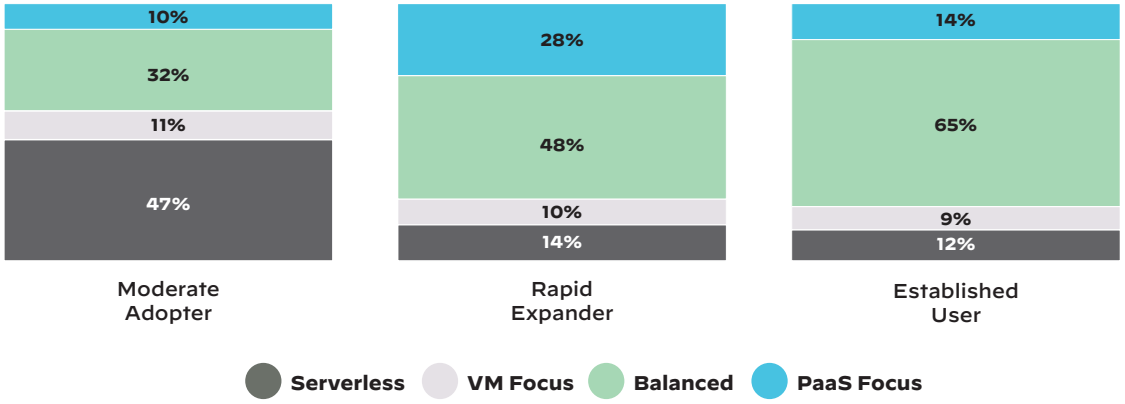


Figure 23: Compute architecture mix by adoption group

Rapid Cloud Expansion Has Polarizing Results

As we investigated the cloud goals of our groups deeper, we uncovered a surprising pattern. The Rapid Expander group split into two distinct sub-groups. **The majority of Rapid Expanders (74%) raced to successfully increase their cloud footprint**, moving 35% of workloads to the cloud in the past year and planning to move another 12% of workloads over the next two years.

In contrast, **the other 26% of Rapid Expanders** moved 28% of workloads to the cloud during the pandemic, but strikingly, they **plan to decrease cloud workloads by 26% in the next two years**, which suggests that they plan to either move workloads out of the cloud or not add any net new workloads to the cloud.

This divide in the rapid-growth group prompted new questions: What caused such a dramatic split? What can we learn from these organizations' experiences? How can we apply that learning to successful future cloud initiatives?

	2020	2021	Next Two Years
Moderate Adopter	35%	14%	+13%
Rapid Expander Challenging Adoption	34%	28%	-26%
Rapid Expander Successful Adoption	24%	35%	+12%
Rapid Expander	61%	13%	+10%

Figure 24: Cloud workload growth for 2020–2021 and expected for 2022–2023

As we dig deeper, this split can be explained by Rapid Expanders, who were successful in their cloud adoption efforts—and those who experienced noteworthy challenges. The Rapid Expanders with challenging adoptions made significantly higher investments in the cloud than their more successful peers, with **45% spending more than $50 million on the cloud in 2021, compared to only 13% of Rapid Expanders that are continuing on their trajectory**. This suggests that some Rapid Expanders may have tried to spend their way out of trouble rather than addressing underlying root issues.

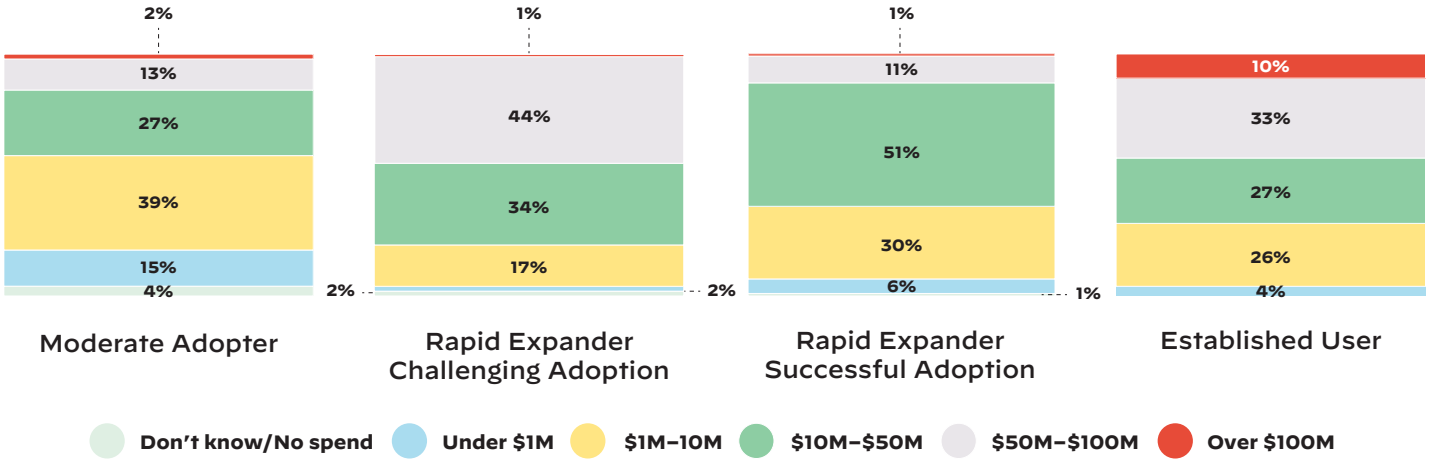


Figure 25: Spending levels by adoption group

We also see significant differences in our groups' cloud objectives. For all groups, short-term goals such as application modernization and maintaining competitiveness were the primary drivers of cloud expansion, while more strategic thinking took a back seat. However, there were large differences in organizational alignment, where our successful Rapid Expanders were significantly more likely to integrate their cloud evolution into a larger strategic digital transformation effort. **Rapid Expanders who successfully expanded their cloud infrastructure over the past year were over two times more likely to have integrated it into a wider, strategic digital transformation effort**.

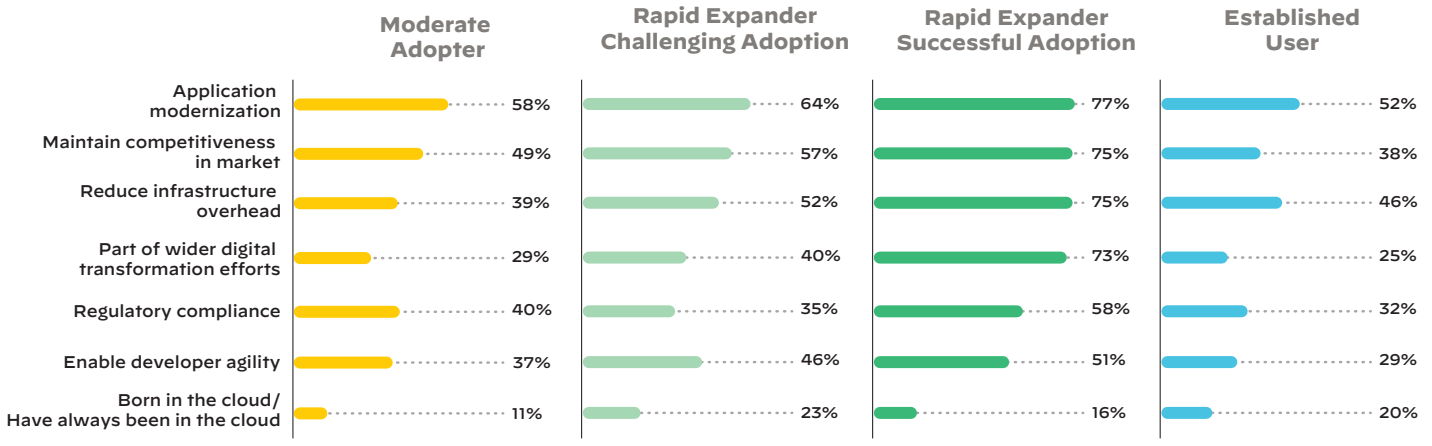


Figure 26: Reasons for moving workloads to the cloud

Additionally, comprehensive security and addressing regulatory compliance were some of the top challenges across all groups, but a critical pattern emerged: **Rapid Expanders cited comprehensive security as a top challenge more frequently than other groups**. They were also significantly more likely to call out challenges with strategy, budget, and talent. **This supports the notion that successful cloud adoption must be part of wider strategic organizational transformations—because the cloud will affect many areas of the business and the wider business must be prepared to support those changes.** While the retreating group of Rapid Expanders represents only 8% of all the organizations studied, they highlight the challenges of integrating security into cloud adoption efforts.

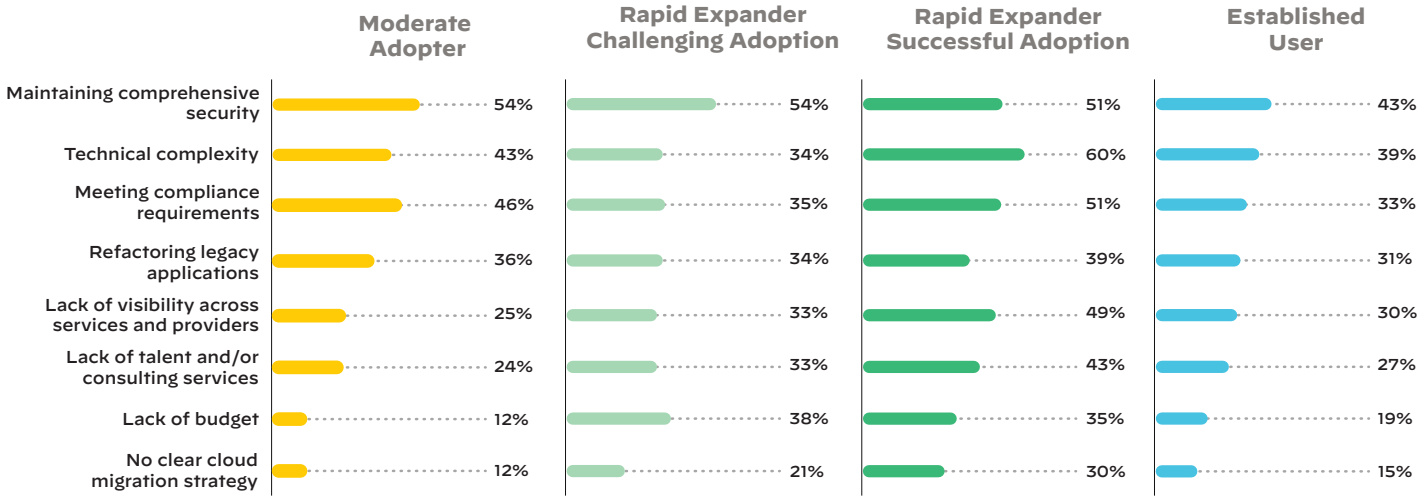


Figure 27: Top challenges for cloud adoption programs

The Role of Security Vendors, Teams, and Tools

The two Rapid Expander groups took two distinct approaches to partner with security vendors—**83% of those who were successful used five or fewer vendors**. At the same time, **only 45% of Rapid Expanders who experienced challenging cloud adoption did the same**.

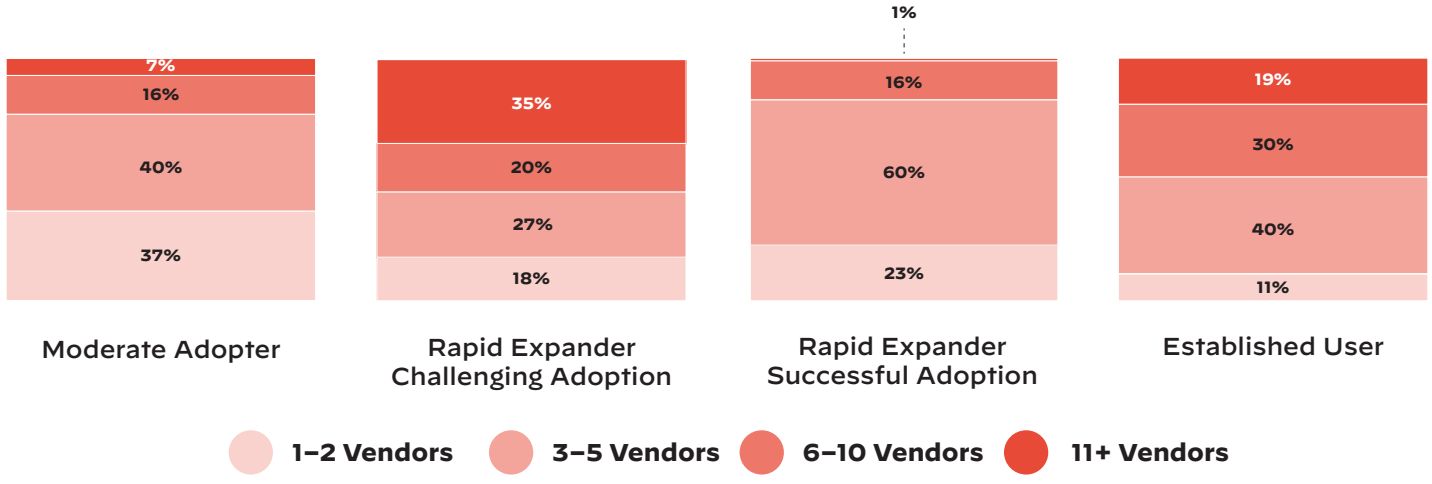


Figure 28: Number of separate security vendors used

Next, as we look at security teams, successful Rapid Expanders tend to have a relatively smaller team along with a smaller vendor network but more security tools (again, security tools are defined as the number of capabilities and/or features cybersecurity companies offer). On the other hand, Rapid Expanders who experienced challenges tended to use larger teams, larger vendor networks, and fewer security tools.

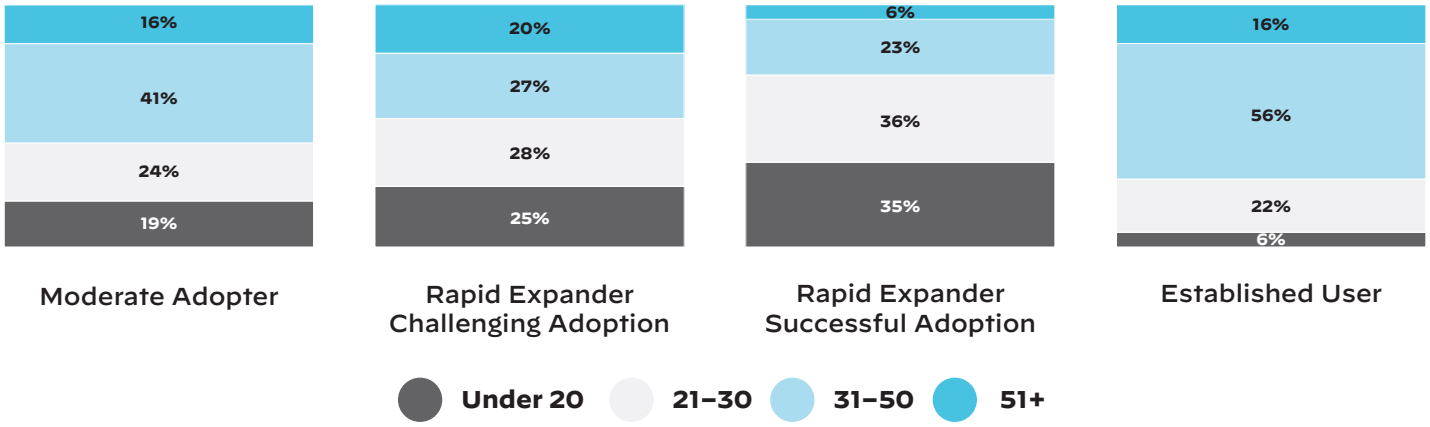


Figure 29: Size of cloud security teams

The research shows high numbers of security tools being used across all groups, with more than half of each using more than five tools. This suggests that there may be a variable equation for the optimal number of security tools needed for a given environment, where larger cloud environments necessarily require more tools or different teams prefer different tool sets. But an over-emphasis on simplicity may be detrimental, where unsuccessful adoptions seem to be driven by a lack of security information and controls due to lack of availability from tooling.

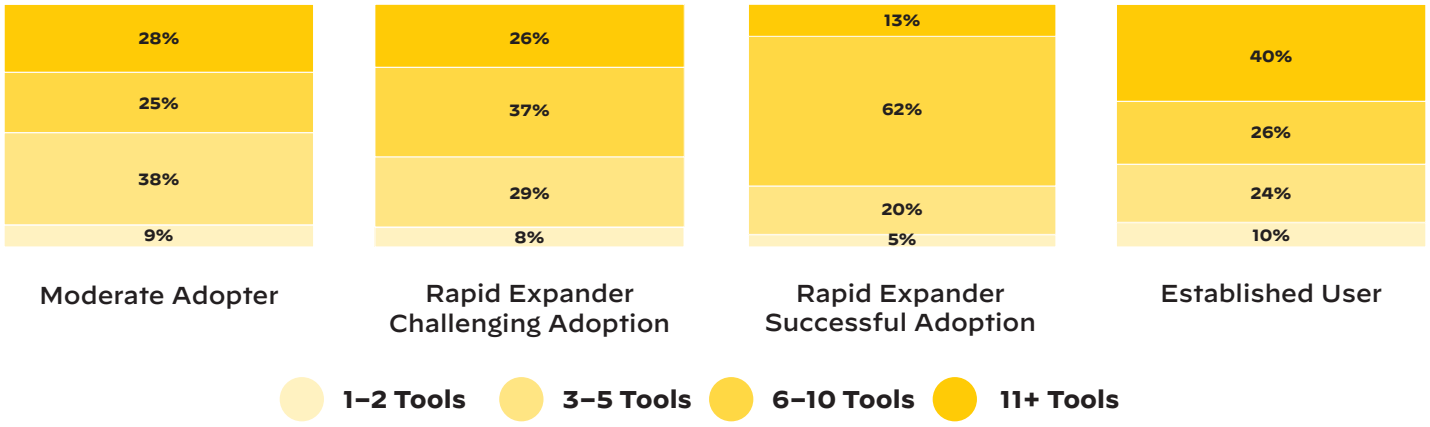


Figure 30: Number of tools used, regardless of vendor

If such a variable equation exists, the data indicates that the integration of security tools is also a critical factor. Companies that leverage fewer than five security tools struggle to deliver a strong or very strong security posture—but friction among teams is unaffected by the number of tools. Rather, it's the ability to integrate your security tools through DevSecOps methodologies—thereby gaining broader visibility and comprehensive control—that results in better outcomes. This aligns with industry trends toward consolidated, comprehensive security platforms.

"It's the ability to integrate your security tools through DevSecOps methodologies—thereby gaining broader visibility and comprehensive control—that results in better outcomes."

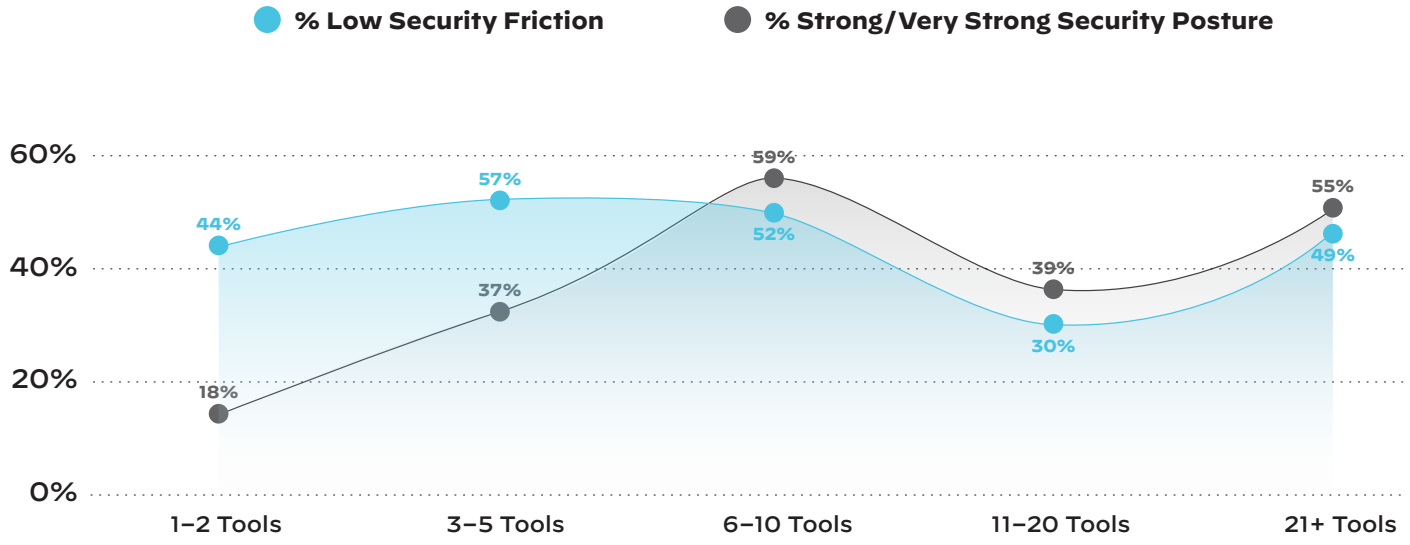


Figure 31: Number of security tools and security outcomes

Group Adoption of Best-in-Class Security

Earlier in the report, we discussed the importance of DevSecOps integration and security automation as critical elements for best-in-class cloud security. Our groups illustrate **63% of Rapid Expanders who successfully expanded their cloud adoption also integrated DevSecOps principles**. This is considerably higher even when compared to Established Users, which suggests that **successful Rapid Expanders paid special attention to integrating security throughout the entire development lifecycle** as they scaled up cloud capabilities.

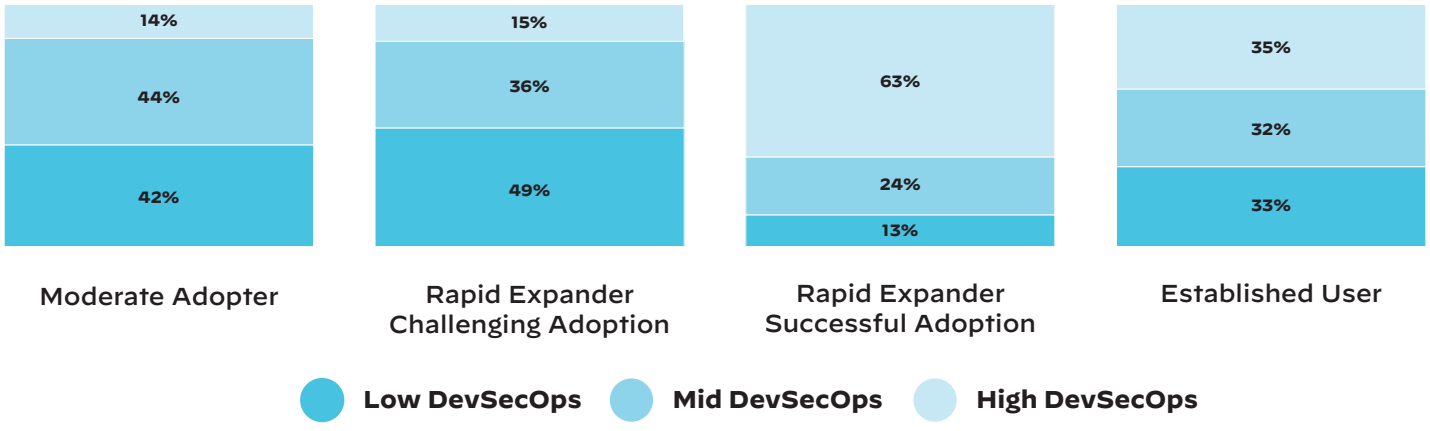


Figure 32: Level of DevSecOps integration into the application lifecycle

Similarly, groups who are heavily leveraging the cloud—Established Users and successful Rapid Expanders—are also leaning into automation, with high levels of automation present for 44% and 40% of the groups, respectively. On the other hand, **Rapid Expanders that struggled with their cloud expansion are lagging, with 40% ranking low in automation**.

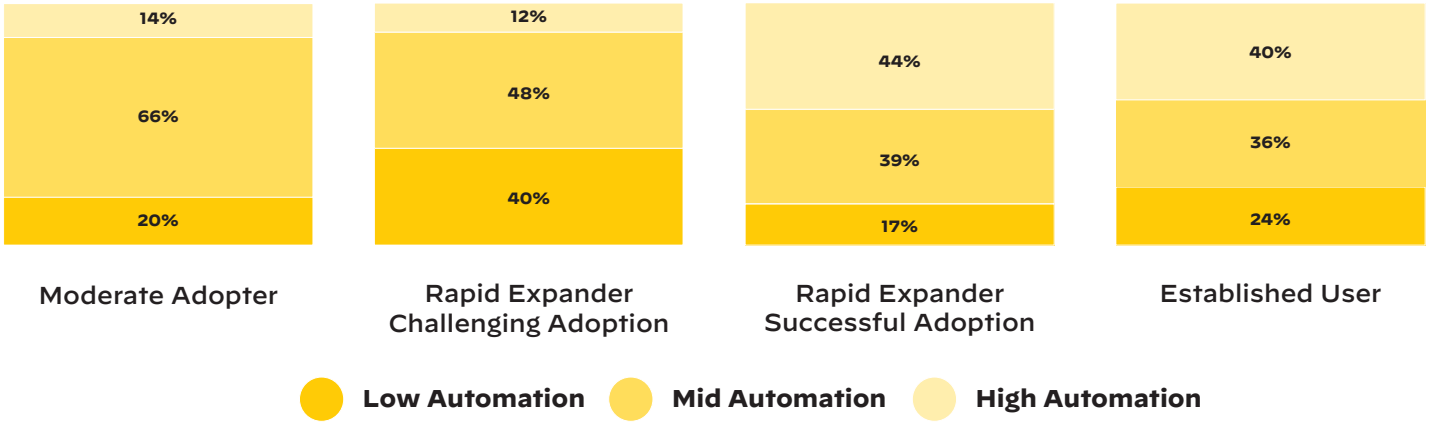


Figure 33: Level of security automation across the development lifecycle

Ultimately, we see that **Rapid Expanders who saw success have the strongest security posture, with 81% ranking strong or very strong**. Established Users are ranked the next-highest at 50%, while **69% of Rapid Expanders who struggled showed a weak or very weak security posture**. Moderate Adopters exhibit a low security posture as well, but as noted earlier, this group, which remains dedicated to lighter cloud usage, may measure cloud success or failure differently.

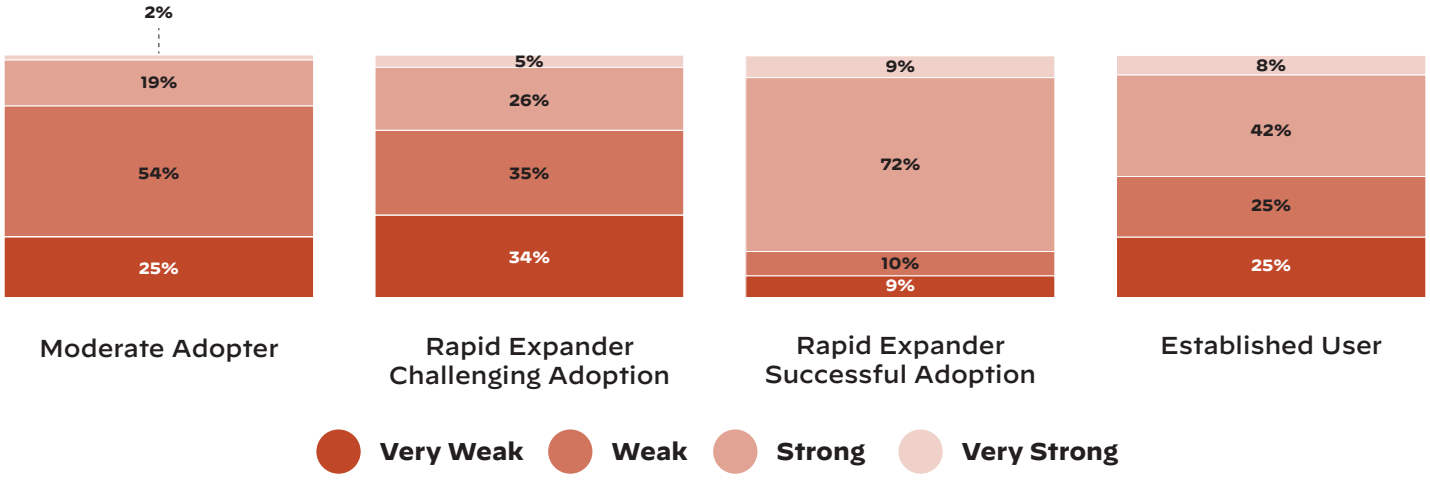


Figure 34: Security posture levels across adoption groups

Here we see more signs that organizational alignment is critical for successful cloud transformations—groups who struggle with their posture also struggle with security friction. **Half of the struggling Rapid Expanders have high security friction, compared to only 13% of successful Rapid Expanders and 14% of Established Users.**

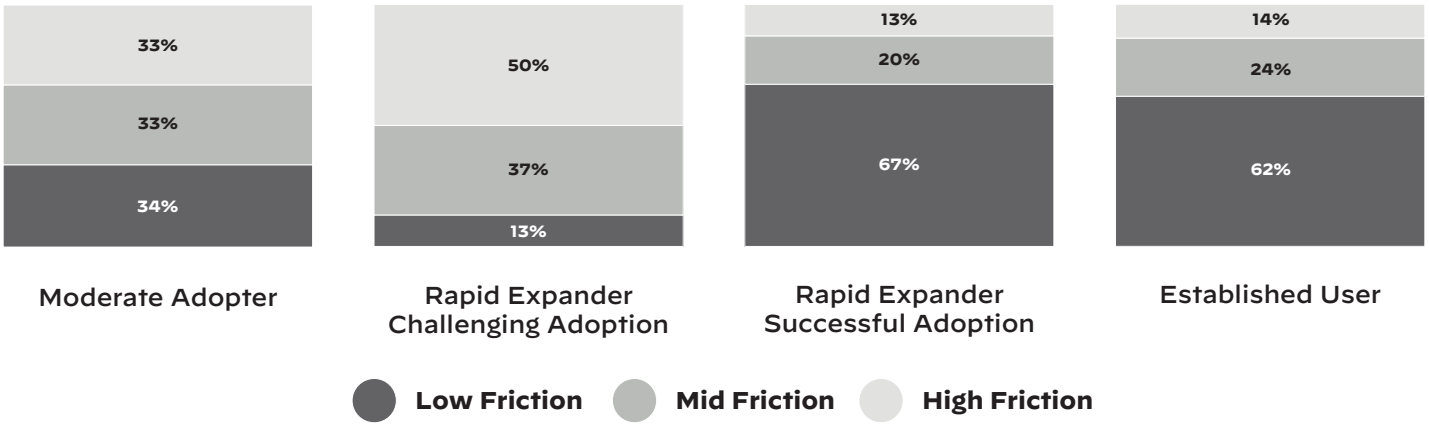


Figure 35: Amount of organizational friction across adoption groups

While organizations used a range of security providers, Rapid Expanders who experienced challenges tended to leverage more open source security providers. **By contrast, those who were successful in their rapid cloud expansion avoided open source and balanced security sourcing, with 87% focusing on either CSP- or third-party-driven security.**

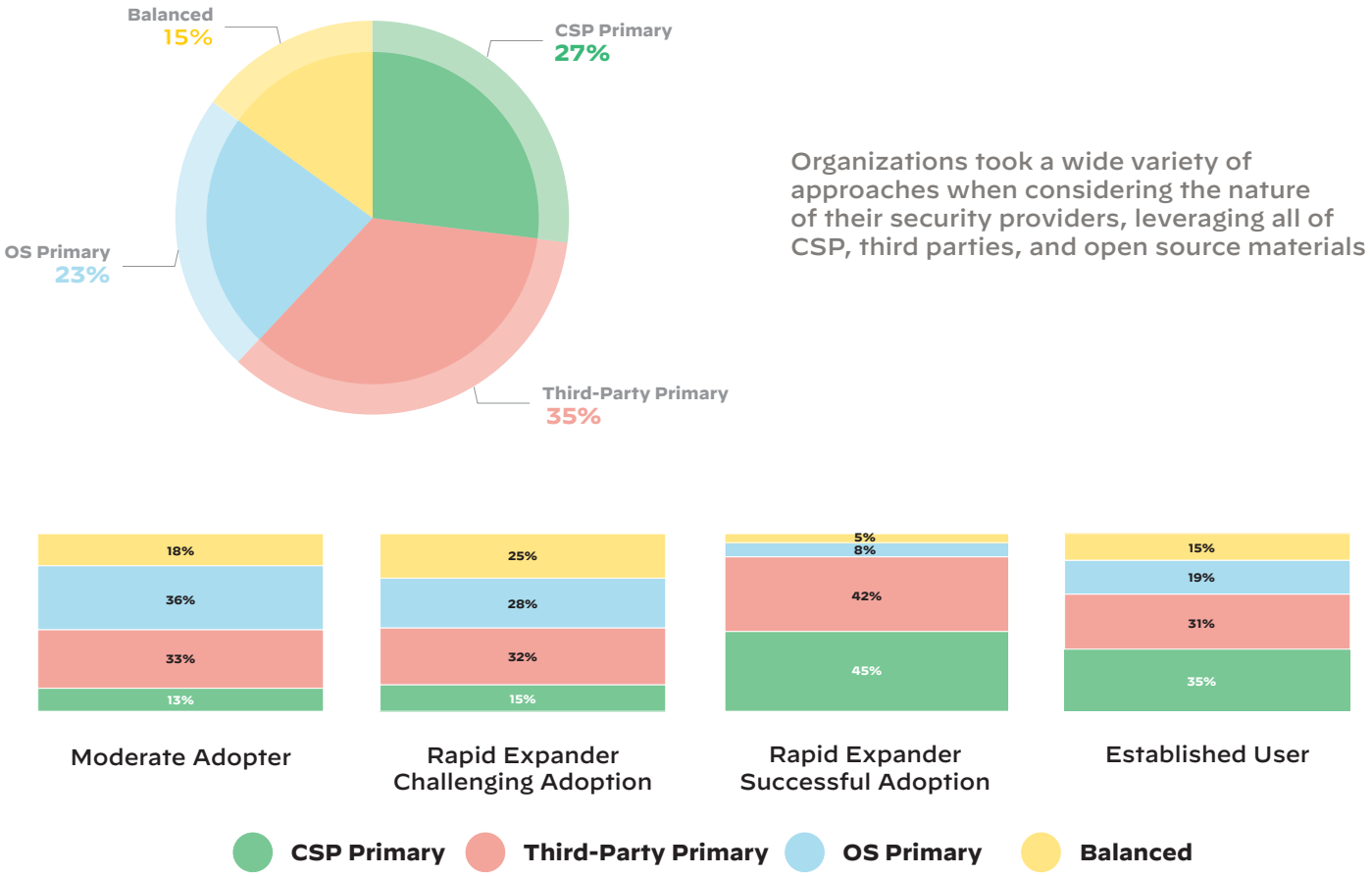


Figure 36: Primary tool provider overall (top) and across adoption groups (bottom)

The divide between Rapid Expanders allowed us to explore what makes a successful rapid expansion to the cloud. In summary, we have learned the following:

- High cloud spend does not equate to successful cloud adoption.
- Integrating cloud adoption into a wider strategic digital transformation effort is key to success.
- Consolidation of security vendors who offer a plethora of security tools leads to successful cloud adoption efforts.
- Larger security teams do not equate to a more secure organization.
- DevSecOps integration and security automation are necessary components to achieving successful cloud adoption.
- CSP- or third-party-driven security providers offer the highest chance of successful and secure cloud adoption.

Final Thoughts

The pandemic put a distinctive mark on this year's State of Cloud Native Security Report, and we expect to see its impact continue. Despite rapid changes in business strategies and resources, however, organizations have mostly been able to succeed in their cloud expansions during this time of upheaval. Even with today's complex, heterogeneous cloud environments—which incorporate a mix of public and private clouds, diverse compute compositions, and a growing number of cloud service providers—our research indicates a proven path forward.

Overall, **organizations that made cloud infrastructure a strategic focus across the business were more successful**. Further, **cloud security is a clear enabler of business outcomes**. For any type of organization, anywhere in the world, security best practices are consistent and can be implemented as key drivers for cloud success. Of course, better security does not necessarily lead to a specific measurement. But having security under control—consolidating tools and vendors as well as using proven DevSecOps and security automation strategies—sets a baseline that lets development teams do their jobs better and enables organizations to succeed in their cloud transformations.

Methodology and Demographics

This survey was administered online, and data was gathered from May 3 to June 1, 2021. Respondents were surveyed from across the globe, spanning the US, Germany, the UK, Brazil, and Japan. This population also included all major industries, with significant representation from consumer products and services, energy resources and industrials, financial services, technology media and telecommunication, and life services and healthcare. Over two-thirds are from enterprise-sized organizations (over $1B in annual revenue), and respondents were gathered from both ends of the organizational spectrum—the sample split between executive leadership and more practitioner-level roles in order to understand sentiments broadly across companies. Practitioner-level respondents were restricted to those who work in development, IT or information security functions. Respondents were sourced from professional survey panels, and all respondents reported themselves knowledgeable and familiar with their organization's cloud operations and cloud security.

About

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Prisma Cloud

Prisma® Cloud is a comprehensive cloud native security platform with the industry's broadest security and compliance coverage—for applications, data, and the entire cloud native technology stack—throughout the development lifecycle and across multicloud and hybrid deployments. Prisma Cloud's integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud native application development and deployment securely. For more information, visit www.paloaltonetworks.com/prisma/cloud.

PRISMA CLOUD | paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com