The State of Cloud Network Security: 2025

AVIATRIX

Contents

Executive Summary

Whatever security tools and protocols you and your organization put in place a few years ago are either at their breaking point or soon will be. It's not just that modern enterprise infrastructures have become highly complex ecosystems that require disparate teams and a wide range of skill sets to operate. Complexity simply implies that there's more to manage; and while that is happening, there's also something else going on–these infrastructures are rapidly metamorphosing in fundamental ways:

- → **The lines between trusted and untrusted environments have blurred.**
  What was once "internal" traffic within a trusted data center now frequently traverses public infrastructure, creating vast, unmonitored attack surfaces.
- → **The perimeter has become exponentially distributed.**
  Enterprises now face thousands of micro-perimeters around every workload, VPC, cloud region, and third-party connection, each requiring consistent security enforcement.
- → **Applications are ephemeral and deeply distributed.**
  Modern applications operate as transient ecosystems of ephemeral components (VMs, containers, and serverless functions) that rapidly cycle across multiple clouds, creating complex dependencies and an ever-shifting attack surface. This change is aggravated by enterprise mandates to rapidly adopt agentic AI, fueling a "shadow AI" crisis that mirrors cloud-era "shadow IT."

All of this is breaking down even the best laid security plans.

Aviatrix fielded a comprehensive survey to understand the current state of cloud network security–how organizations are handling the complexity and the foundational changes, and how network security fits into organizations' broader cloud initiatives.

The study uncovered several key trends that can help organizations focus their investments and efforts to improve cloud security.

Key findings:

- ✓ **Widely adopted cloud firewalls are challenging to implement and integrate.**
- ✓ **Zero trust remains theoretical without solving for existing gaps.**
- ✓ **Blind spots remain a large threat in cloud network security.**
- ✓ **Companies lack transparency into legacy cloud firewall costs.**
- ✓ **DevOps security and east-west traffic controls are non-existent or lagging.**
- ✓ **AI adoption in security is high.**

Additional findings shed light on systemic operational risks. A majority of respondents (69%) report a shortage of skilled security personnel, raising concerns about the capacity to manage increasingly complex cloud environments. Unexpected costs tied to cloud firewalling impact 63% of organizations–some reporting overruns of nearly $500,000. Adoption of zero trust architectures for securing inter-region and inter-cloud traffic remains minimal, at just 8%, highlighting a gap between strategic security goals and current implementation. These trends underscore the need for scalable, cost-transparent, and operationally simplified approaches to multicloud security. Further insights include:

Organizations report a high level of confidence in existing **cloud security controls**, but this doesn't mean there aren't weak links or opportunities for improvement within the network fabric itself–the foundational layer where workloads communicate and threats propagate. They must be realistic about ever-changing security vulnerabilities and business risks, and continually evolve their protections and processes accordingly.

A unified approach across **hybrid/ multicloud environments**–for management, visibility, policy enforcement, and more–is critical, not just for reducing complexity, but for boosting an organization's security posture.

Organizations should not underestimate the complexity of **cloud firewall solutions** and the potential problems that can lead to. Consider solutions that offer advanced security capabilities with centralized management.

Sensitive data needs to be encrypted both in transit and at rest, and organizations that have not already done so should audit their **encryption** practices and update their strategies as needed.

There is significant room for improvement in **cloud networking** operations to identify and mitigate problems, both internal and external, before they lead to outages.

Organizations are struggling with **cloud talent** shortage. They will need to look for alternative ways to set their cloud strategies up for success, which could include training and certification, automation, AI and ML, and other approaches.

Despite having a good grasp on overall **cloud networking costs**, organizations need to be able to allocate costs to business units or applications based on actual usage.

Key Findings

- Widely adopted cloud firewalls are challenging to implement and integrate
- Zero trust remains theoretical without solving for existing gaps
- Blind spots remain a large threat in cloud network security
- Companies lack transparency into legacy cloud firewall costs
- DevOps security and east-west traffic controls are non-existent or laggingx
- AI adoption in security is high

Widely adopted cloud firewalls are challenging to implement and integrate

Nearly all (91%) of U.S. respondents use firewalls provided by their cloud service provider (CSP), but 64% also deploy third party solutions (Figure 1). Despite this widespread adoption, two out of three respondents (67%) struggle to integrate these tools effectively within their broader security stack. And there are additional operational friction points that affect scaling and performance, with 55% of respondents experiencing performance overhead, and half citing scalability challenges (Figure 2). This indicates that native tools alone are often insufficient to meet the demands of modern, distributed environments.

Figure 1

Cloud firewall solutions currently deployed

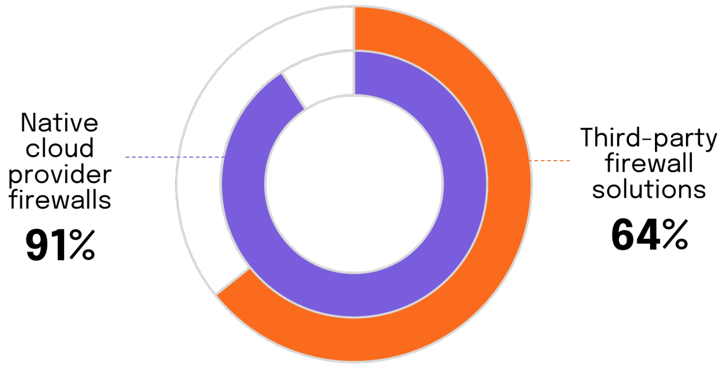
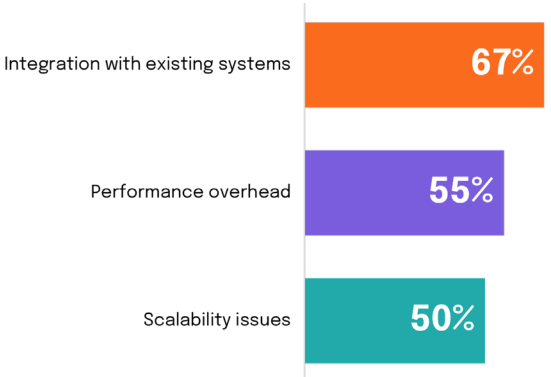


Figure 2

What challenges have you faced in implementing cloud firewall solutions?



2/3 OF RESPONDENTS

struggle to integrate cloud security tools effectively within their security stack.

ACTIONABLE INSIGHT

Multi-vendor, fragmented setups are a challenge.

This can create dangerous security gaps, so organizations need to find approaches to unify their protection across clouds to eliminate integration headaches.

Zero trust remains theoretical without solving for existing gaps

There is a major misalignment between zero trust awareness and actual implementation when it comes to securing traffic between clouds. Only 8% of U.S. respondents use zero trust architectures for securing inter-cloud traffic (Figure 3). This low adoption rate highlights a growing maturity gap. While zero trust is a strategic priority for many organizations, implementation remains elusive–especially in multicloud and inter-region contexts where legacy access models still prevail. A similar trend appears in API security, where just 29% of respondents report using zero trust API security models (Figure 4).

Figure 3

Use of zero trust architectures to secure traffic between cloud regions and providers

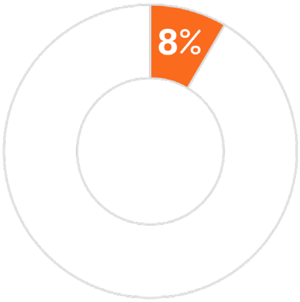
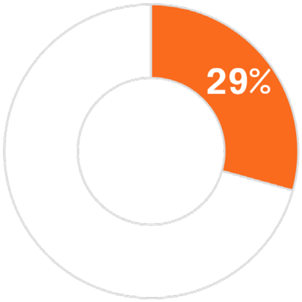


Figure 4

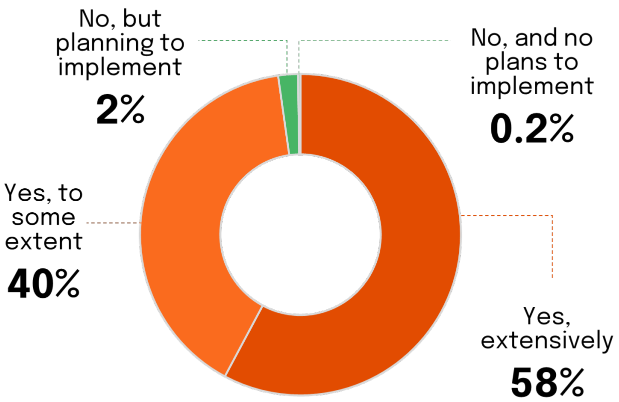
Use of zero trust API security models to secure APIs in the cloud



Microsegmentation fares better, with 58% of respondents deploying it extensively, but 42% are still immature or not yet adopting it (Figure 5).

Figure 5

Does your organization enforce microsegmentation for cloud security?



ACTIONABLE INSIGHT

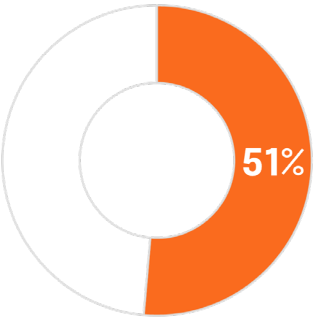
Organizations need to look for ways to operationalize and enforce zero trust across their clouds to bring adoption from theoretical to practical–ideally without requiring disruptive rip-and-replace.

Blind spots remain a large threat in cloud network security

More than half of U.S. respondents call out network traffic visibility as an area needing improvement (Figure 6).

Figure 6

Visibility into network traffic is the security capability that needs the most improvement



ACTIONABLE INSIGHT

Real-time embedded observability across multicloud environments is critical for closing persistent visibility gaps.

So, what are respondents currently using? Only 20% leverage third-party threat intelligence feeds, indicating limited reliance on external context for security monitoring (Figure 7). While more than half (56%) use third-party observability platforms, 76% lean on native cloud tools, which means they are relying on basic telemetry (Figure 8).

Figure 7

Use of third-party threat intelligence feeds to monitor cloud security threats in real-time

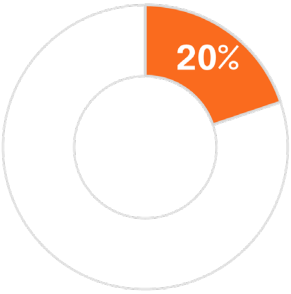
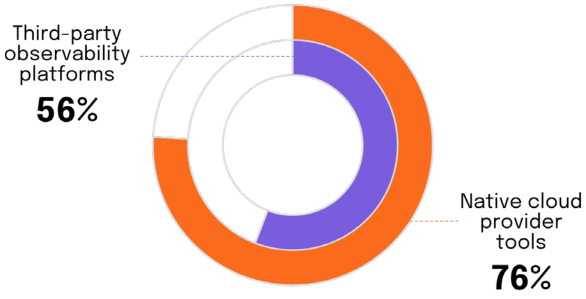


Figure 8

Tools or platforms used for monitoring and managing cloud network activities



This reliance on multiple tools illustrates the fragmentation and overhead many teams face. The absence of an integrated, multicloud-aware observability layer limits both responsiveness and scalability.

Companies lack transparency into legacy cloud firewall costs

About two-thirds (63%) of U.S. respondents faced unexpected firewall costs in the past year (Figure 9). Of those respondents, 69% were on the hook for more than $50,000 in unexpected costs and 35% for more than $100,000 (Figure 10).

Figure 9

Have you ever encountered unexpected costs related to cloud firewall implementations in the last 12 months?

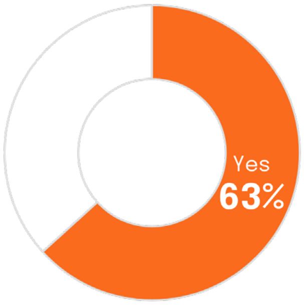
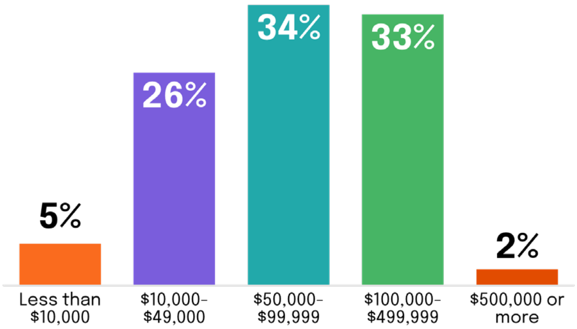


Figure 10

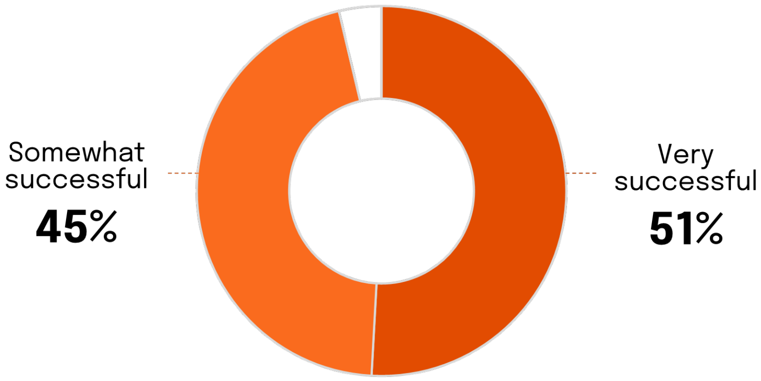
What was the approximate amount of these unexpected costs?



Interestingly, these cost overruns come despite high confidence levels in forecasting spend—94% of respondents rate their forecasting accuracy as good or very good. This contradiction may stem from hidden costs within licensing models, usage-based pricing, or underestimating operational complexity during deployment (Figure 11).

Figure 11

How successful are you in forecasting cloud security costs?



2/3 OF RESPONDENTS

faced over $50,000 in unexpected firewall costs in the past year.

ACTIONABLE INSIGHT

Putting an end to cloud firewall sticker shock requires transparent pricing and a cost-aware architecture.

DevOps security and east-west traffic controls are non-existent or lagging

Almost half (46%) of U.S. respondents face major challenges securing DevOps pipelines, with another 39% experiencing minor issues (Figure 12), and more than half (52%) report difficulty managing east-west traffic–i.e., communication between services within the same Kubernetes cluster–for cloud-native apps (Figure 13).

Figure 12

Has your organization faced challenges with securing DevOps pipelines in the cloud?

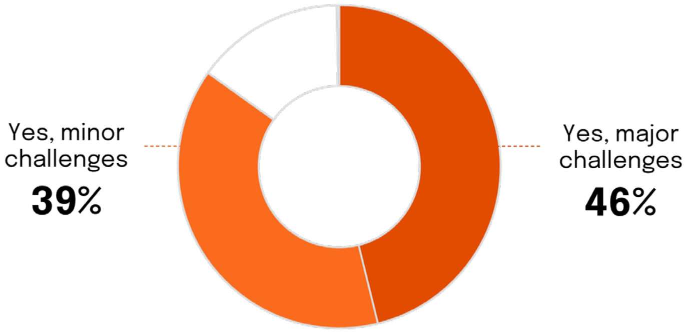
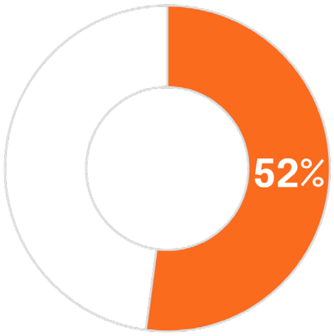


Figure 13

Managing east-west traffic security is a challenge with cloud native applications



These challenges suggest that while Kubernetes-native controls are widely deployed, they often lack the cross-environment policy enforcement and traffic visibility necessary to secure service-to-service communications.

50%+

report difficulty managing east-west traffic for cloud-native apps.

ACTIONABLE INSIGHT

Cloud-native security shouldn't mean fractured policies.

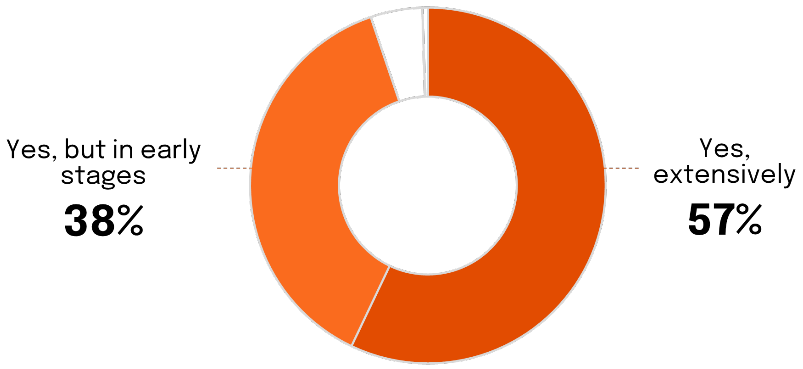
Enterprises need to ensure consistent protection across IaaS and Kubernetes environments.

AI adoption in security is high

The vast majority of respondents (95%) are leveraging artificial intelligence and/or machine learning for threat detection, with 57% doing so extensively (Figure 14).

Figure 14

Is your organization leveraging AI or machine learning for cloud security threat detection?



95%

leverage artificial intelligence and/or machine learning for threat deteciton

ACTIONABLE INSIGHT

As organizations continue to evaluate different tools in their cloud security stack, they should review AI and ML capabilities for intelligent traffic analysis, automated policy enforcement, etc.

Full Results

The current state of:

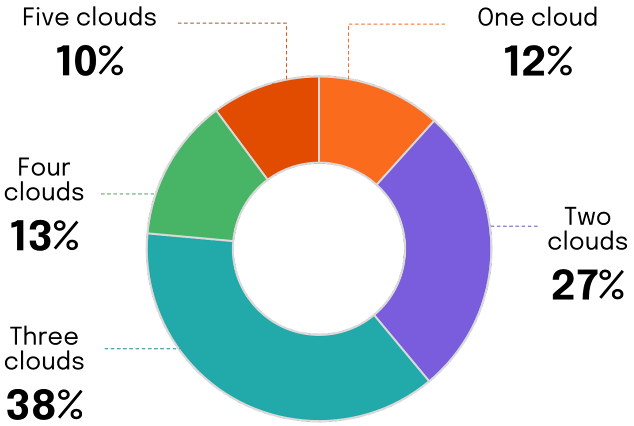
- ✓ Hybrid/multicloud
- ✓ Cloud network security postures and controls
- ✓ Cloud firewalls
- ✓ Encryption
- ✓ Cloud networking
- ✓ Cloud talent
- ✓ Cloud costs

The current state of hybrid/multicloud

Multicloud is the norm, with the vast majority of organizations (88%) using more than one CSP and 61% are using three or more CSPs (Figure 15). Microsoft Azure is the top cloud in use by 80% of U.S. respondents, though use of Google Cloud and AWS continue to be widespread–73% and 61% respectively (Figure 16).

Figure 15

Number of cloud service providers currently being utilized

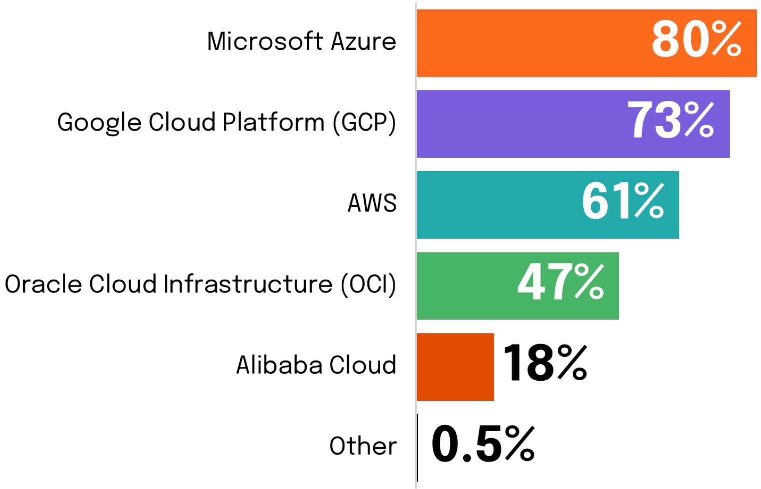


61%

use more than 3 CSPs, with Microsoft Azure the most commonly used.

Figure 16

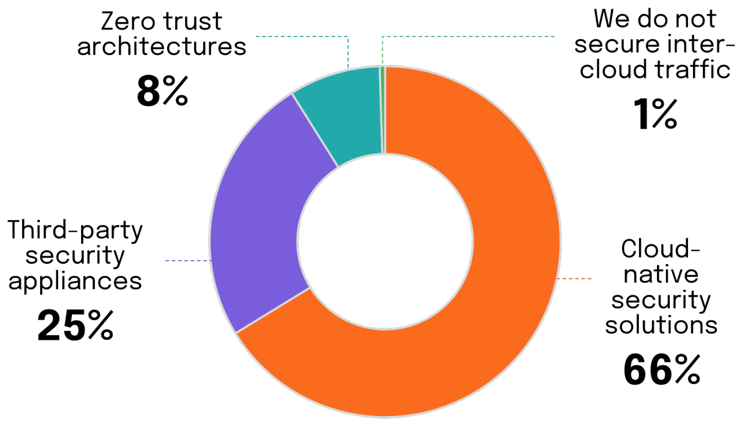
Which cloud service provider(s) does your organization currently use?



Given the prevalence of multicloud, how are organizations securing their traffic? Two-thirds (66%) are relying on their cloud-native security solutions, while one-quarter (25%) have invested in third-party security appliances (Figure 17). Even with these tools, respondents are still facing challenges when it comes to securing workloads in a multicloud environment. In particular, 35% struggle with managing multiple security tools, and 30% have compliance complexity (Figure 18).

Figure 17

How does your organization secure traffic between cloud regions and providers?

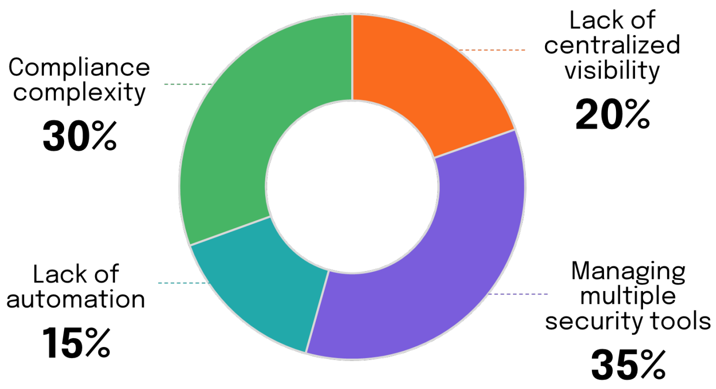


66%

rely on cloud-native security solutions.

Figure 18

What is the biggest barrier to securing workloads in a multicloud environment?



Top challenges

1. Multiple security tools
2. Compliance complexity
3. Lack of centralized visibility

Of course, organizations aren't just multicloud; respondents are also running hybrid cloud environments, adding yet another layer of complexity to their operations. Nearly half (49%) say they're struggling with consistently enforcing cloud security across their hybrid and on-premises environments, while 59% are simply handling policy enforcement separately (Figure 19). And 78% say managing hybrid connectivity in a multicloud environment is somewhat or very complex (Figure 20).

Figure 19

How are you handling cloud security for hybrid and on-premises environments?

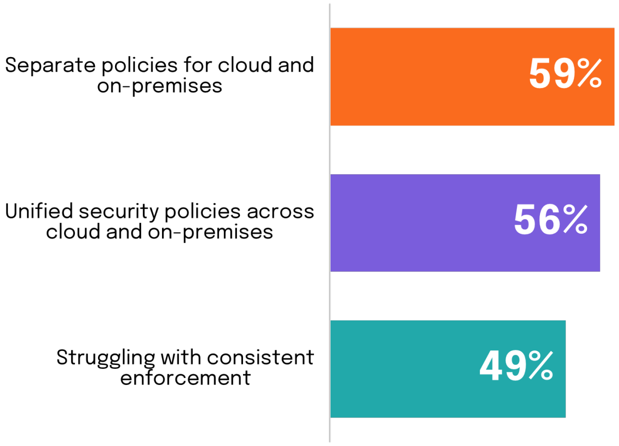
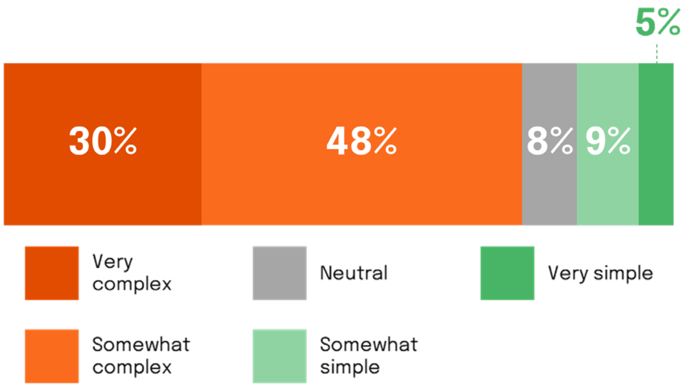


Figure 20

How would you rate the complexity of managing hybrid cloud connectivity in a multicloud environment?



78%

report that managing hybrid connectivity in a multicloud environment is complex.

ACTIONABLE INSIGHT

A unified approach across hybrid / multicloud environments–for management, visibility, policy enforcement, and more–is critical, not just for reducing complexity, but for boosting an organization's security posture.

The current state of cloud network security postures and controls

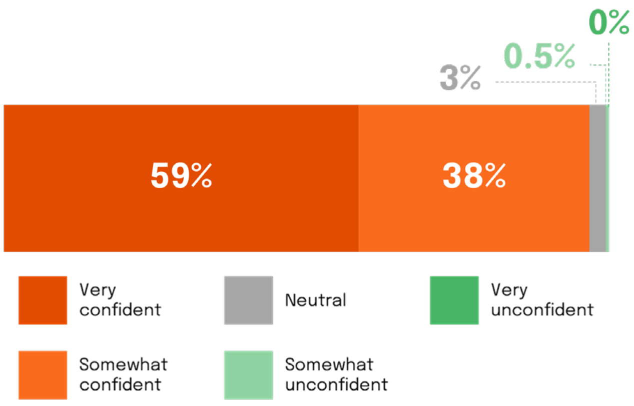
Virtually all U.S. respondents (95%) are confident in their ability to detect and respond to threats for cloud workloads, with well over half—59%—saying they are very confident (Figure 21).

59%

are very confident in detecting and responding to cloud workload threats.

Figure 21

How confident are you in your organization's ability to detect and respond to threats for cloud workloads?



So, what controls and practices do they have in place that give them such high levels of confidence? We asked about a variety of approaches. Microsegmentation and secure access service edge (SASE) are seeing similar high levels of adoption—58% of respondents are all in on both approaches, and a somewhat smaller number (40% for microsegmentation and 37% for SASE) have some level of implementation (Figure 22, Figure 23).

Figure 22

Does your organization enforce microsegmentation for cloud security?

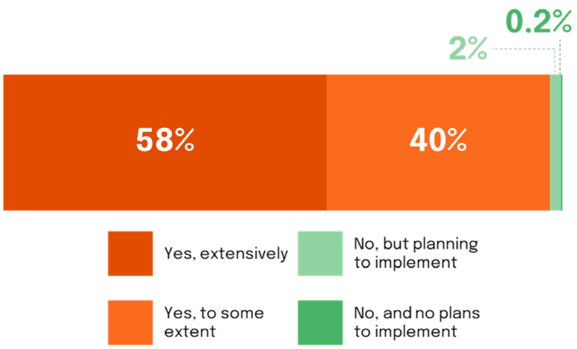
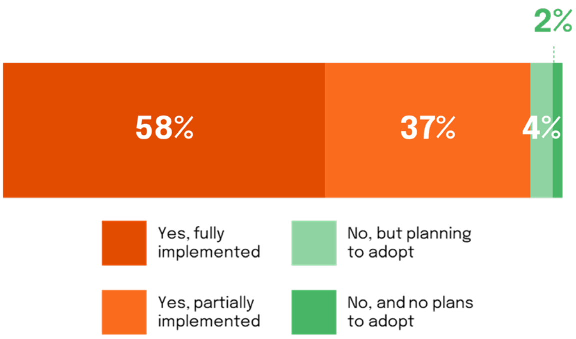


Figure 23

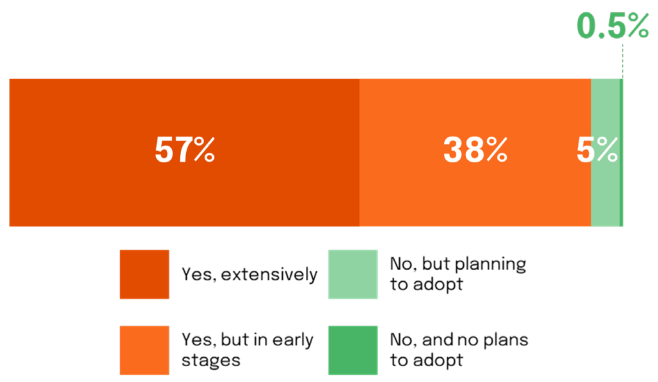
Has your organization adopted secure access service edge (SASE) frameworks?



Another technology that enterprises have fully invested in for cloud security threat detection is AI/ML. While 38% are still in the early stages, 57% are using it extensively today (Figure 24).

Figure 24

Is your organization leveraging AI or machine learning for cloud security threat detection?



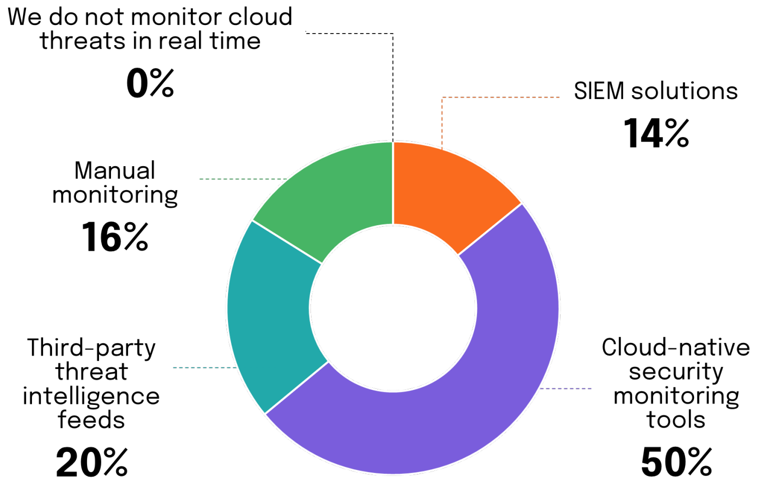
Over 50%

extensively use AI and machine learning for cloud security threat detection.

When it comes to real-time threat monitoring, half of respondents rely on cloud-native security monitoring tools, while only 20% leverage third-party threat intelligence tools (Figure 25).

Figure 25

How does your organization monitor cloud security threats in real time?



There are a couple of threat vectors that can be overlooked or underestimated: insider threats and APIs. While 99% of respondents have insider threat protections, many rely on encryption and data masking (60%), zero trust access policies (58%), and user behavior analytics (58%) (Figure 26). Similarly, 98% of respondents have API security in place, with the most common approach, cited by 43% of respondents, being web application firewalls (WAFs) (Figure 27).

Key threat vectors

1. Insider threats
2. APIs

Figure 26

What security measures does your organization use to protect against insider threats in the cloud?

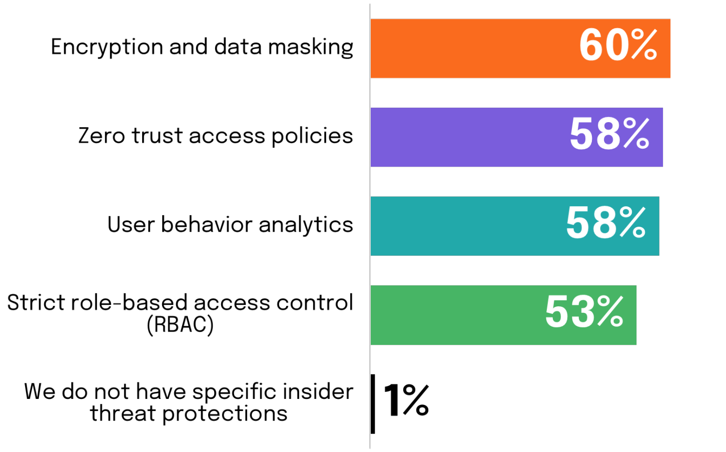
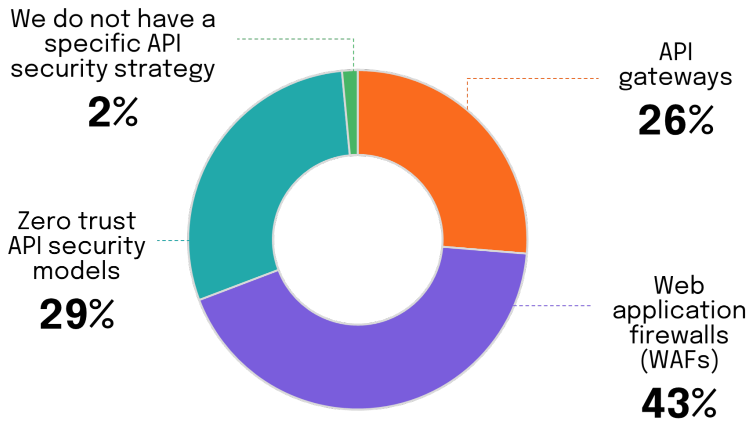


Figure 27

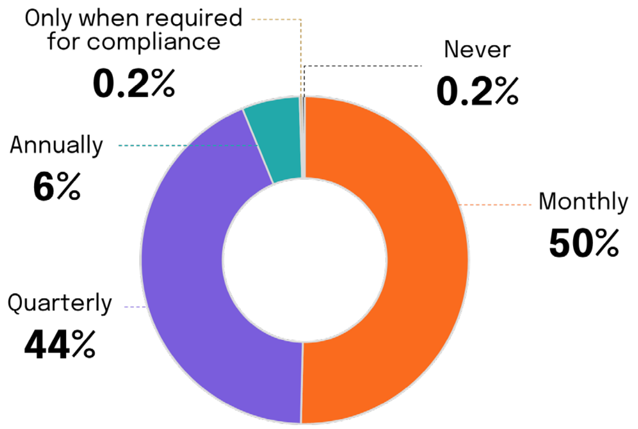
What is your organization's approach to securing APIs in the cloud?



While it's important to have robust security tools and processes in place, it's also critical to audit those controls and practices on a regular basis. The good news is that 94% are doing so more than once a year, with 44% performing audits quarterly and 50% monthly (Figure 28).

Figure 28

How often does your organization conduct cloud security audits?



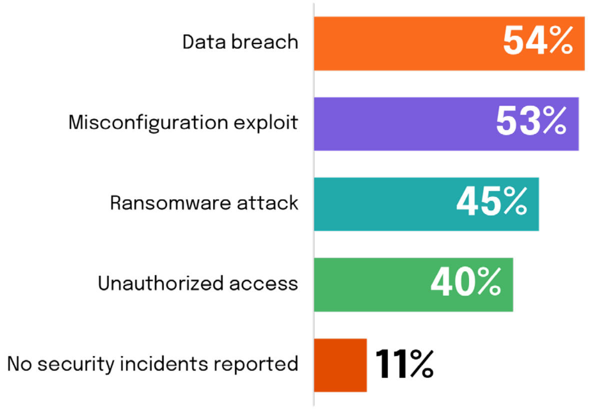
94%

audit controls and practices on at least an annual basis.

Despite the high levels of confidence and the variety of protections in place, however, organizations are still facing a number of challenges and concerns. There is simply no way to fully bulletproof any IT environment, and 89% of respondents say they have experienced some kind of security incident in the past year, with data breaches and misconfiguration exploits being the most common (54% and 53% respectively) (Figure 29).

Figure 29

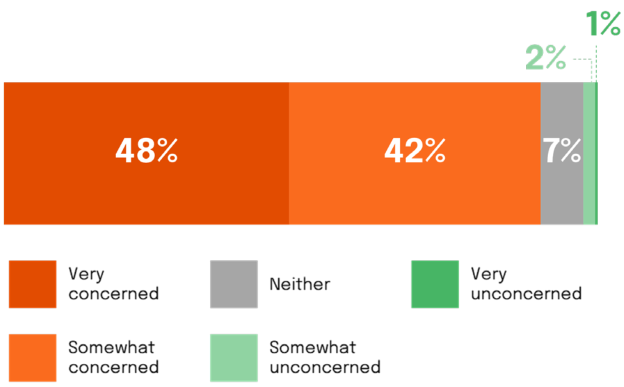
Which of the following cloud security incidents has your organization experienced in the last 12 months?



Security breaches can have a wide variety of consequences, including significant financial impact–a worry for 90% of respondents, with nearly half (48%) expressing a high level of concern (Figure 30).

Figure 30

How concerned are you about the financial impact of future security breaches?



90%

are concerned with the financial impact of security breaches.

What's interesting is that when asked which cloud security capabilities need the most improvement, respondents did not have a strong consensus–there's only a 12-point difference between the most-cited (automation of security policies at 57%) and the least-cited (compliance enforcement, 45%) (Figure 31). When it comes to the security challenges of cloud-native applications, there's only a 5-point spread (Figure 32).

Figure 31

Which cloud security capabilities do you believe need the most improvement?

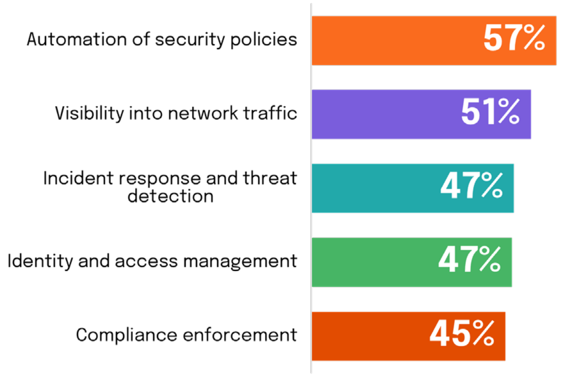
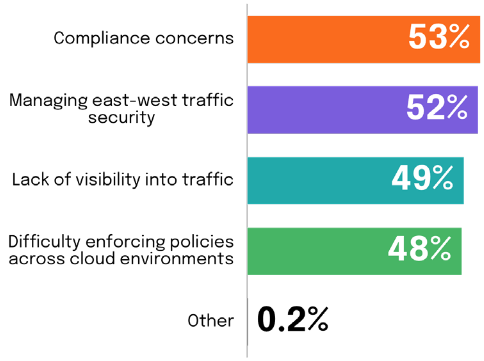


Figure 32

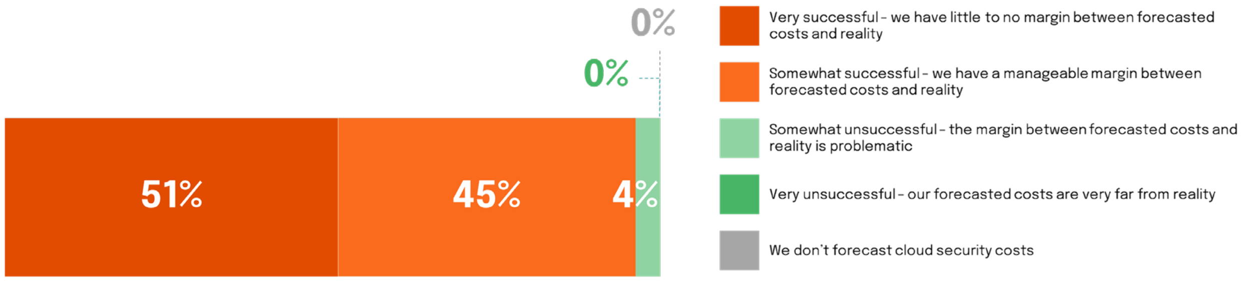
What security challenges is your organization facing with cloud-native applications?



Cloud security is clearly a job that's never finished. But it also can't be managed at any cost—all organizations have budget and resource limitations. When it comes to cloud security costs, 96% of respondents are forecasting with a reasonable degree of accuracy, with over half (51%) saying their forecasts are highly accurate (Figure 33).

Figure 33

How successful are you in forecasting cloud security costs?



That's good news, but cloud security also needs to be effective without impeding the business. Most respondents (85%) say they've been challenged with securing DevOps pipelines in the cloud, with 46% qualifying those challenges as major (Figure 34). Furthermore, 67% say that security reviews are creating service deployment delays (Figure 35).

Figure 34

Has your organization faced challenges with securing DevOps pipelines in the cloud?

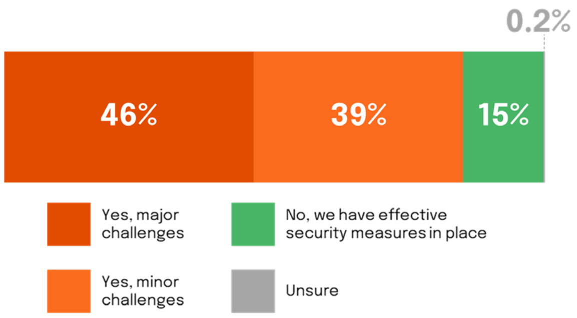
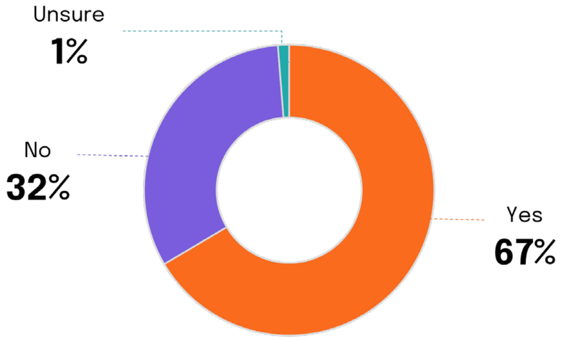


Figure 35

Has your organization faced delays to service deployment in the cloud as the result of security reviews?



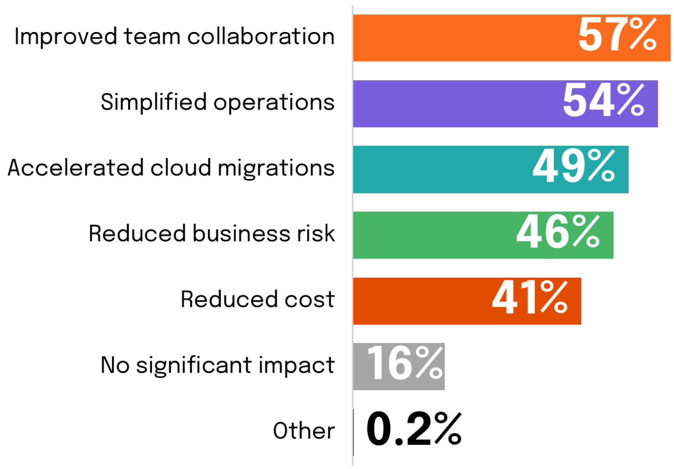
67%

report that security reviews delay service deployments.

Despite these challenges, there are positive business benefits resulting from the convergence of networking and security in the cloud, most notably improved team collaboration (57%) and simplified operations (54%) (Figure 36).

Figure 36

How has the convergence of networking and security in the cloud impacted your operations?



ACTIONABLE INSIGHT

A high level of confidence in existing cloud security controls doesn't mean there aren't weak links or opportunities for improvement.

Organizations should be realistic about ever-changing security vulnerabilities and business risks, and continually evolve their protections and processes accordingly.

The current state of cloud firewalls

All of the respondents surveyed are using cloud firewalls, and virtually all (91%) are leveraging the firewalls provided by their CSPs, with two-thirds (64%) also using third-party firewall solutions (Figure 37). In fact, 75% of respondents are using two or more types of cloud firewall solution (Figure 38).

Figure 37

Which cloud firewall solutions are currently deployed in your environment?

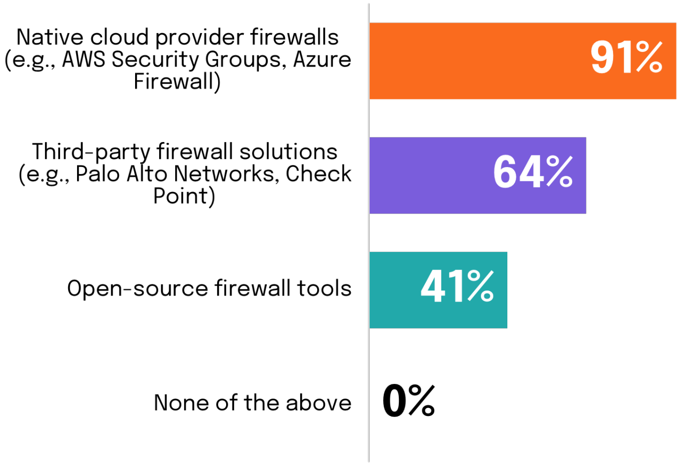
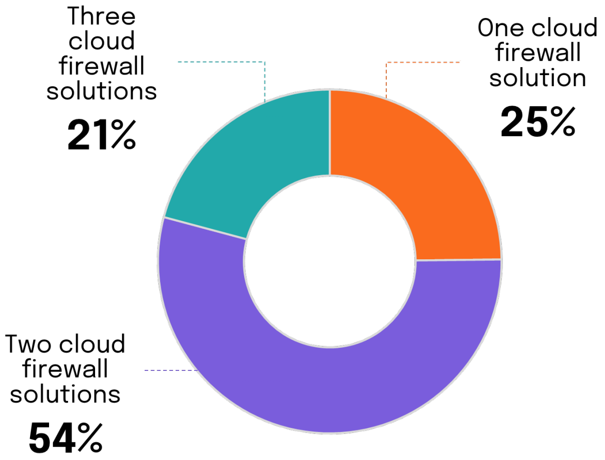


Figure 38

Number of cloud firewall solutions currently deployed



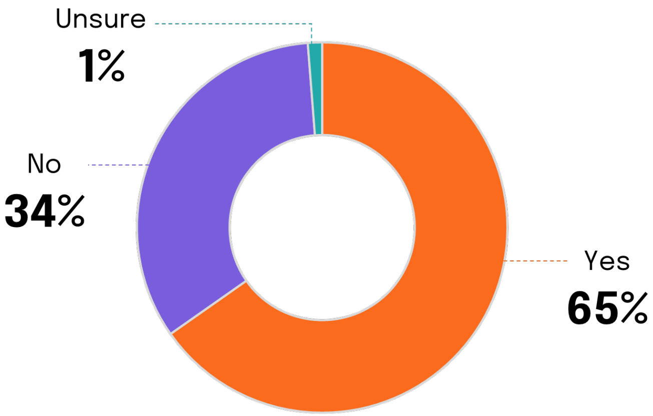
75%

use two or more types of cloud firewall solution.

For cloud firewalls to provide optimal protection–and comply with all relevant regulatory requirements–they have to be configured correctly. This is clearly easier said than done, as 65% of respondents say that misconfigurations in cloud firewall settings led to security breaches in the past year (Figure 39). It is therefore interesting to note that despite the security incidents related to misconfigurations, 96% of respondents state they are confident that their cloud firewall configurations align with new compliance requirements, and 59% are highly confident (Figure 40).

Figure 39

Have you experienced any security breaches in the past 12 months due to misconfigurations in cloud firewall settings?

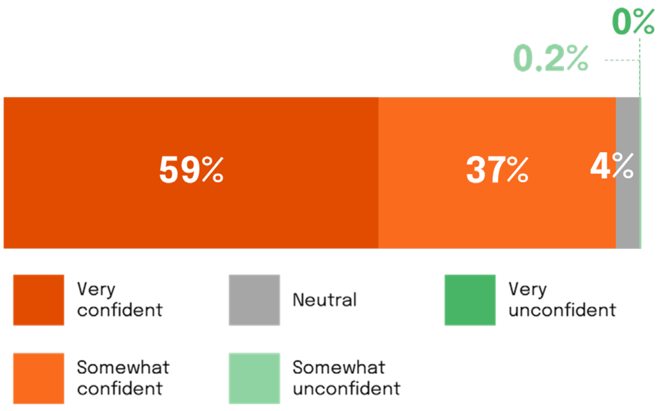


65%

report cloud firewall misconfigurations resulted in security breaches.

Figure 40

How confident are you that your cloud firewall configurations align with new compliance requirements (DORA, updates to HIPAA, NIST, etc.)?



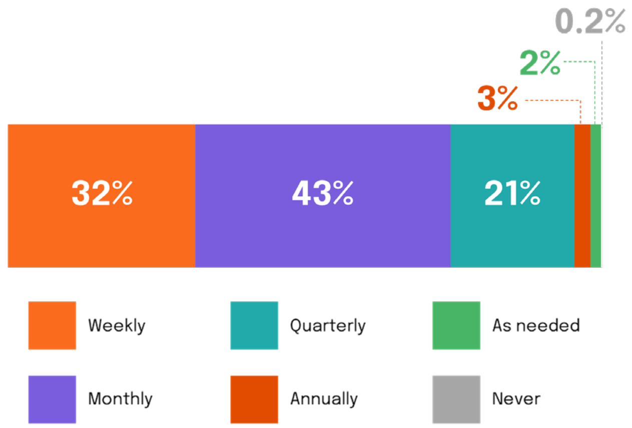
96%

are confident that their cloud firewall configurations align with compliance requirements.

Perhaps this confidence comes, at least in part, from the fact that respondents frequently review and update their cloud firewall rules and policies–95% do so more than once a year, and about one-third (32%) have a weekly cadence (Figure 41).

Figure 41

How often does your organization review and update cloud firewall rules and policies?



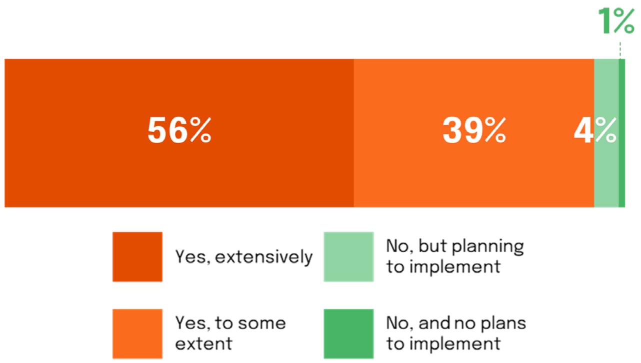
95%

review and update cloud firewall rules and policies more than once a year.

Firewalls are also important in Kubernetes environments to secure network traffic between containers and pods and the broader internet. These specialized firewalls are used by 95% of respondents today, with 56% doing so extensively (Figure 42).

Figure 42

Is your organization utilizing Kubernetes firewall solutions (e.g. network policies, service mesh) to secure containerized applications?



95%

utilize Kubernetes firewall solutions to secure containerized applications.

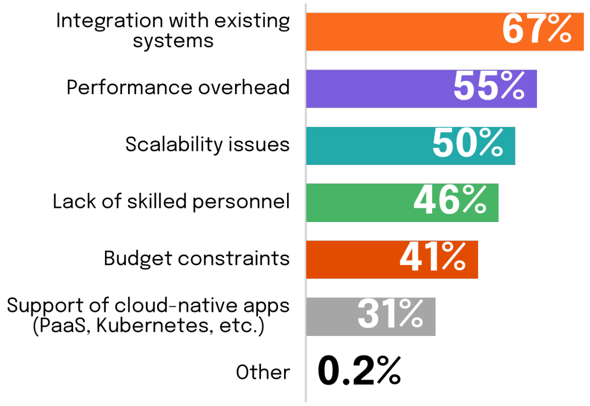
Despite the value and prevalence of cloud firewalls, they can be complex to understand and deploy. There are a host of challenges companies face during implementation. The biggest, experienced by two-thirds of respondents (67%), is integrating them with existing systems. Other significant challenges are performance overhead (55%) and scalability issues (50%) (Figure 43).

Top challenges

1. Integration within systems
2. Performance overhead
3. Scalability issues

Figure 43

What challenges have you faced in implementing cloud firewall solutions?



Native cloud firewalls are ubiquitous, but they are not without challenges. There are some widespread misconceptions that can lead to serious performance, security, cost, operational complexity, and compliance challenges, as well as project delays. All of these issues are experienced at similar rates: 44–52% of respondents (Figure 44). Worse, they're not facing just one of these issues—93% of respondents that have run into problems experienced two or more issues, and 66% had to deal with three or more issues (Figure 45).

Figure 44

Have assumptions about native cloud firewall capabilities led to any of the following issues?

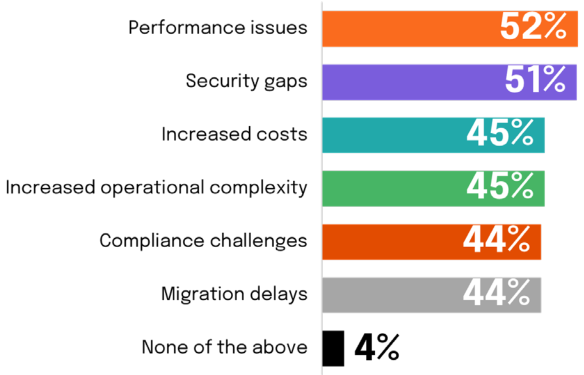
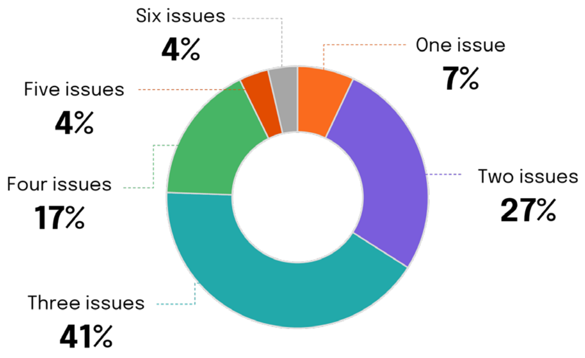


Figure 45

Number of issues experienced due to assumptions about native cloud firewall capabilities



While 45% of respondents say that increased costs were an issue with native cloud firewalls, 63% report seeing unexpected costs related to their overall cloud firewall implementation over the past year (Figure 46). And those costs add up, with 69% spending more than $50,000 and 35% spending more than $100,000 above what they had planned (Figure 47).

Figure 46

Have you encountered unexpected costs related to cloud firewall implementations in the past 12 months?

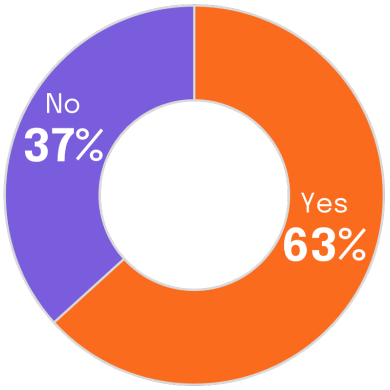
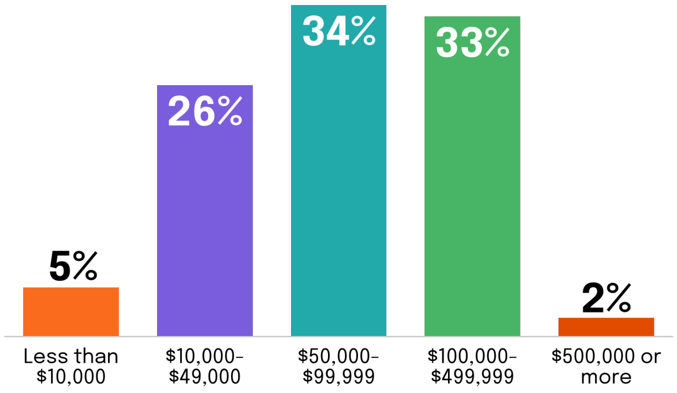


Figure 47

What was the approximate amount of these unexpected costs?



63%

report unexpected costs related to cloud firewall implementations.

ACTIONABLE INSIGHT

Don’t underestimate the complexity of cloud firewall solutions and the potential problems it can lead to.

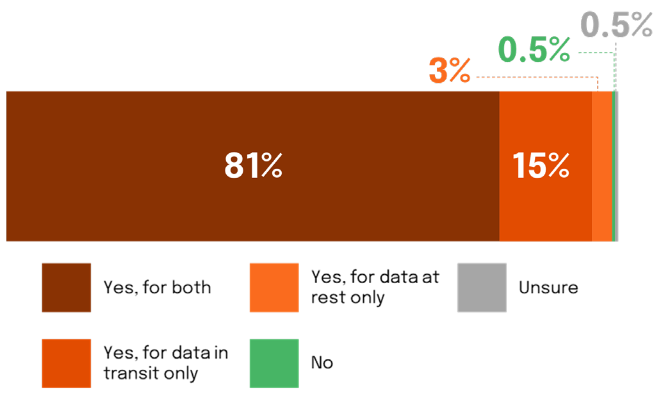
Consider solutions that offer advanced security capabilities with centralized management.

The current state of encryption

Encryption is a critical security control to safeguard data privacy and integrity, both while in transit and at rest. But are enterprises encrypting in both cases? Most (81% of respondents) are, but while a mere 3% are only encrypting data at rest, a not insignificant 15% are only encrypting in-transit data (Figure 48).

Figure 48

Does your organization employ encryption for data in transit and at rest within your cloud environment?



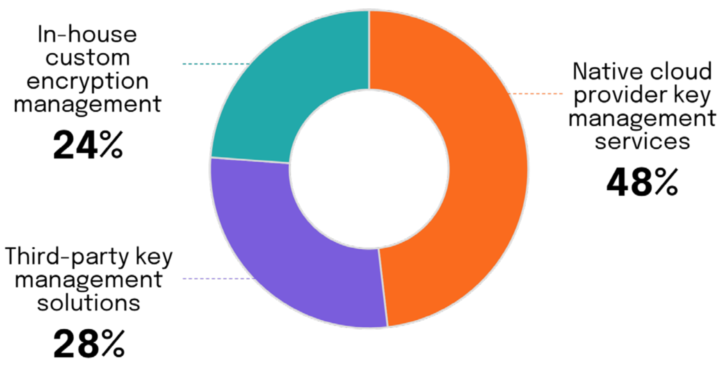
81%

encrypt both data in transit and at rest.

A critical component of encryption is key management and there are different approaches enterprises can take. Almost half of respondents (48%) rely on key management services from their cloud provider; the remaining are fairly evenly split between third-party tools (28%) and in-house custom solutions (24%) (Figure 49).

Figure 49

How does your organization handle encryption key management for cloud security?



48%

rely on cloud provider key management services.

Because of the heterogenous nature of hybrid/multicloud environments–and the fact that there are different "owners" of the systems through which the data travels–it can be difficult to ensure full encryption at every point, a challenge that has been highlighted by recent encryption-related events such as Salt Typhoon. In fact, these headlines have prompted nearly all organizations to undertake an audit of their encryption protocols–and they've done so with a sense of urgency, with 50% having already completed the audits and another 40% currently in progress (Figure 50). Furthermore, these much-publicized events have spurred 97% of respondents to reevaluate their broader cloud security strategies (Figure 51).

Figure 50

Following recent encryption-related news (e.g., Salt Typhoon), have you audited your encryption protocols?

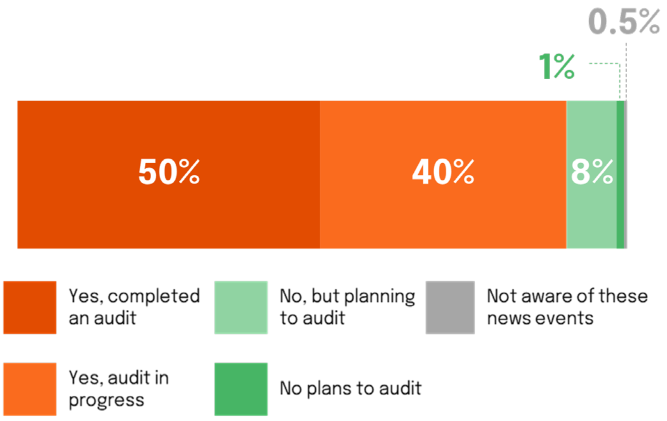
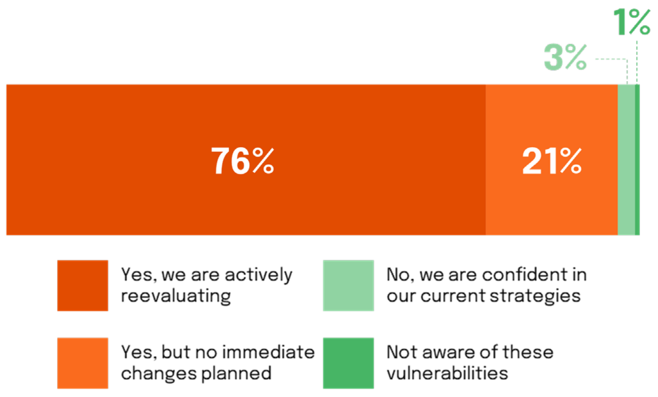


Figure 51

In light of recent encryption vulnerabilities (e.g., Salt Typhoon breach),is your organization reevaluating its cloud security strategies?



90%

either already completed or are in the middle of an audit following encryption-related news events.

ACTIONABLE INSIGHT

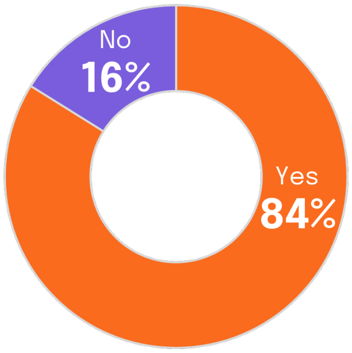
Sensitive data needs to be encrypted both in transit and at rest, and organizations that have not already done so should audit their encryption practices and update their strategies as needed.

The current state of cloud networking

Overall, organizations seem to be satisfied with the ROI of the cloud, with 84% of respondents saying they are getting everything they can out of their cloud investments (Figure 52).

Figure 52

Do you feel that your organization is getting everything it could out of its cloud investments?



Top challenges

1. Security
2. Networking

It's not all smooth sailing, however–there are hurdles to taking full advantage of the cloud. Security and networking are the two biggest challenges, cited by 68% and 59% of respondents respectively, even if they say their organization is getting full ROI on the cloud (Figure 53). So, it's no surprise that cloud complexity and security concerns are the top two obstacles respondents report facing while deploying cloud-based technologies–55% and 54% respectively (Figure 54).

Figure 53

What is preventing your organization from taking full advantage of cloud? Where are you burning the most man-hours?

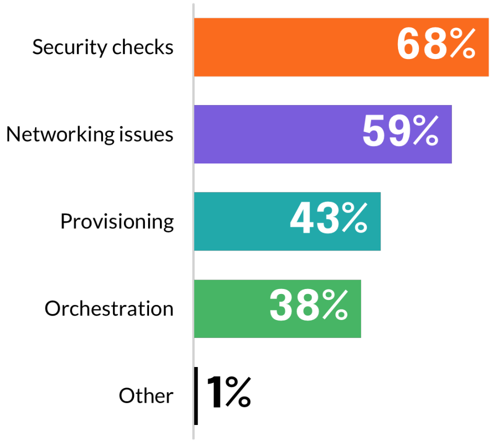
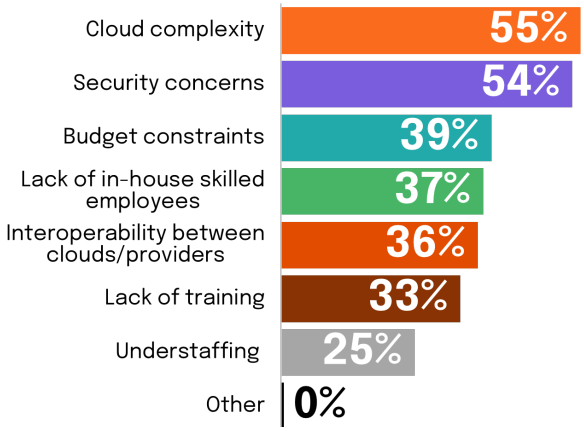


Figure 54

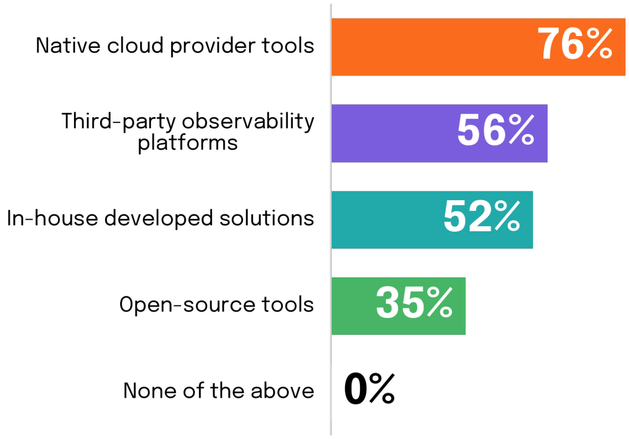
What obstacles has your company faced while deploying cloud-based technologies?



Given these challenges, it's critical for organizations to have the right systems in place to monitor and manage their cloud network activities. More than three-quarters (76%) are leveraging native cloud provider tools to do this, but a large number are using third-party observability platforms (56%) and custom solutions they've developed in house (55%) (Figure 55).

Figure 55

What tools or platforms do you use for monitoring and managing cloud network activities?



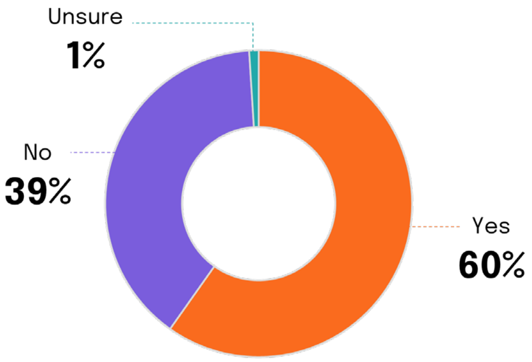
60%

experience cloud networking-related outages.

Even with monitoring and management tools, outages are still a problem. In fact, 60% of respondents experienced a cloud networking-related outage in the past year (Figure 56).

Figure 56

Has your organization experienced a cloud networking-related outage in the past 12 months?



There are a variety of outage-causing factors, ranging from internal issues, like human error (43%) and misconfigurations (37%), to external problems, including CSP infrastructure failure (48%), third-party integration issues (40%), and cyberattacks (40%) (Figure 57). And 69% of respondents are battling outages on multiple fronts; 31% experienced outages as a result of three or more of these factors in the past 12 months (Figure 58).

Figure 57

Which of these have caused cloud outages in your organization in the past 12 months?

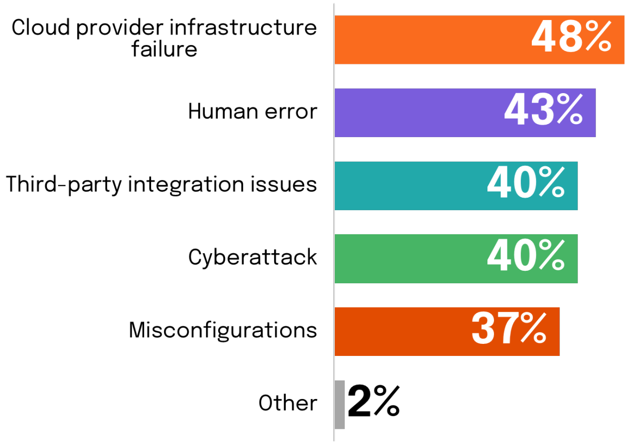
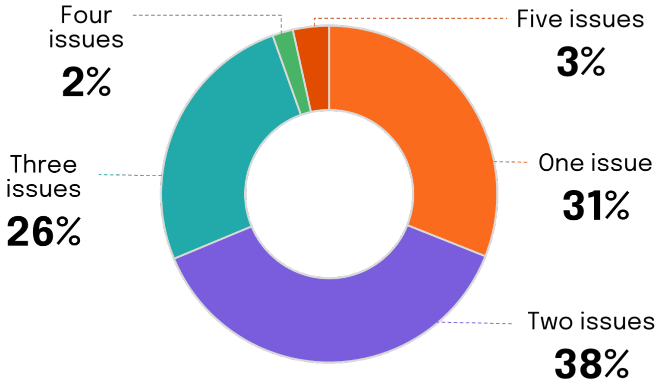


Figure 58

Number of different issues leading to cloud outages in past 12 months



Top outage causes

1. Human error
2. Misconfigurations
3. CSP infrastructure failure
4. Third-party integration issues
5. Cyberattacks

ACTIONABLE INSIGHT

There is significant room for improvement in cloud networking operations to identify and mitigate problems, both internal and external, before they lead to outages.

The current state of cloud talent

One critical cloud strategy success factor is having staff with the right skill sets, according to 97% of respondents, with 68% saying this is very important (Figure 59). Unfortunately, 69% of respondents say that hiring to support cloud initiatives has been a struggle (Figure 60).

Figure 59

How important is having staff with the appropriate skill levels in determining the success of your organization's cloud strategy?

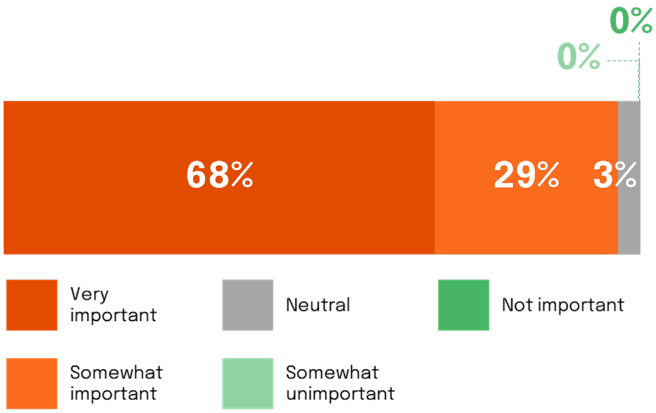
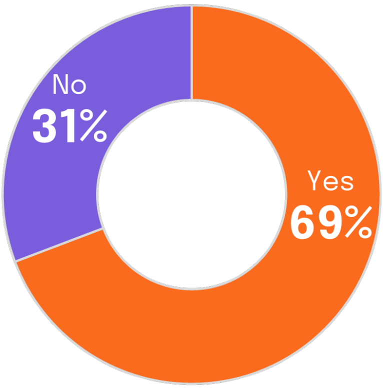


Figure 60

Has your company struggled to hire the necessary candidates to support cloud initiatives within your organization?



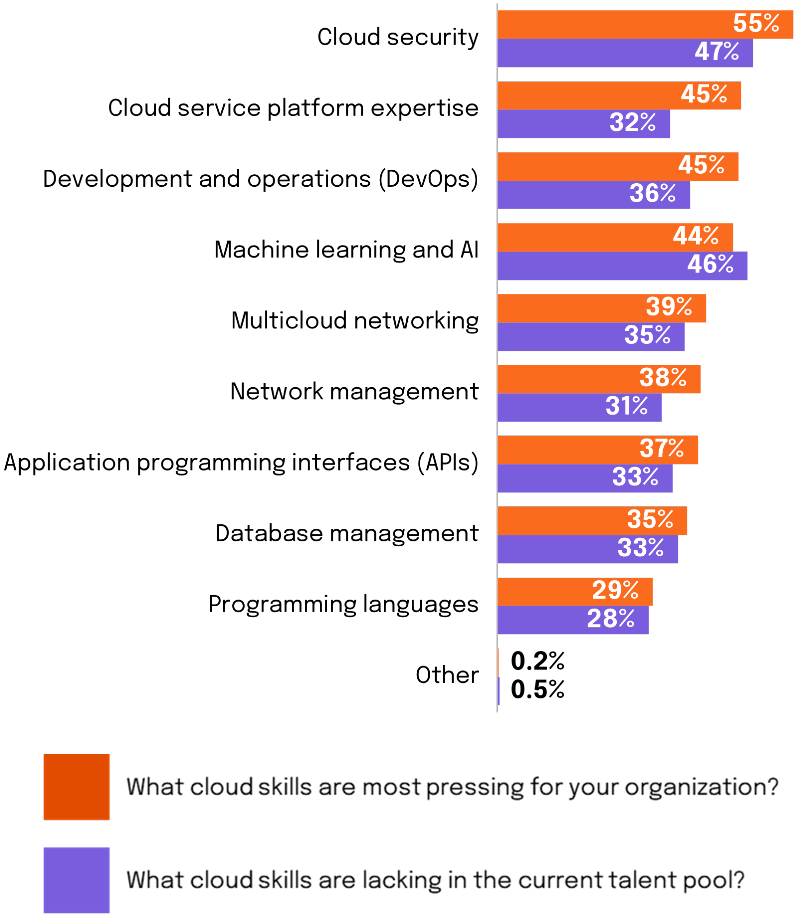
69%

struggle in hiring efforts to support cloud initiatives.

Given the ongoing overall technology talent shortage, these hiring challenges should not come as a surprise. However, comparing the specific cloud skills that organizations actively need with the current holes in available skill sets puts the problem in sharp relief. For example, 55% of respondents say that cloud security skills are most pressing for their organization and 47% say those same skills are missing in the current talent pool (Figure 61).

Figure 61

Skills gap



47%

report that critical cloud security skills are missing in the current talent pool.

ACTIONABLE INSIGHT

Given the hiring challenges, enterprises are going to have to look for alternative ways to set their cloud strategies up for success, which could include training and certification, automation, AI and ML, and other approaches.

The current state of cloud costs

Networking can consume a significant portion of an organization's overall cloud costs. For 41% of respondents, networking accounts for one-quarter to one-half of their overall cloud budget (Figure 62). And those budgets seem to be relatively accurate, with virtually all respondents reporting that they are somewhat or very successful at forecasting their cloud networking costs (Figure 63).

41%

spend 25-50% of their overall cloud budget on networking.

Figure 62

What percentage of your cloud budget is allocated to networking costs?

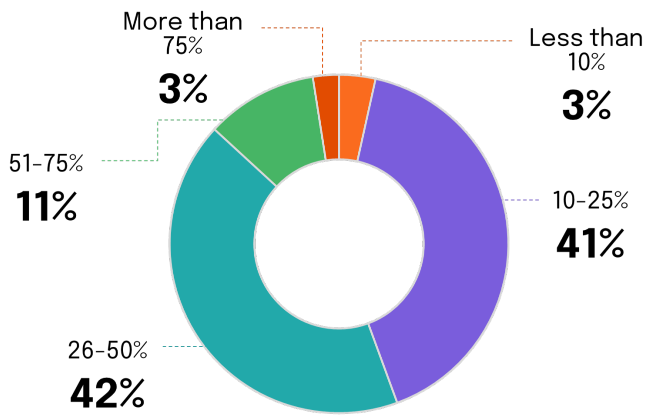
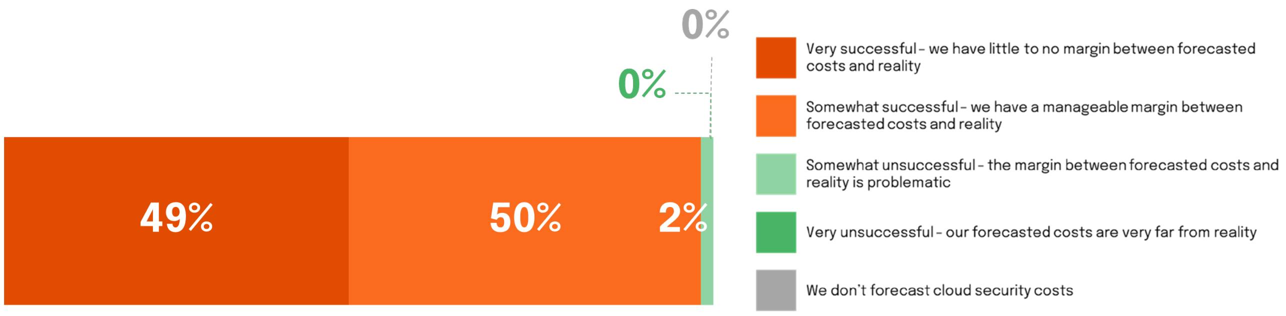


Figure 63

How successful are you in forecasting cloud networking costs?



It's not enough for organizations to accurately forecast their overall cloud costs, however, as over 96% of respondents say that the ability to understand cloud costs by department for billback/ chargeback is somewhat or very important (Figure 64). And a similar number (almost 95%) need that information for their customer-facing applications (Figure 65).

Figure 64

How important is billback/chargeback of cloud costs to various departments in your organization?

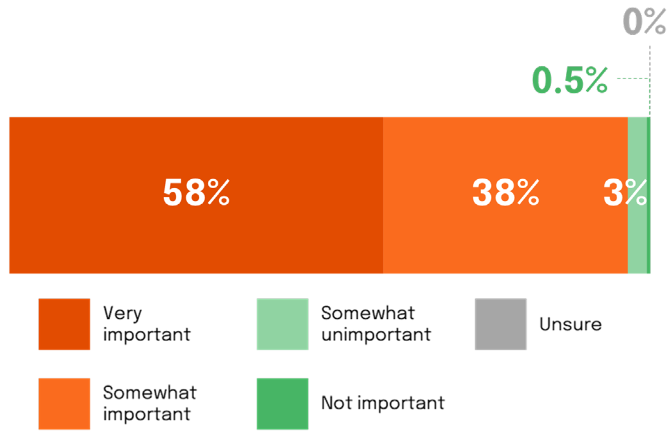
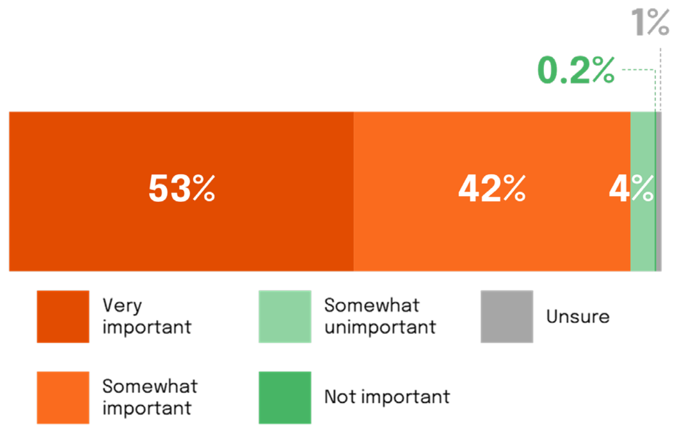


Figure 65

How important is billback/chargeback to your customer-facing applications?



95%

need to understand cloud costs by department for customer-facing applications.

Despite this widespread need, 52% of organizations struggle with establishing effective billback/chargeback models (Figure 66)—and a whopping 79% are interested in moving to a consumption-based billing for their customer-facing applications (Figure 67).

Figure 66

Does your organization struggle with billback/chargeback models?

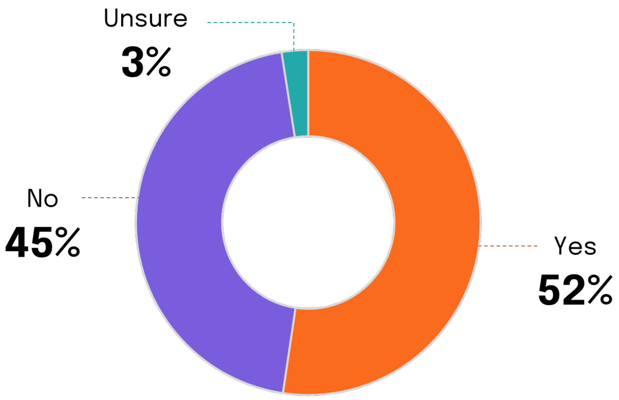
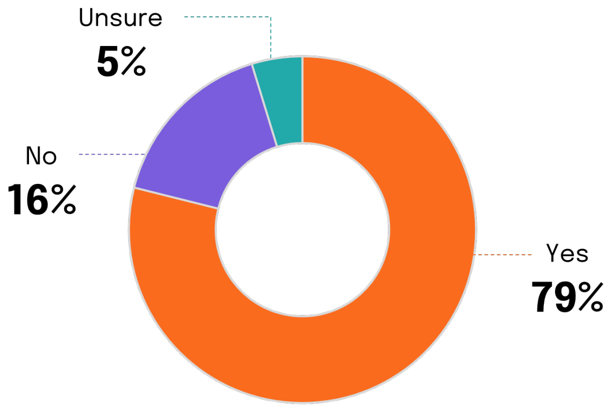


Figure 67

Are you interested in moving to consumption-based billing for your customer-facing applications?



79%

are interested in consumption-based billing for customer-facing applications.

ACTIONABLE INSIGHT

Despite having a good grasp on overall cloud networking costs, organizations need to be able to allocate costs to business units or applications based on actual usage.

Methodology

An online survey of 403 U.S. IT professionals, ages 25 and over, was conducted by Propeller Insights on behalf of Aviatrix from March 17 to March 31, 2025. The maximum margin of sampling error was +/- 5 percentage points with a 95% level of confidence.

What cloud network security challenges is your organization struggling with?

Aviatrix can help. **Aviatrix Cloud Native Security Fabric** delivers the security, visibility, and cost controls that maximize cloud success. With a cloud-native data and control plane providing secure connectivity to, through, and across clouds, Aviatrix gives you the power to change the game. The Aviatrix platform is the only secure networking solution built specifically for the cloud to help companies modernize their cloud by eliminating trade-offs between security, agility, and performance.

Get started today, with an interactive demo or schedule a personalized walkthrough.

Get Started

AVIATRIX®

About Aviatrix

Aviatrix® is the cloud network security company trusted by more than 500 of the world's leading enterprises. As cloud infrastructures become more complex and costly, the Aviatrix Cloud Network Security platform gives companies back the power, control, security, and simplicity they need to modernize their cloud strategies. Aviatrix is the only secure networking solution built specifically for the cloud, that ensures companies are ready for AI and what's next. Combined with the Aviatrix Certified Engineer (ACE) Program, the industry's leading secure multicloud networking certification, Aviatrix unites cloud, networking, and security teams and unlocks greater potential across any cloud.