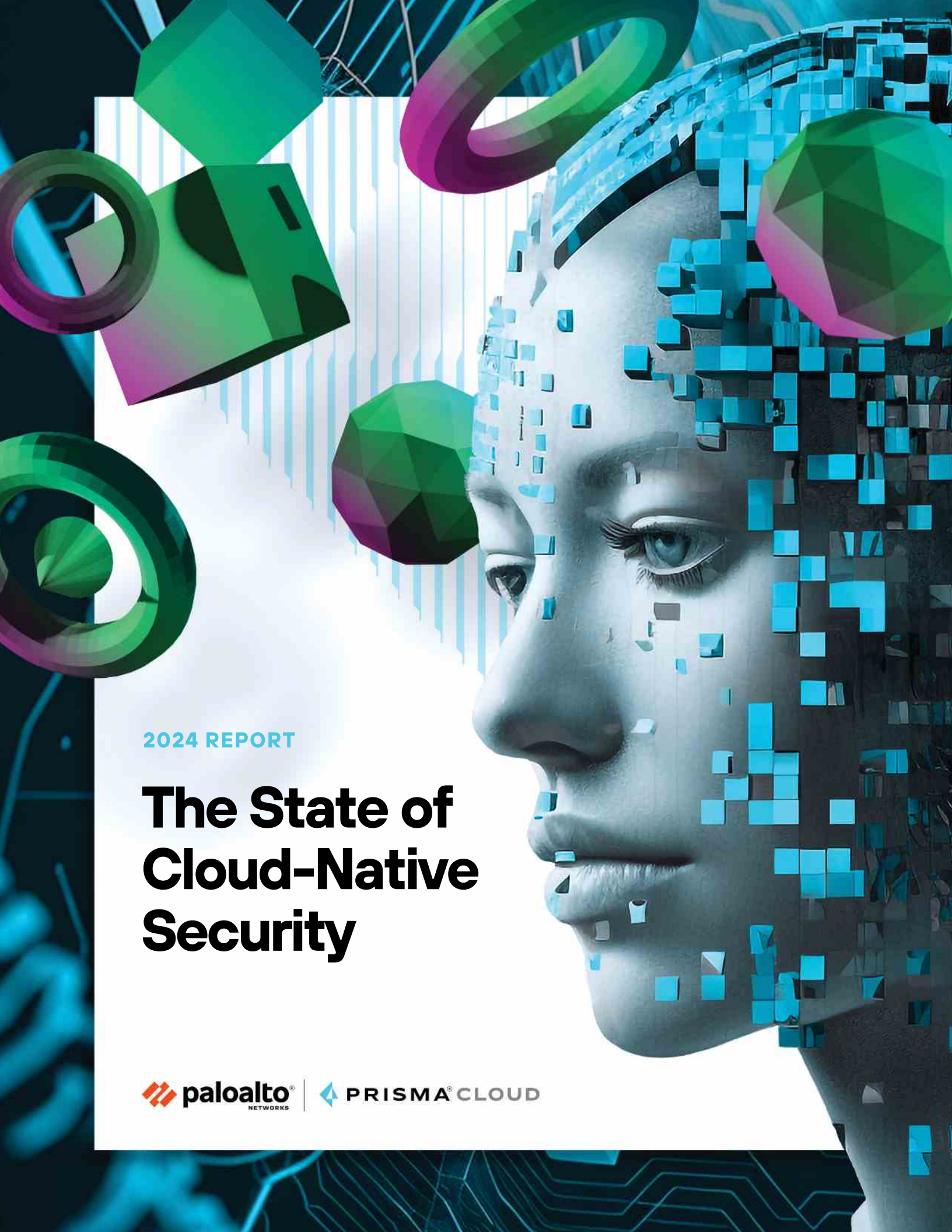


2024 REPORT

The State of Cloud-Native Security

paloalto NETWORKS | PRISMA CLOUD

EXECUTIVE SUMMARY

A Retrospect on the Previous Year

We begin our exploration of the 2024 state of cloud-native security with a look back at the events and influences of 2023, each of which factors into our current postures, the challenges we confront, and the strategies we've chosen to achieve our desired outcomes.

While agile development, open-source software, and cloud-native technologies gained momentum in 2023, attacks targeting the application layer have become an established trend. The cloud-native ecosystem grappled with a surge in supply chain attacks, highlighting the prevalence of vulnerabilities in open-source software and third-party libraries. Real-world data analyzed by our Unit 42 team enhanced this picture, identifying the cloud as the dominant attack surface, with 80% of medium, high, and critical exposures found in cloud-hosted assets.[1]

For some time, we've prioritized application and infrastructure security. But we mustn't forget that third, all-important ball in the air. With the global datasphere reaching 120 zettabytes in 2023,[2] securing sensitive data remains mission critical. The challenges of monitoring and controlling sensitive information, however, have escalated.

[1] Cortex Xpanse ASM Threat Report 2023

[2] Data Created Worldwide 2010-2025

Cloud security is as much a business goal as anything else we endeavor to achieve.

What's more, generative AI emerged in 2023 as a groundbreaking force with the potential to halve development time and costs, ultimately redefining the application economy.[3] But much like the cloud and its myriad benefits inextricably tied to challenges we must address, generative AI as a development tool comes counterweighted with concerns. We had no sooner begun to wonder about potential issues when OWASP released the Top 10 LLM Security Risks for security teams, alerting us to prompt injection, insecure output handling, and new avenues for supply chain vulnerabilities and sensitive information disclosure.

But challenges are not new to us. It's safe to say that generative AI is as much a mainstay as the cloud. We will increasingly tap into its power with an awareness of responsibility and a priority of security.

Looking at the path ahead, as we move forward in the pursuit of our objectives, we are certain of one thing—cloud security is as much a business goal as anything else we endeavor to achieve.

[3] Economic Potential of Generative AI | McKinsey

INTRODUCTION

Time Favors the Prepared

Anticipating threats and adapting strategies ensures resilience in complex cloud environments.

When readiness wins the race against time, it's the name of the game. You'll hardly hear cloud security practitioners talk about pain points apart from the constraints of time. They are, after all, inundated with alerts and manually collating data from satellite tools while racing against attackers moving at machine speed to identify vulnerabilities.

Understandably, 90% of respondents from this year's State of Cloud-Native Security survey want better risk prioritization. Upwards of 90% say the number of point tools they use creates blind spots affecting their ability to prioritize risk and prevent threats. Sixty-two percent of security practitioners want easy-to-use security solutions, with 1 in 3 respondents citing rapid technology changes as the primary obstacle contributing to attack surface expansion.

How multi is multicloud? Organizations are leveraging an average of 12 cloud service providers (CSPs) across SaaS, IaaS, and PaaS for their deployed applications. This, coupled with an average use of 16 cloud security tools, underscores the intricate ecosystem security teams must navigate. A 98% consensus emphasizes the importance of reducing the number of security tools, defining readiness in terms of simplification and consolidation.

Organizations are leveraging an average of 12 cloud service providers.

Emerging concerns, such as the security risks associated with AI-generated code and unmanaged APIs, alongside traditional challenges like inadequate access management and the expanding attack surface, underscore the evolving nature of cloud security threats. Organizations are rethinking their strategies, with many emphasizing the need for foundational changes to enhance cloud security from the outset. Understanding the landscape is central to equipping security and DevOps teams with the necessary resources.

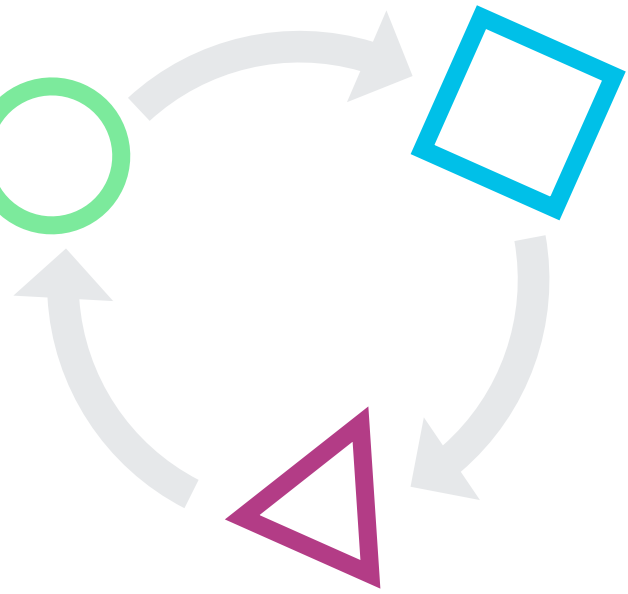
What steps are organizations taking to effectively navigate data security and the need for rapid deployment? Where are organizations running into challenges? How are they bridging security and development teams? How ready are organizations to handle AI-related security risks? How effectively are they integrating solutions into their operational frameworks?

Our annual multi-industry survey seeks to answer these questions and more to provide insights into the best practices shaping the future of cloud-native security.

HIGHLIGHTS OF

2024 Survey Findings

People are rethinking their lift and shift deployments.



When asked what they would do differently if migrating to the cloud for the first time, 50% of respondents said they would spend more time refactoring their applications instead of migrating with minimal changes.

Supporting this sentiment, our survey shows that organizations that moved workloads to the cloud without optimizing them for the cloud had higher total costs of ownership. What's more, their applications didn't gain the advantages of agility and scalability the cloud is renowned for.

When security is seen as a hindrance, stress levels are high.

Security is a gating factor hindering software releases, according to 86% of respondents.

71%

Highlighting the risks associated with accelerated time-to-market schedules, **71% of respondents attribute rushed deployments to security vulnerabilities**, underscoring the tension between the need for rapid development and the imperative of maintaining security.

48%

Almost half of respondents experience **major release delays** all or most of the time

52%

Of respondents cite **conflict** between DevOps and SecOps as a significant source of stress.

AI-generated code is more worrisome than AI-assisted attacks.

More than 2 in 5 security professionals (43%) predict AI-powered threats will evade traditional detection techniques to become a more common threat vector.

Of respondents rank AI-powered attacks as a **top cloud security concern**.

Are **more apprehensive** about risks introduced by AI-generated code.

Yes, **all respondents** are reportedly embracing AI-assisted coding.

Table of Contents

The fourth annual State of Cloud-Native Security Report examines the security practices, tools, and technologies that organizations worldwide are employing to take advantage of cloud services and new application tech stacks.

Major sectors of industries were included in our research sample, with representation from consumer products and services, energy resources and industrials, financial services, healthcare, technology, media, and telecommunications.

More than 50% of the sample came from enterprise-sized organizations (over $1 billion in annual revenue).

Survey participants included an equal mix of executive leadership and practitioner-level roles to cover a broad spectrum of viewpoints across organizations. Practitioner-level participants were specifically from development, IT, or information security functions.

All respondents self-reported as knowledgeable and familiar with their organization's cloud operations and cloud security and were sourced from professional survey panels.

Palo Alto Networks partnered with Wakefield Research, who conducted our survey.

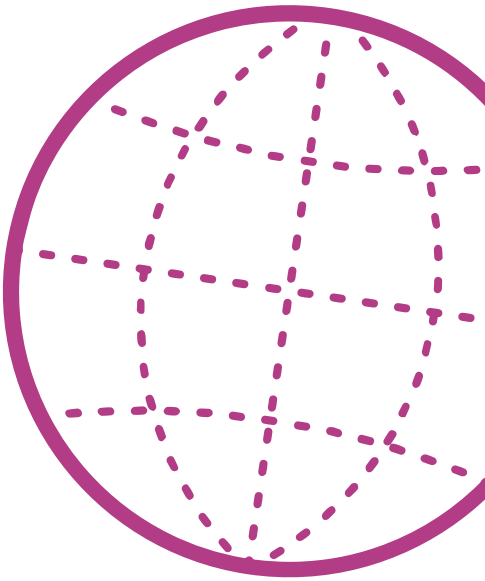
Fielded from December 20, 2023, to January 17, 2024, the survey gathered data from 2,800-plus respondents in 10 countries, including Australia, Brazil, France, Germany, India, Japan, Mexico, Singapore, the United Kingdom, and the United States.

THE CLOUD ECONOMY

A Global Perspective

Across regions, cloud investment trends affirm the cloud's strategic significance.

Organizations worldwide made substantial investments in cloud infrastructure, services, and operational efficiencies to drive digital transformation and expansion. The overall trend shows a surge in cloud spending with over 50% of organizations investing more than $10 million annually in cloud services. This integration of cloud technologies into various aspects of business operations suggests that investment trends will persist, if not accelerate, as organizations pursue greater agility, scalability, and innovation.



Cloud Spending Snapshot

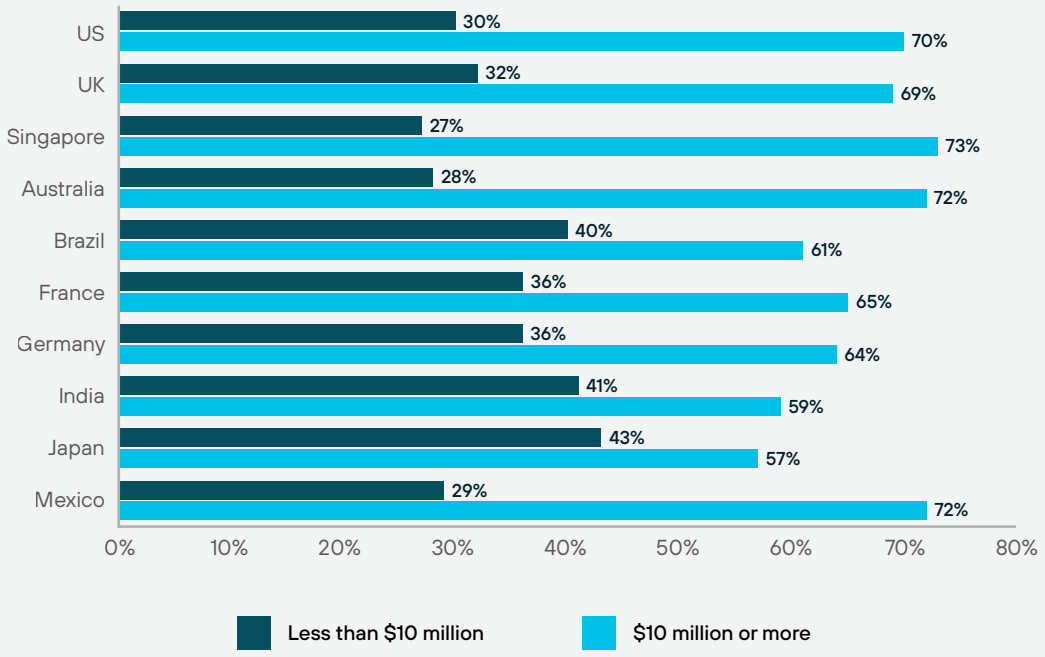


Figure 1. Regional investment patterns

Among regions, we see slight but telling variations. Australia, Mexico, and Singapore exhibit strong cloud spending in higher investment brackets, while the United States and the United Kingdom continue to invest significantly in moderate ranges. Cloud spending patterns in France and Germany indicate a mature yet cautious approach, with the bulk of investments falling within the €9 million to €46 million range.

In contrast, emerging markets like Brazil and India, along with Japan, have a higher proportion of organizations investing below the $10 million mark, at 40%, 41%, and 43%, respectively. Beyond cloud maturity, this trend may reflect a greater presence of small to medium-sized organizations, as well as conservative spending strategies in these regions.

Organizations reporting "Extensive Integration" or "Fully Native Environment" tend to invest more in cloud technologies compared to those with "Basic Infrastructure". In the U.K., for instance, 32% of organizations spending less than $10 million are at the initial stages of exploring the cloud, compared to 76% of those investing $10 million or more, having achieved extensive cloud integration. This pattern is consistent across regions, indicating that as organizations mature in their cloud journey, their cloud spend increases, likely due to the adoption of more advanced cloud services and architectures, in addition to scaling.

From Exploration to Cloud-Native Innovation

The cloud journey is not linear. It is a continuum of adaptation, learning, and transformation—one shaped by strategic investments, maturity levels, deployment methodologies, and operational efficiencies.

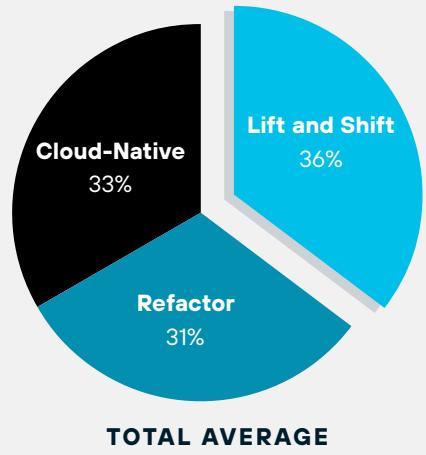
Cloud maturity extends beyond the adoption of technologies. It is both a reflection of and influence on an organization's culture, processes, and the ability to harness cloud capabilities for business transformation. Among this year's survey respondents, maturity levels range from using basic cloud infrastructure for select projects to extensive integration and fully native cloud environments.

Across this range, we see a correlation in application deployment methodologies.

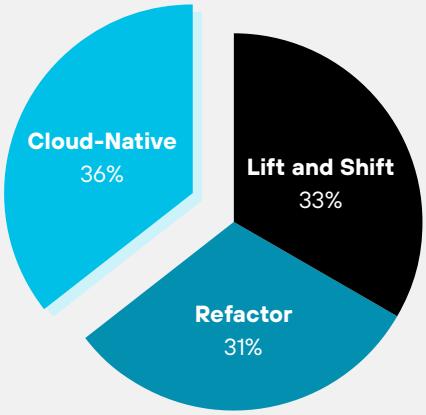
50%

Of respondents say they would spend more time refactoring their applications.

Experienced Organizations Move to Cloud-Native



TOTAL AVERAGE



AVERAGE 3+ YEARS

Figure 2. Primary method of application deployment to the cloud

The deployment preference for lift and shift (35%) aligns with the pragmatic approach many organizations take toward cloud migration. While cloud-native and refactoring deployments offer long-term benefits, the initial focus on fast, low-disruption migration has been a historic approach.

Organizations that begin with lift and shift typically progress through refactoring to cloud-native development, maturing beyond seeking quick wins to embracing cloud-first strategies for gains in performance, scalability, and cost-efficiency. Our survey bears out this trend, with cloud-native deployments displacing lift and shift at 36% among organizations with 3 or more years in the cloud.

Performance, scalability, cost-efficiency

>

Quick wins

Across regions, maturity trends show Australia (26%), Singapore (26%), and the U.S. (24%) out front with roughly a quarter each having full cloud-native environments. France and Germany follow at 17% and 14%, respectively.

As organizations deepen their cloud investments, they also evolve their approaches to application deployment.

Larger organizations are more inclined toward advanced deployment methodologies, likely due to their greater resources, complex requirements, and strategic focus on innovation.

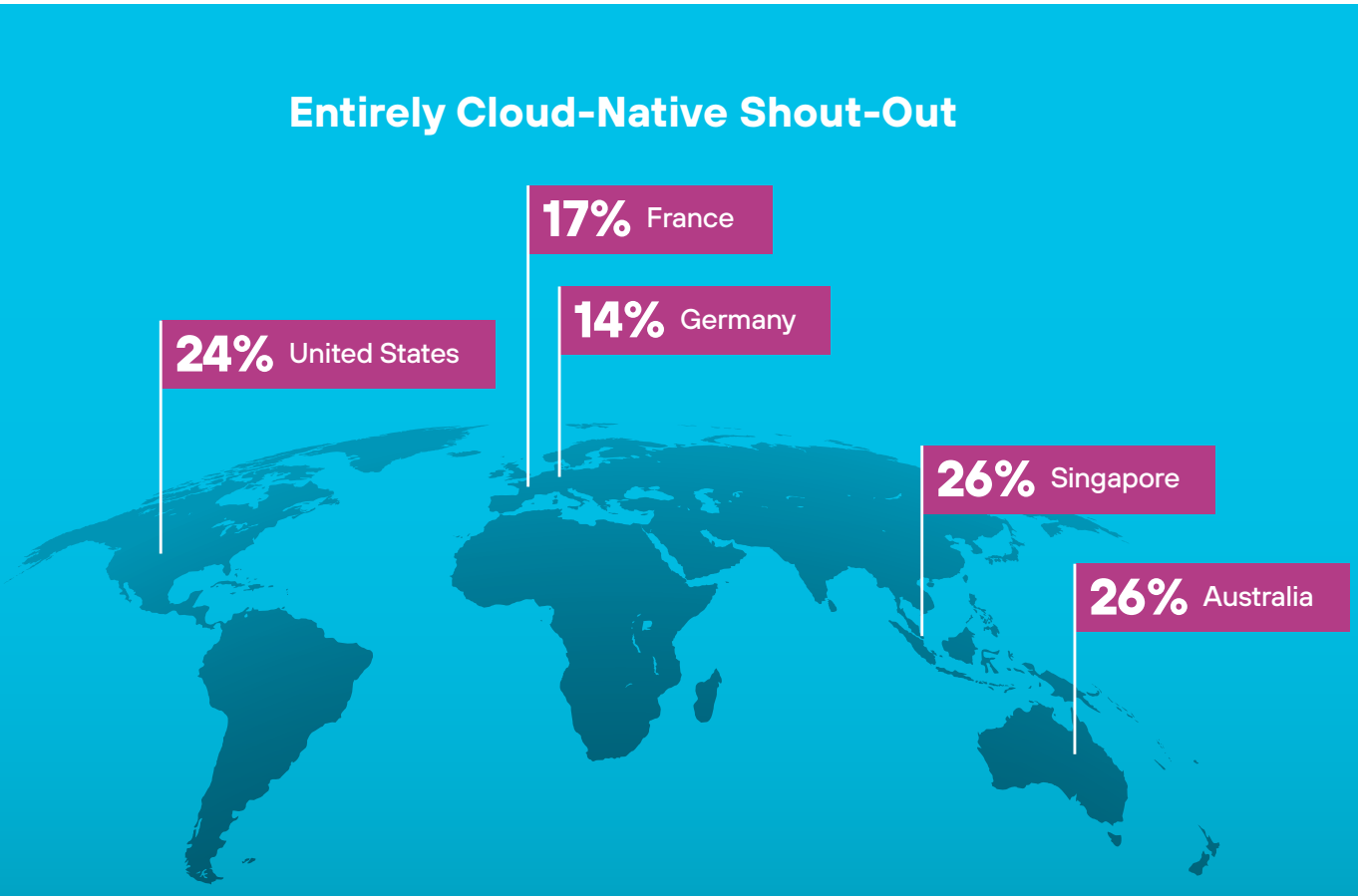


Figure 3. Countries with the most all cloud-native environments

Plan for Cost Optimization of Legacy Apps

Legacy app modernization consumes a significant portion of cloud TCO, emphasizing the importance of strategic cloud migration planning.

The majority of respondents (67% globally) reports spending between 10% to 30% of their cloud total cost of ownership (TCO) on legacy app modernization. For 24% of organizations, costs soar upwards of 30%, highlighting the need to balance operational continuity and the pursuit of innovation.

30% of cloud costs go to overhauling legacy apps.

45% of respondents say application architecture issues take too much time.

Among regional variations, Latin America and Japan and Asia-Pacific report a higher percentage (29% and 26%, respectively) of respondents spending 30% or more of their cloud TCO on legacy app optimization. India stands out with 42% of respondents indicating that 30% or more of their cloud TCO goes toward optimizing legacy apps for the cloud. When asked why developers' time is diverted to resolving bugs and code vulnerabilities, 45% blame application architecture.

The significant spend on legacy app modernization underscores the need for strategic planning in cloud migration projects. Organizations should assess which applications are suitable for lift and shift versus those that require refactoring or complete redevelopment to optimize costs and benefits. Security and compliance challenges make this particularly important, in that older applications may not have been designed with cloud-native security in mind.

Balancing Tools, Vendors, and Organizational Needs

The cloud is, well, nebulous. Add a cloud service provider (CSP) here, a security tool there. The ecosystem extends. And extends. Complexity is a constant companion.

With an average of 16 cloud security tools on board, it's no surprise that 98% of respondents consider it important to reduce this number. Almost as many (97%) want to reduce the average 14 vendors they work with.

Taking on complexity in one form or another is a recurrent theme in annual publications of the State of Cloud-Native Security Report. To date, we've not seen an indication of progress on this front. The number of tools dedicated to cloud security has, in fact, increased 60% from last year's findings. The drive to address complexity, however, is visceral for those who routinely confront it.

98%

Of respondents consider it important to reduce the average 16 cloud security tools they have on board.

In 2024, multicloud translates into approximately 12 cloud service providers across SaaS, IaaS, and PaaS per organization. Regional averages range from 16 in the U.S. to a no less impressive 9 in Latin America. And this represents only the public cloud portion of the ecosystem, accounting for little more than half (52%) of an organization's cloud workloads. As organizations use more CSPs, maintaining visibility and ensuring consistent security policies, access controls, and data protection measures becomes taxing. Complexity and fragmentation of cloud environments, for more than half of survey respondents (54%), presents a major security challenge.

54% of respondents agree that complexity and fragmentation of cloud environments presents a major challenge to security.

Architecture-Hopping: Trend or Transition?

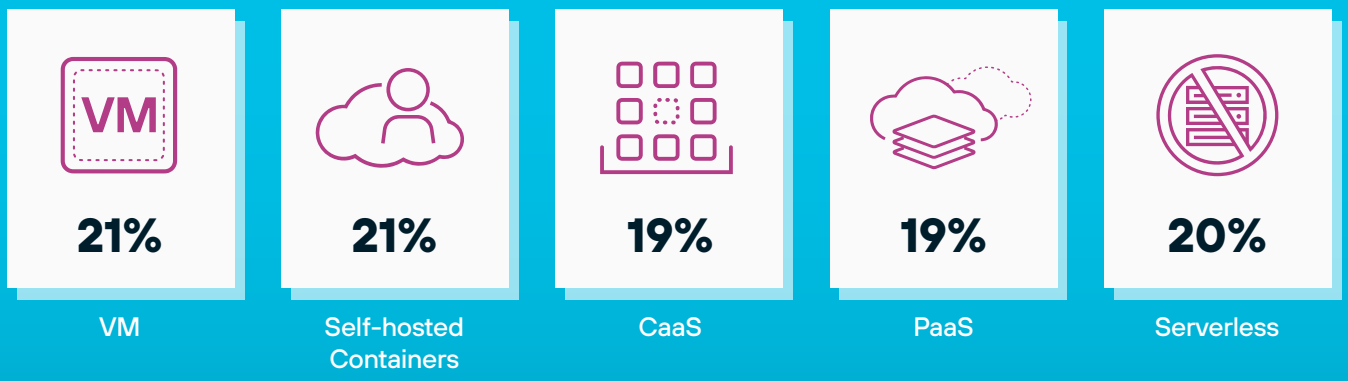


Figure 4. Cloud architecture usage

Cloud architecture introduces another layer of complexity. The distribution of workloads among different architectures seen among 2024 survey respondents suggests a transitional cloud landscape with organizations navigating between traditional (VMs) and modern (serverless) architectures.

This diversity challenges security teams to create consistent policies and security solutions for these environments. Characterized by portability, granularity, ephemerality, and heterogeneity, modern workloads have expanded the attack surface. They require a different approach to security, one with actionable insights, monitoring, and incident response.

Survey responses suggest a transitional cloud landscape with organizations navigating between traditional and modern architectures.

Top Concerns in Cloud Security

A range of threats poses serious security concerns, pointing to the importance of proactive measures that can outpace emerging and perennial risks.

When exploring top cloud security concerns, survey responses portray a global community acutely aware of the multifaceted threats facing cloud environments. From the nuanced challenges of securing AI-generated code and APIs to the universal threats posed by inadequate access management and insider risks, concerns are varied and far-reaching.

1. **AI-Generated Code**
2. **API Risks**
3. **AI-Powered Attacks**
4. **Inadequate Access Management**
5. **CI/CD's Impact on the Attack Surface**
6. **Insider Threats**
7. **Unknown, Unmanaged Assets**

1

AI-Generated Code

Unforeseen vulnerabilities and exploits introduced by AI-generated code are worrisome to 44% of organizations. As algorithms autonomously create software, the lack of human oversight may lead to undetected security flaws.

Additionally, the rapid pace of AI-generated code development could outstrip traditional security testing methods, resulting in a likelihood of vulnerabilities making it into production.

While concerns in this area are widespread, apprehension is more pronounced in the U.S. and India.

0110010100110110
1001101100101101
0110010100110110

2

API Risks

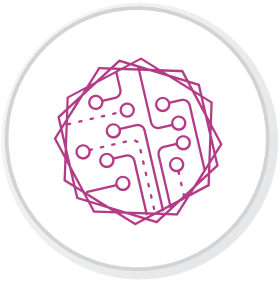
Close behind in top-ranked concerns, **43% of global respondents have their sights on API-associated risks**. As gateways for data exchange and integration between applications, APIs can enable unauthorized access, expose sensitive data, and create vulnerabilities for cyberattacks.

Apprehension among organizations centers on unmanaged and unsecured APIs, third-party API risks, and the lack of oversight in API integrations.

Regionally, concern for API risks peaks in Brazil, where 52% of respondents view it as a significant threat vector.

3

AI-Powered Attacks



As AI technology continues to develop, the potential for AI-powered attacks rises.

A growing awareness of how AI might be weaponized—coupled with an uncertainty that makes it difficult to plan for and defend against—has 38% of organizations concerned.

The potential for greater sophistication and targeting leading to greater damage should alert organizations to the evolving threat landscape that AI represents.

4

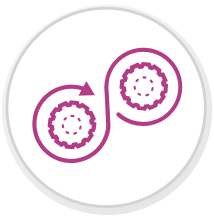
Inadequate Access Management

Inadequate access management is cited by 35% of organizations as a top concern, emphasizing the challenges organizations face in controlling who has access to what within the cloud.

Access control concerns are particularly acute in regions like Latin America, where 44% of respondents cite the need for effective identity and access management solutions.

5

CI/CD's Impact on the Attack Surface



With its potential to introduce vulnerabilities and quickly deploy them into production, the **CI/CD pipeline's impact on the attack surface concerns 34% of organizations.**

The concern spikes in Japan and Asia-Pacific, where 40% consider the risks of increased vulnerabilities and security breaches a significant issue.

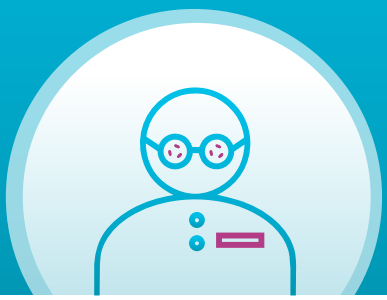
6

Insider Threats

Insider threats are a concern for 32% of respondents. This rate is fairly consistent across regions, amplifying the universal challenge of mitigating risks associated with compromised insiders—including business partners, third-party vendors, and contractors, as well as employees.

Given that 98% of organizations report storing data across numerous environments, opportunities for insider threats are particularly high.

In fact, elevated opportunities may have contributed to the rise in advanced persistent threats (APTs) reported by 45% of organizations.

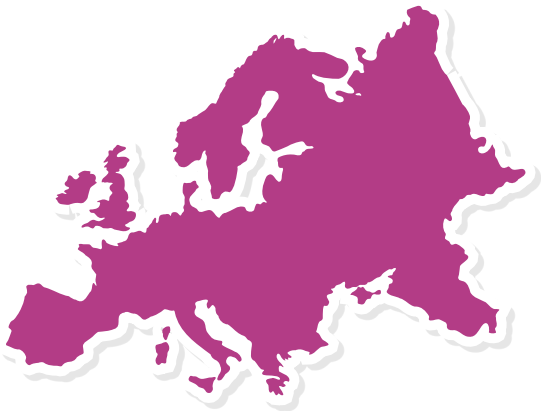


7

Unknown, Unmanaged Assets

Finally, **29% of respondents are concerned about unknown, unmanaged assets in the cloud.**

This issue is seen as more pressing in Europe, indicating greater awareness for a possible gap in asset management and visibility that could lead to vulnerabilities and breaches.



INCIDENT RESPONSE:

The Race Against Time

Security incidents require organizations to continuously adapt and evolve their practices to stay ahead of the curve.

Cloud security incidents are on the rise, with increases in what is typically the most consequential incident—data breaches—reported by an alarming 64% of organizations.

Another 48% of organizations report increases in compliance violations, which are followed by increases in operational downtime due to misconfigurations encountered by 45%.

The top three increases in security incidents are the most costly.

- #1 Data breaches $$$$
- #2 Compliance violations $$$
- #3 Downtime due to misconfigs $$$

Security Mishaps on the Rise

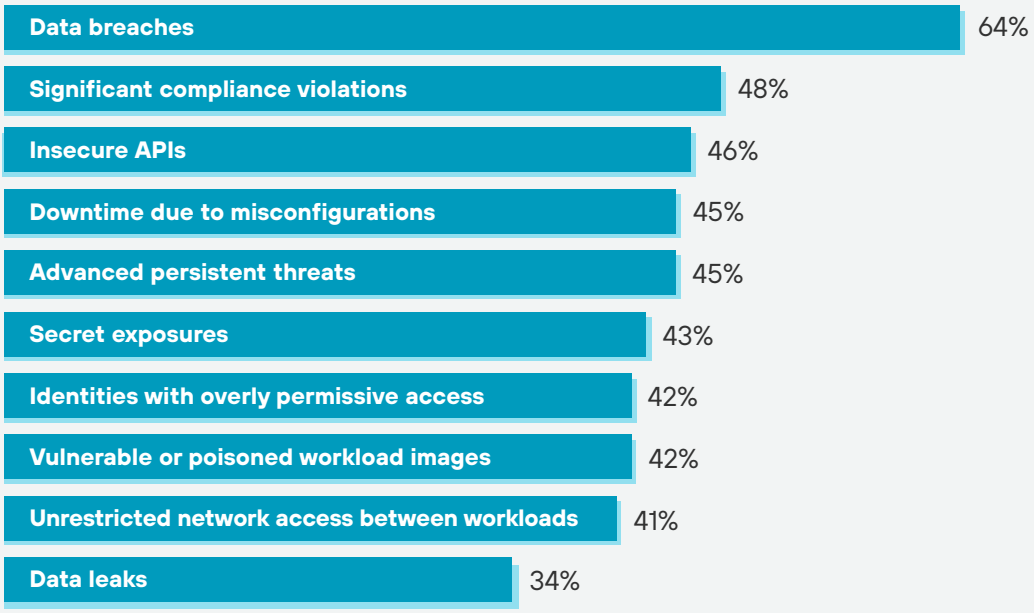
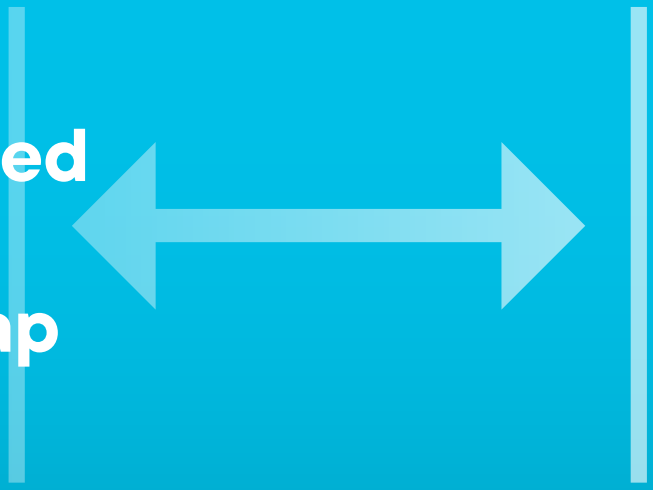


Figure 5. Increases in security incidents over the last 12 months

Of the security incidents detailed above, increases in excessive permissions reported by 42% of respondents is troubling. Organizations understand that identity management is the perimeter of cloud environments, and yet the problem with permissions persists. Rises in everything from breaches and data leaks to compliance violations and secrets exposure likely involve an IAM component.

The upward trend in incidents underscores the need for strict access controls and adherence to the principle of least privilege to safeguard systems and sensitive data.

The increasing incidence of advanced persistent threats (APTs) points to a gap in security posture.



Organizations are witnessing an increase in advanced persistent threats (APTs), which are known for their sophistication, stealth, and ability to infiltrate networks while remaining undetected for extended periods. The concern here lies in the juxtaposition, that although organizations report no unusual challenges with detecting and responding to incidents, they're still succumbing to this high-stakes jeopardy.

The increasing incidence of APTs points to a gap in overall security posture. Given that APTs often exploit zero-day vulnerabilities or use social engineering tactics that can bypass traditional detection mechanisms, the scenario emphasizes the imperative of taking a proactive, rather than reactive, approach to security. It drives home the need for continuous monitoring, threat hunting, and implementing advanced security measures that can predict and prevent attacks before they occur. As discussed above, risk assessment might begin with a careful study of identity management.

Securing Sensitive Data in the Cloud

Organizations face significant data security challenges, with many relying on insufficient methods to safeguard sensitive information.

Of the organizations we surveyed, 50% conduct manual reviews to identify and classify sensitive data within the cloud, which is a concerning indicator of the state of data security. Manual reviews are time-consuming, error-prone, and often incomplete, leaving organizations vulnerable to data breaches. Sixty-four percent of respondents report an increase in data breaches over the last 12 months.

With 98% of organizations storing sensitive data across multiple locations—on-prem servers, the public cloud, in SaaS applications with local storage, on private clouds hosted by third parties, and endpoints—we know that security challenges are high.

50% of organizations review code manually to locate their sensitive data.

Data's Wide-Ranging Odyssey

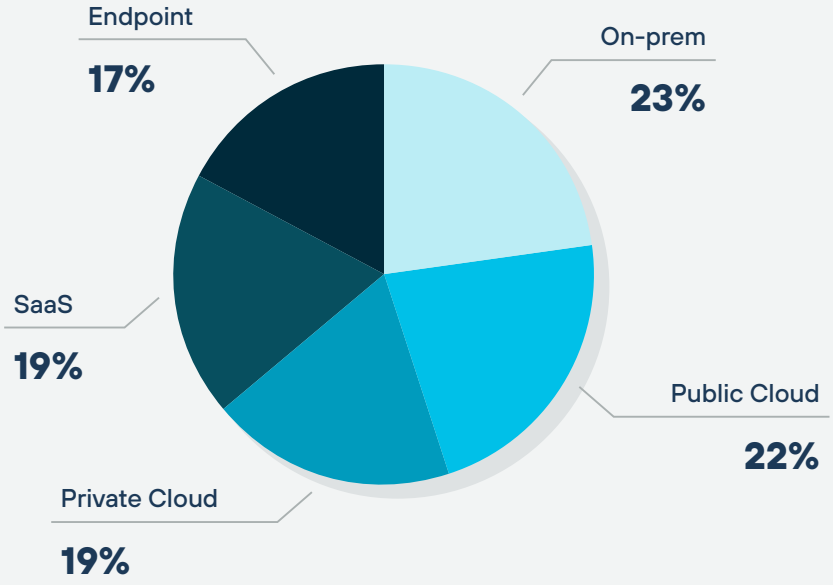


Figure 6. Data storage distribution

Data spread across multiple locations is difficult to track and protect. Security teams need a deep understanding of the controls and configurations for each environment, as well as the ability to coordinate security efforts across multiple teams. Management is complex and time-consuming, which we see reflected in the top data security challenges.

2 in 3 cybersecurity professionals (64%) saw an increase in data breaches.

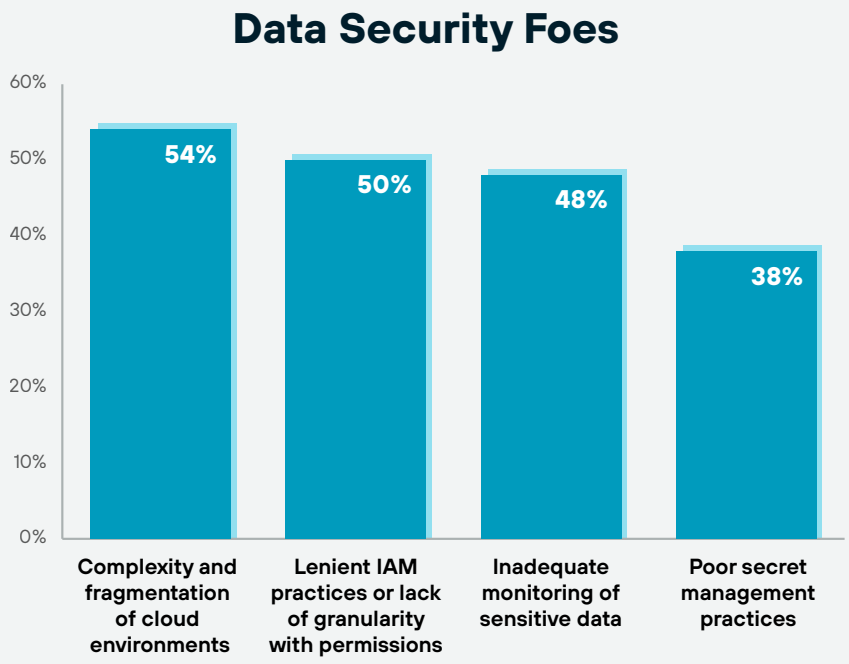


Figure 7. Top challenges in data security

Interestingly, in the previous 12 months, while only 38% of organizations flagged difficulties with secrets management, 43% of organizations saw an increase in secrets exposure. Even more curious, more Latin American organizations (47%) reported challenges with poor secret management than any other region. At the same time, 26% of Latin American organizations, a greater segment than any other region, saw a decrease in secrets exposure. This raises the question: Does awareness of a problem correlate with improved outcome?

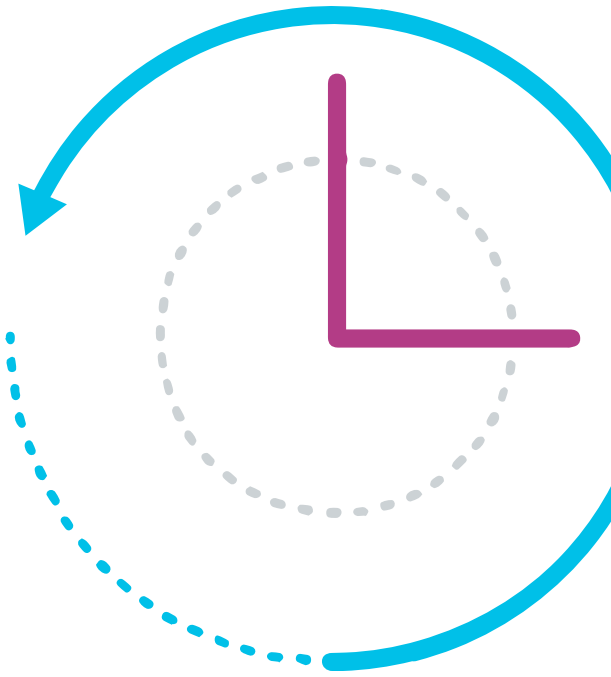
43% of organizations saw an increase in secrets exposure.

What Would You Do Differently?

Hindsight offers 20/20 insights for improved cloud migration.

When organizations recall migrating to the cloud for the first time, hindsight reveals areas where they could have approached the process differently to mitigate risks and enhance efficiency.

By exploring these insights, we gain a collective experience—a blend of strategic planning, security focus, technical adaptation, and market research, each contributing to a more effective and secure cloud migration process.



71%

71% of respondents say that rushed deployments have introduced security vulnerabilities.

Establishing a Governance Framework

A significant 53% of respondents stress the importance of investing in a governance framework to manage cloud resources. This is something we've heard from our customers, with some referring to their early days in the cloud as "the wild, wild West". By defining clear roles, policies, and processes, organizations can ensure resources are used efficiently and securely. Establishing such a framework from the outset provides a structured environment that can adapt to changes and scale with the organization. It's noteworthy that this perspective is valued across executive and practitioner levels, emphasizing its relevance.

Refactoring Applications

Half of survey participants (50%) suggest spending more time on refactoring applications rather than migrating them with minimal changes. This strategy involves reimagining how applications are architected and developed to fully leverage cloud-native features and services, which can significantly improve scalability, performance, and cost-efficiency. Survey responses portray a balanced view across organizational roles, highlighting its value in enhancing application readiness for the cloud environment.

Organizations are rethinking their strategies, with many emphasizing the need for foundational changes to enhance cloud security from the outset.

Prioritizing Security and Compliance

Reflecting an understanding that security in the cloud is fundamentally different from traditional on-premises security, 50% of respondents advocate for prioritizing security and compliance from the beginning of the cloud migration process. By embedding security and compliance considerations into the migration strategy, organizations can avoid pitfalls that lead to vulnerabilities, data breaches, and noncompliance penalties. This approach is emphasized by information security and IT departments, underlining their focus on safeguarding organizational assets. Regionally, it's particularly important to Latin American organizations (57%).

50% of organizations would prioritize compliance from the beginning.

Complexity and fragmentation of cloud environments challenges more than 50% of respondents.

Researching Tools and Vendors

Another 48% of respondents stress the importance of dedicating more time to researching tools and vendors. This insight underscores the complexity and diversity of the cloud services market, where the right tools and partnerships can dramatically influence the success of cloud adoption. By thoroughly evaluating options, organizations can select solutions that best fit their needs, budget, and strategic goals. This perspective is particularly valued by those in DevOps roles, reflecting their direct involvement in implementing and utilizing these tools.

The Human Factor

Security processes trigger delays, stress, and DevOps-SecOps conflict, suggesting the need for a people-first approach to secure application development.

Conflict between cloud security and application development is nothing new. Like complexity in the cloud and the drive to lessen it, the strife between those who build and those who secure persists. Although we see little progress on this front, participants in this year's State of Cloud-Native Security survey give us a closer look at the challenges—and maybe even a glimpse at the solution.

The most telling data point, or at least a good place to begin exploring the issue, is that 84% of respondents—an overwhelming majority—say that security processes cause delays to their project timelines.

This likely factors into why 83% view security processes as a burden. Another 79% say their employees frequently ignore or work-around security processes. And still another 71% admit they don't understand their security responsibilities.

92% of organizations attribute conflicting priorities between DevOps and SecOps teams to inefficient development and deployment.

How do these data points play out for the 94% of organizations with cloud security professionals embedded in their cloud DevOps teams? The defense strategy, for many, involves a myriad of tickets generated by security for developers to resolve. At best, this is unsustainable. At worst, it's a source of missed deadlines, inefficiencies, vulnerabilities in runtime, and team stress.

Developers are organizationally pushed to create code, innovate, and deliver features with revenue potential. Tickets, in other words, tend to accumulate, creating a backlog of security issues. And here's where most go-to-market dates are missed, perpetuating a culture of scapegoating.

Stress levels are palpable, with 71% of respondents saying not only are they stressed, but also their teammates are stressed. Turnover rates are predictably high, according to 93% of respondents.

Security is seen as a gating factor hindering software releases for 86% of respondents. Meanwhile, 91% say that developers need to produce more secure code.

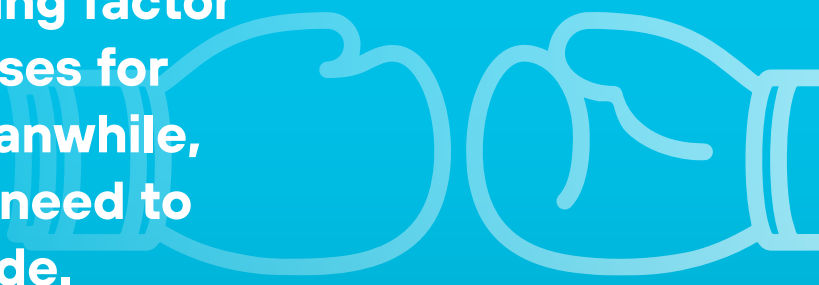


Figure 8: Sources of stress among DevOps and cloud SecOps professionals

As leadership considers workplace morale, they need to understand how organizational conflict and misaligned procedures contribute to it—as well as how it erodes performance.

The cultural emphasis on productivity appears to undermine productivity, as it ultimately becomes both the catalyst of conflict and the casualty of conflict.

An overwhelming 92% of respondents agree that conflicting priorities for DevOps and cloud SecOps hinders efficient development and deployment. Alarmingly, 71% say that rushed deployments have introduced security vulnerabilities.

Both the cause and the casualty of conflict is productivity.

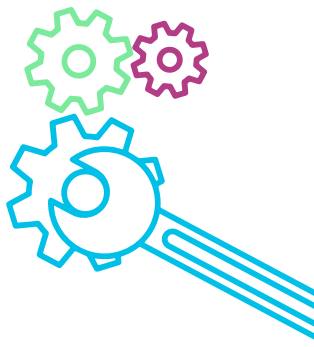
Risks, Realities, and Cloud Security Strategies

Organizations seek efficient security tools with automation, centralized visibility, and easy-to-use features to reduce blind spots and streamline operations.

Tooling issues significantly contribute to delays in resolving security bugs and vulnerabilities, affecting the development process for 40% of survey respondents. One in 3 security practitioners attribute legacy security tools to their inability to stay on top of threat vectors. Nearly 2 in 5 (38%) say alert noise contributes to delays.

Managing security in a multicloud environment is challenging. It requires a highly detailed, big-picture strategy that includes seamless visibility into all cloud assets, consistent security policy enforcement across providers, advanced threat detection and response capabilities...comprehensive security from code to cloud.

40% of organizations are delayed by inadequate tooling when resolving bugs and vulnerabilities.



When it comes to tooling, the overarching theme from 2024 respondents is a move toward efficiency and effectiveness. Organizations are recognizing the importance of streamlining operations—not just for cost management but as a key component of an effective security posture.

For 91% of respondents, the number of point tools used creates blind spots that affect their abilities to prioritize risk and prevent threats. An acute awareness of the impact of tool sprawl has 98% of respondents wanting to reduce the number of cloud security tools in use.

But 88% of organizations struggle to identify what security tools they need. This population has increased considerably from last year, suggesting that goals to consolidate have been baffled by the proliferation of discrete tooling options.

Teams do, however, know what capabilities they need. Ninety-four percent want a solution that provides immediate remediation steps. Nearly as many (93%) agree that their organization would benefit from a solution that automatically finds interconnected vulnerabilities and misconfigurations with the highest potential of a successful attack.

93% agree their organization would benefit from a solution that can automatically find interconnected cloud security flaws with the highest potential of an attack.

Top of the Shopping List

Easy for SecOps to learn and use	52%
Easy for DevOps to learn and use	23%
Competitive pricing and/or cost	12%
Best-in-breed security capabilities	8%
Supports a broad variety of platforms and tech stacks	4%
Potential impact on application and network performance (e.g., latency)	2%

Figure 9. No. 1 factor considered when choosing a cloud security tool

Security teams (90%) need more automation for risk prioritization, which would help alleviate some of the security burdens discussed in the previous section. More than 9 in 10 (92%) agree that cloud security needs more out-of-the-box visibility and risk prioritization filtering with minimal learning. Ease of use, in fact, is the most important factor when selecting a solution for 52% of organizations.

While their focus is on threats, security professionals are interested in their entire application lifecycle. An overwhelming 94% agree that they would benefit from a centralized security solution that sits across all cloud accounts and services, and 93% would benefit from having cloud and application security integrated with traditional network security.

94% of organizations would benefit from a centralized security solution that sits across all cloud accounts and services.

EMBRACING THE UNKNOWN

The Impact of AI on the Application Lifecycle

Organizations demonstrate a forward-looking approach to the future of cloud and application security in an AI-driven world.

AI is here, and it's fair to say that organizations are anxious, optimistic, and committed. Yes, nearly 2 in 5 cloud security professionals (38%) consider AI-powered attacks a top concern. When inquiring specifically about data security—particularly about the potential for AI-powered attacks to compromise sensitive data—the number shoots up to 89%, more than doubling. Respondents are clearly in uncharted territory.

More than 2 in 5 respondents (43%) predict AI-powered threats will evade traditional detection techniques and become more common. What are the most worrisome trends they expect to see? Forty-seven percent anticipate AI-fueled supply chain attacks compromising software components or cloud services. Personalized phishing, social engineering, or deepfakes to deceive users (45%), and manipulation of outputs or exploitation of vulnerabilities in AI systems (44%) follow closely.

On the other side of the fence, 47% of organizations have security risks associated with AI-generated code on their radar. Be that as it may, 100% of survey respondents—a first-ever unanimous response in the history of Palo Alto Networks The State of Cloud-Native Security Report—are embracing AI-assisted application development. AI is not only here, it's here to stay.

Organizations are currently at different stages in their AI journey. A significant portion of respondents (50%) use AI extensively to generate and optimize code. Regional trailblazers in this category include Singapore (60%), India (58%), and Brazil (57%). Taking a more conservative approach, just over half of organizations in Germany (52%) and Japan (51%) describe their adoption as moderate with selective use.

100%

Of survey respondents—**a first-ever unanimous response in the history of the Palo Alto Networks State of Cloud-Native Security Report**—are embracing AI-assisted application development. AI is not only here, it's here to stay.

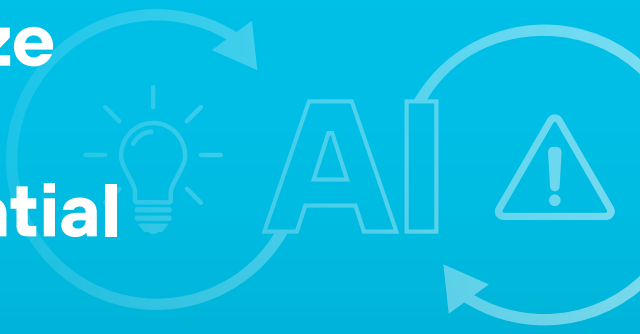
90%

Of organizations say that developers need to produce **more secure code**.

47%

Of organizations have **security risks** associated with **AI-generated code** on their radar.

Organizations recognize AI as an enabler of innovation and a potential vector for attacks.



Either way, organizations aren't throwing caution to the wind. When asked about priorities for 2024, 100% of organizations are committed to gaining visibility into their entire pipeline for AI deployments. Visibility includes datasets containing sensitive data and inferred context. Almost every organization (99%) will define policies and ensure access to AI models and services is granted on a need-to-know basis. Another 98% of organizations plan to build an inventory of AI models and the GenAI-assisted applications they've deployed.

The embrace of AI in development processes alongside the high level of concern about AI-powered threats indicate an informed perspective. Organizations, recognizing AI as an enabler of innovation and a potential vector for attacks, appear keenly aware that they must balance their pursuit of AI benefits with the need for rigorous security measures to protect against AI-powered threats.

100% of organizations will prioritize gaining visibility into their entire pipeline for AI deployments.

Recommendations for Securing the Cloud

Cloud-native security in 2024 requires a comprehensive, multifaceted approach with strategic attention on longstanding challenges and emerging risks. Researchers at Palo Alto Networks suggest prioritizing five key areas.

1 Consolidation with Platformization

Consider using a centralized security management platform that will follow you on your journey to cloud maturity and protect your applications and data end to end. As organizations expand their cloud and diversify their architecture usage, a holistic, architecture-agnostic approach to cloud security becomes essential for optimal visibility, control, and automation.

A strategic way to prepare for new cloud security requirements is to start with a platform vendor that can expand into your future use cases, encompassing both application and operations security. In this way, your security teams can quickly respond to new requirements, reduce training costs, and greatly simplify integration of new security capabilities.

Make sure policies and secure development environments are in place for your developers so your security teams aren't starting from behind.

2 Adopting AI Securely

AI is playing a tremendous and quickly growing role in application development—including GenAI-accelerated code development, corporate data used as training data, and applications leveraging newly trained AI models.

These trends heighten cloud security challenges. Because AI-generated code can lead to faster proliferation of misconfigurations, vulnerabilities, and bugs, be sure to regulate AI usage.

Protect your software supply chains and enable your developers to raise their code security posture ahead of their applications reaching production. Automate sensitive data discovery to ensure that sensitive data isn't used in model training.

Applications written to leverage these models also need to be protected. Make sure policies and secure development environments are in place for your developers, including your AI developers, so your security teams aren't starting from behind.

3 Intelligent Data Security

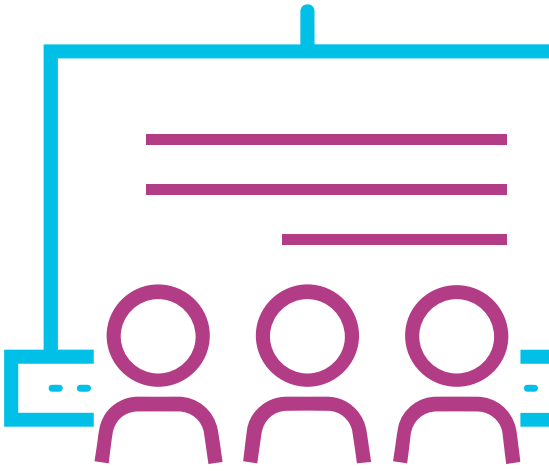
Implement a data security strategy that defines how sensitive data will be protected, regardless of where it's stored. The strategy should include measures to encrypt data, control access to data, and monitor data for suspicious activity. Policies should be enforced through technical controls and regular security audits.

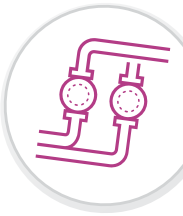
Invest in an automated data discovery and classification solution. Data security posture management (DSPM) with data detection and response (DDR) can scan large volumes of data quickly and accurately, including data stored in unstructured formats, such as text documents and images. Choose cloud security tools that include a large number of global best practices and compliance reporting out of the box. This will prepare your security team for new audit requirements that appear quickly from innovative businesses.

Regularly review and update data security measures to ensure they effectively address the evolving threat landscape, and train employees on data security best practices. Employees need to be aware of the risks of data breaches and how to protect sensitive data. Security teams should provide training on data security best practices and regularly remind employees of these practices.

Employees need to be aware of the risks of data breaches and how to protect sensitive data.

Security teams should provide training on data security best practices and regularly remind employees of these practices.





Regardless of how often you push code to production, observe how frequently security becomes a gating factor.

4 Reduce Traffic Jams in Your DevOps Pipeline

Evaluate your DevOps maturity and workflows. Regardless of how often you push code to production—daily, weekly, or monthly—observe how frequently security becomes a gating factor. Understand the extent of vulnerability cleanup your software engineers must perform prior to releasing an application. For improved efficiency and reliable security, consider implementing a secure-by-design approach.

5 Install Proactive Security Measures

Appreciate that security and development teams have different workflows and performance metrics. Each camp targets a unique agenda and approaches it from a unique perspective. Although both teams work to support the organization, they often work in opposition. If you don't deliberately, strategically, 100% commit to building a DevSecOps culture, your business outcomes are at risk.

If you don't deliberately, strategically, 100% commit to building a DevSecOps culture, your business outcomes are at risk.

How Palo Alto Networks Helps

Palo Alto Networks Prisma Cloud secures applications from code to cloud, across multicloud environments.

The platform delivers continuous visibility and threat prevention throughout the application lifecycle, including zero-day threats at proven scale. With Code to Cloud™ coverage that encompasses code, infrastructure, workloads, data, networks, web applications, identity, and API security, Prisma® Cloud is the platform that addresses organizations' security needs at every step of their cloud journey.

Prisma Cloud enables security and DevOps teams to effectively collaborate to accelerate secure cloud-native application development and deployment. The platform is integrated to simplify management and tool consolidation, and its modular pay-as-you-go architecture allows organizations choice of security use cases and various cloud service providers as needed.

Methodology

The fourth annual State of Cloud-Native Security survey was conducted between December 20, 2023, and January 17, 2024, using an email invitation and an online survey. The respondent population comprised 2,800 executives and practitioners from development, information security, or information technology departments across four key regions: NAM (US, 36%), EMEA (DE, FR, UK, 21%), LATAM (BR, MX, 14%), and APJ (IN, SG, AU, JP, 29%).

Additionally, this survey sampled input from all major industries, garnering representation from consumer products and services, energy resources and industrials, technology, media and telecommunication, financial services, and healthcare.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 1.9 percentage points for the Global Sample, 3.1 percentage points in NAM, 4.0 percentage points in EMEA, and 3.5 percentage points in APJ, from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

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 by Palo Alto Networks

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, check out www.paloaltonetworks.com/prisma/cloud.

paloalto® NETWORKS | PRISMA® CLOUD