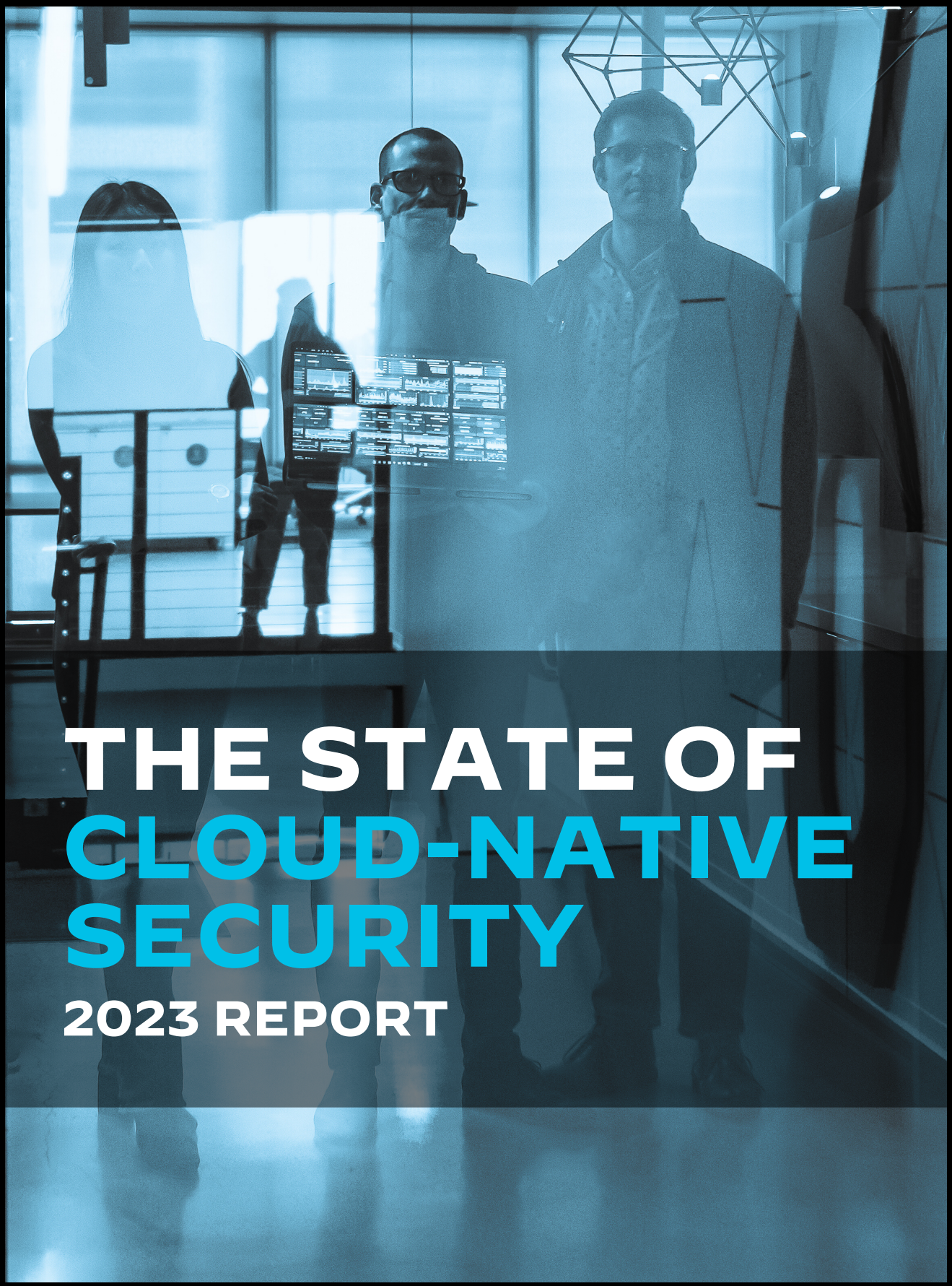
2023



THE STATE OF CLOUD-NATIVE SECURITY

2023 REPORT

PRISMA® CLOUD BY PALO ALTO NETWORKS | paloalto® NETWORKS

THE ONLY CONSTANT IS CHANGE

Few can relate to the adage like cloud security professionals.

Cloud security is dynamic and unpredictable, but the move to hybrid work has accelerated change and increased the complexity of application security. As cloud-native application development evolves, so too do organizations' cloud infrastructure (80% of survey respondents say their cloud infrastructure is evolving). What's more, the cloud has changed the applications lifecycle, with DevOps now delivering production code at warp speed and security personnel struggling to keep pace.

More than 75% of respondents from this year's survey are deploying new or updated code to production weekly, and almost 40% are committing new code daily. Add to that the ratio of ten developers for every security professional[1,2] and the potential for challenges in scale and complexity are not difficult to understand.

In contrast to on-prem environments, cloud computing follows a shared responsibility model. Responsibility for the infrastructure (e.g., compute, networking, and storage) is held with the cloud service provider (CSP) and responsibility for security is shared between the CSP and their customers. But the sharing stops when it comes to responsibility for customers' applications, data, and access management. Organizations' security and development teams own this responsibility and must collaborate to successfully secure their cloud environments.

To equip these teams with the resources they need, it's necessary to understand the challenges they face (whether emergent or perennial), the solutions they use, and the effectiveness of solutions in helping them meet their responsibilities.

How are organizations choosing security tools, and how are those tools being operationalized? Which practices are producing the best security outcomes, and which are hampering efforts? We explored these questions and others in our annual multi-industry survey on the state of cloud-native security.

1 Occupational Outlook Handbook - Software Developers, Quality Assurance Analysts, and Testers, Bureau of Labor Statistics
2 Bureau of Labor Statistics, Occupational Outlook Handbook - Information Security Analysts, Bureau of Labor Statistics

WHAT DID WE FIND?

Shift-left security is accelerating.

Since unaddressed vulnerabilities can be exploited in production, it's critical to catch and fix these vulnerabilities early in the application development lifecycle. Our survey revealed that risks introduced early in application development are the #1 concern. Known vulnerabilities, embedded malware, and sensitive data, such as secrets or configuration data, are some examples of early risks. To catch emergent threats upstream, security teams turn to tools such as code repo scanning, software composition analysis (SCA), and registry scanning.

Decisions on tooling have become clouded by complexity.

Overwhelmed by the proliferation of discrete tooling options, more than 75% of respondents reported that their organization struggles to identify which security tools can help them meet their needs. The sheer number and role of each discrete tool can present operational headaches and further isolate silos, often creating blind spots in an organization's security posture.

Collaboration across teams is essential to better security outcomes.

Unlike traditional security, the cloud requires users to unite disparate teams around a common goal. To do this, organizations need to be intentional about breaking down silos. Our survey shows 81% of enterprises have embedded security professionals in their development and operations team. From here, organizations must stay attuned to friction as it arises and develop a security architecture that inspires confidence and doesn't slow DevOps processes down.

TABLE OF CONTENTS

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

Fielded from November 21 to December 14, 2022, the survey gathered data from 2,500-plus respondents in seven countries, including the United States, Australia, Germany, France, Japan, Singapore, and the United Kingdom.

- All major industries were included in the 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 $1B in annual revenue).
  - Respondents were split evenly between executive leadership and practitioner-level roles to understand sentiments broadly across organizations. Practitioner-level respondents were restricted to those who work in development, IT or information security functions.

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

Palo Alto Networks partnered with The Fossicker Group, a majority woman-owned, full-service research firm, on all elements of this year's report, including survey design, fieldwork, analysis, narrative, data visualizations, and report design.

CLOUD MIGRATION IS STILL GROWING

Similar to years past, organizations in 2023 have shifted toward more public hosting of their cloud workloads.

Fifty-three percent of cloud workloads are hosted on public clouds, an increase of 8% in the past year. Platform as a service (PaaS) and serverless were the dominant application execution environments.

Regionally, we did not identify significant differences in cloud workloads hosted publicly among North America (NAM), Asia, Pacific, and Japan (APJ), and Europe, the Middle East, and Africa (EMEA).

Application Execution Environments

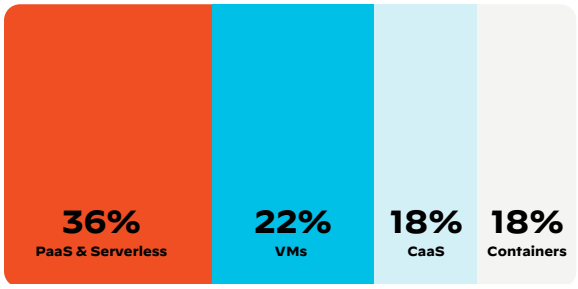


Figure 1. % Workload Distribution by Architecture Type, 2023

Cloud Workloads Publicly Hosted by Region

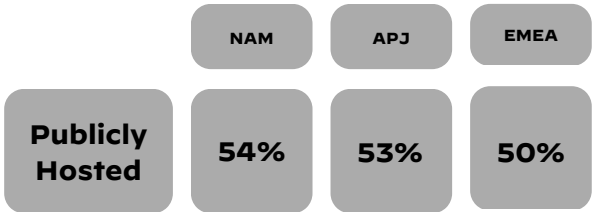


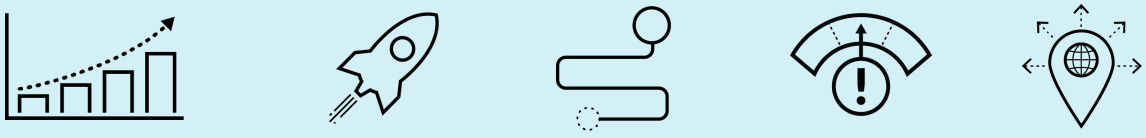
Figure 2. % Cloud Workloads Publicly Hosted by Region, 2023

What drives organizations to expand to the cloud?

The top reason is building new and expanding existing products and services, followed closely by the desire to increase efficiency and agility.

But security considerations continue to impede the ability of enterprises to address risks and take advantage of the cloud.

Top Five Reasons for Expanding to the Cloud



- Building new and expanding existing products and services
- Increasing efficiency and agility
- Creating new processes and workflows
- Mitigating business and regulatory risk
- Expanding into new markets

CLOUD MIGRATION DOES NOT ALWAYS EQUATE WITH CLOUD-NATIVE APPLICATIONS

Cloud native and lift and shift were the two most used methodologies for application deployment to the cloud, both preferred by a 10% margin to refactor or rebuild.

This is the first time cloud native is at the forefront in application development.

Deployment to the cloud differed among the three regions. NAM had a higher proportion of cloud-native development compared to APJ and EMEA. APJ was split almost evenly between the three methods and EMEA had the highest percentage of lift and shift among the regions.

Primary Method of Application Deployment to the Cloud

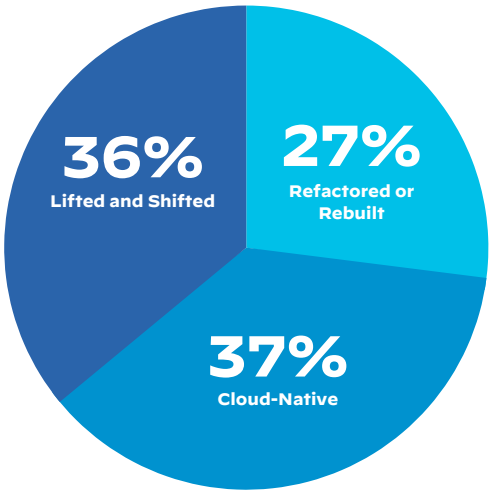


Figure 3. Primary Method for Application Deployment to the Cloud, 2023

Method for Application Deployment to the Cloud by Region

	NAM	APJ	EMEA
Lifted and Shifted (Migrated application to the cloud as-is or with only minor modifications)	35%	32%	40%
Refactored or Rebuilt (Migrated application to the cloud with significant modifications)	25%	34%	26%
Cloud-Native (Net new applications that were completely built in the cloud)	40%	34%	34%

Figure 4. Primary Method for Application Deployment to the Cloud by Region, 2023

OVER TWO-THIRDS REPORTED HIGHER CLOUD TCO THAN EXPECTED

On average, organizations spent the largest proportion of their total cost of ownership (TCO) toward application migration costs.

Despite this, all but one respondent said they will be expanding their cloud in the future. Survey respondents reported a 13% increase of workload moved to the cloud since the previous year and expect a further increase of 11% in the next 24 months.

Perhaps not surprisingly, a greater number of C-suite respondents calculate TCO as higher than expected (70%+) vs practitioner-level respondents (63%). Related to this, almost 60% of C-suite respondents reported higher than expected security costs as compared to less than 50% of practitioners.

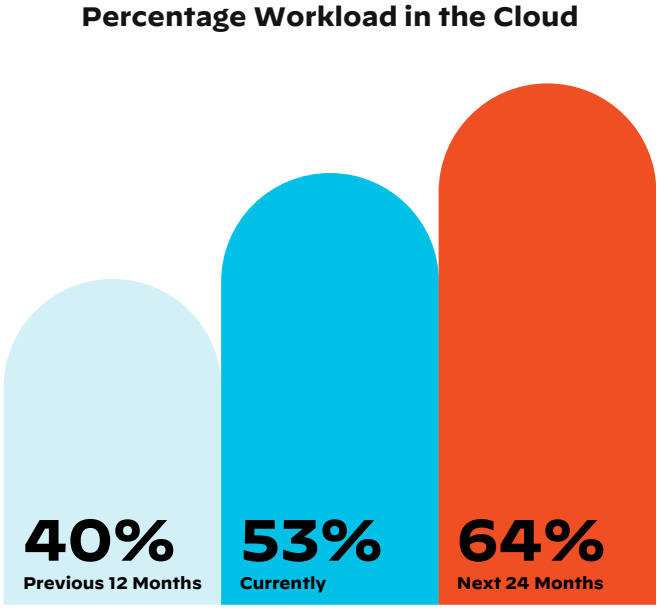


Figure 5. Percentage Workload in the Cloud, 2023

In the next 24 months, respondents expect an 11% increase in workload moved to the cloud.

NOW TRENDING:
#CLOUDMIGRATION

Cloud migration is forecasted to continue, but what does that really mean? It depends who you ask.

For a cloud architect, cloud migration means utilizing a mix of application migration methods, such as lift and shift, refactoring, and cloud-native development. Depending on timelines, budget, underlying technology, and corporate compliance, each method can take a different path. These architectural decisions result in a mix of workload technologies to run the applications, such as serverless, containers (self-hosted or managed), platform as a service (PaaS), and virtual machines (VMs). VMs are still a dominant architecture for hosting workloads, but serverless and PaaS are expected to experience further growth, as 70+% of respondents reported an expected increase in usage over the next 24 months.

For a developer, migrating to the cloud is an opportunity to adopt DevOps and accelerate the application development lifecycle. In fact, 77% are deploying new or updated code to production weekly, and 38% are committing new code daily. With respondents reporting that deployment frequency has increased by 67% in the past twelve months, it's clear that the drive from code to cloud is only accelerating.

For a security professional, the challenge in migrating to the cloud is about more than the migration of apps and data. Modern architectures and tech stacks for building, deploying and running applications require a new approach employing application-aware tools, products, and methodologies. In view of the expansive attack surface, securing cloud-native architectures must be the security professional's objective.

APPLICATION VELOCITY IN CLOUD-NATIVE ENTERPRISES

Two-thirds of all enterprises say that deployment frequency has increased or significantly increased over the past year, and 38% of enterprises deploy code to production or release to end users every day, with 17% deploying multiple times a day.

A third of enterprises reported operating with internal SLOs (service level objectives) of less than a day of lead time for changes, and 38% expected service restorations within a day.

Sixty-eight percent of all survey respondents reported increased deployment frequency. What's more, 64% also reported increased lead time for changes.

Frequency of Deployment of Code

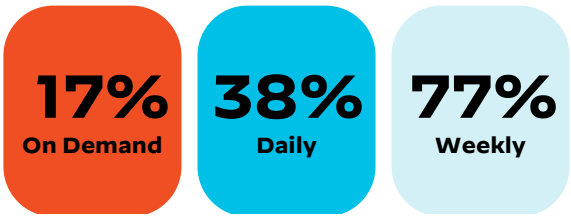


Figure 6. Frequency of Deployment of Code to Production or Release to End Users, 2023

Deployment frequency and lead time for changes measure velocity. So if enterprises are not achieving and sustaining their velocity performance goals, it can point to inefficiencies in the DevOps process. Increases in both arenas may suggest that pressure faced by security professionals (who are outnumbered by developers 10:1) is taking a toll amid increases in application velocity.

We went a step further and looked at how nimble enterprises were responding to change, specifically deployment frequency and their lead time for change in the last 12 months.

Among cloud-native enterprises, more than 60% reported an increase in deployment frequency in the previous year. For that same period, only 48% reported an increase in lead time for change.

Changes to Deployment Frequency over the Last 12 Months

	Total	Cloud-Native	Non-Cloud-Native
Increased	68%	61%	68%
Stayed the Same	22%	28%	22%
Decreased	10%	11%	10%

Figure 7. Changes to Deployment Frequency Over the Last 12 Months, 2023

OBSTACLES TO CLOUD ADOPTION AND EXPANSION

Over-tooling leads to an overly complex cloud environment.

Although application and workload cloud migration is high, the growth rate is slightly lower than last year. Some of this can be attributed to current macroeconomic conditions. When asked about the challenges they have faced in moving to the cloud, the top five responses given by organizations were not financially related. In fact, budget only increased as a concern by 2 points from 2020. Compared to three years ago, the greatest change came in reporting on the "lack of talent," which increased by 11 points.

Interestingly, the top five concerns are inextricably linked to the top-ranked concern — technical complexity. Complex environments require higher levels of talent and adaptiveness to changing technology, are more difficult to secure comprehensively, more difficult to gain visibility across, and result in greater compliance challenges.

When looking at C-suite and non-C-Suite responses, the C-suite rated lack of talent or consulting services as a bigger challenge than non-C-suite respondents (aka, those likely to be implementers) who viewed technical complexity as a greater challenge to cloud migration.

On average, organizations rely on 30+ tools for overall security and six to ten tools dedicated to cloud security.[3] Upwards of 75% of our State of Cloud-Native Security survey respondents reported that the number of cloud security tools they use creates blind spots that affect their ability to prioritize risk and prevent threats. Why are so many tools being utilized? It's telling that 77% of organizations struggle to identify what security tools are necessary to achieve their objectives.

Complexity, it seems, is impeding security, and that's a problem. Greater than 60% of organizations surveyed have been operating in a cloud environment for three or more years, but technical complexities and maintaining comprehensive security still hamper their cloud migration efforts.

3 What's Next in Cyber, Palo Alto Networks

Top 5 Challenges in Moving to the Cloud

1. Technical complexity
2. Lack of talent and/or consulting services
3. Maintaining comprehensive security
4. Lack of visibility across services and providers
5. Meeting compliance requirements

77%

of organizations struggle to identify what security tools are necessary to achieve their objectives.

76%

of respondents say the number of cloud security tools they use create blind spots.

IMPLICATIONS FOR SECURITY TEAMS

As vulnerabilities and misconfigurations move upstream, new application-level risks are emerging.

Of the five security metrics we analyzed, less than a quarter of respondents saw outcomes similar to last year. Over the previous 12 months, key security metrics worsened.

Ninety percent of respondents say their organization cannot detect, contain, and resolve threats within an hour. Regarding visibility into vulnerabilities across cloud resources, more than 30% of respondents indicated that lack of visibility created a challenge to ensuring comprehensive security. While compliance violations were at the bottom of the list, 25% of organizations still experienced a significant compliance violation.

Top 5 Security Incidents

1. Risk introduced early in application development
2. Workload images with vulnerabilities or malware
3. Vulnerable web applications and APIs
4. Unrestricted network access between workloads
5. Downtime due to misconfiguration

Five Key Security Metrics

Mean time to detect

Mean time to remediate

Number of breaches

Number of intrusion attempts

Unplanned downtime

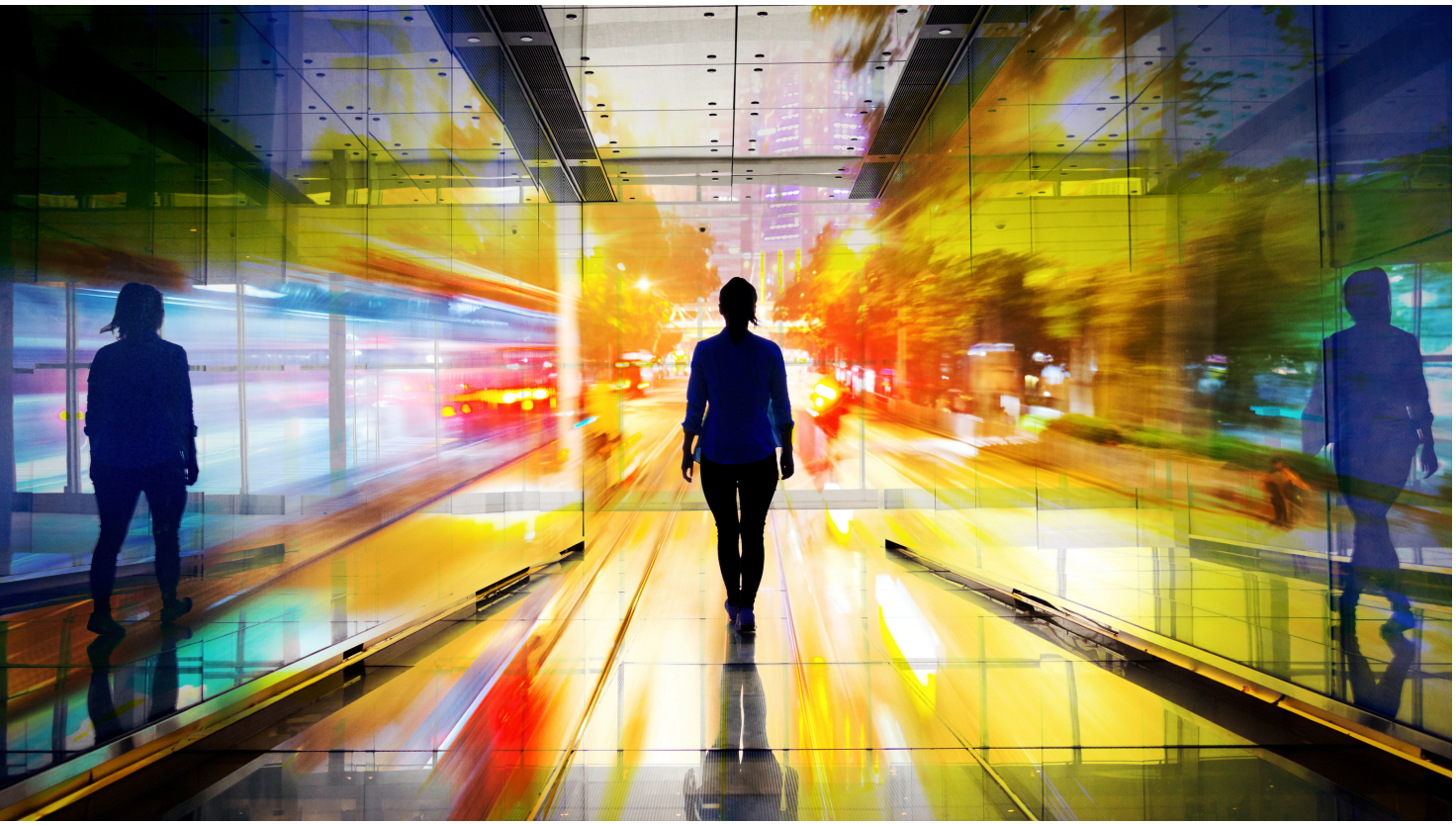
90% of organizations cannot detect, contain, and resolve cyber threats within an hour.

There's a limit, though, to how much shift-left responsibility developers can and want to handle.

More than 75% of respondents said that developers are held accountable for writing insecure code, and more than 80% said they understand their responsibility to deliver security across the development lifecycle. Security is not their primary responsibility. Security teams should provide development teams with the tools they need, according to 80% of survey respondents.

Organizations have largely distributed responsibility for designing and implementing cloud security policies and procedures to individual teams (78%). But nearly half (47%) of respondents report that the majority of their workforce does not understand their security responsibilities.

Ultimately, security teams are caught between responding to app teams and securing an increasingly complex cloud environment comprising multiple layers in the cloud stack — infrastructure, networks, VMs, containers, serverless functions, data, APIs, web apps, code, open source libraries, etc.



THE TOP CHALLENGES TO PROVIDING COMPREHENSIVE SECURITY

1

Managing holistic security across teams

Breaking down silos and creating processes that teams can adhere to make all the difference when it comes to comprehensive security. In addition to a shared responsibility model between cloud service providers and cloud users, there is another shared responsibility model within organizations. Development, operations, security teams, and every stakeholder along the application development lifecycle share responsibility. Effective collaboration between teams is important, regardless of how good security tools are. One of the central topics today is shift-left security. To effectively go upstream and prevent vulnerabilities at source before deployment requires aligned teams and security products with value to every member contributing to the app development lifecycle.

2

Embedding security across the cloud-native development lifecycle

In addition to the collaboration between development, operations, and security teams, it's vital to embed the right cloud security solutions at every stage of the application development process from code to runtime. Based on our data, it's clear that organizations continue to add new tools to their lineup.

3

Training IT/development/security staff to use security tools

Cloud-native application development has created the need to secure exponentially more cloud assets across code, workloads, identities, data, etc., and across multiple execution environments, such as containers, serverless, and PaaS. Utilizing multiple point tools to address each environment presents the challenge of ensuring staff are proficient with each tool.

4

Lack of visibility into security vulnerabilities across cloud resources

The holy grail of application security is vulnerability management — prioritizing and addressing vulnerabilities as they arise. To be effective, cloud security needs to mirror the scale, speed, and agility of the cloud itself. Scanning periodically is insufficient. A cloud security solution needs to provide continuous and near real-time detection of misconfigurations, vulnerabilities and threats across the full application lifecycle. Only then are organizations able to react quickly and effectively to the detection of a breach or vulnerability.

5

Finding the correct tools to address security needs

Not all organizations are at the same stage in their cloud adoption journey, nor do all embrace the same methodologies in their approach to cloud adoption. While some organizations develop applications exclusively in the cloud, others use a lift and shift approach. The ideal cloud security solution addresses immediate security requirements while enabling organizations to expand for additional use cases as their cloud maturity increases. A company that begins with cloud configuration visibility and guardrails, for instance, may discover a requirement to secure a containerization project or open source software 12 months down the road. Adopting a platform designed with flexibility and choice in its architecture ensures future-proof cloud security.

78% **of respondents agree that cloud security needs more out-of-the-box visibility and risk prioritization filtering with minimal learning.**

HOW ENTERPRISES ARE APPROACHING CLOUD SECURITY

Best-in-breed security capabilities and ease of use rose to the top as the most important factors when choosing security solutions.

Top 5 Factors in Choosing a Security Vendor or Tool

Ease | Best-in-breed capabilities | Potential impact on performance | Familiarity with vendor and/or tool | Competitive pricing and/or cost

Competitive pricing and cost also made the top five factors, which comes as no surprise given that cloud security costs were higher than expected for more than 50% of enterprises.

When we looked at how organizations are securing their clouds, networks, data and applications, we found that enterprises are split between a single security vendor/tool approach and a multiple security vendor/tool approach for each of their security needs.

When it came to securing their cloud, a quarter of respondents also used in-house and open source tools. This approach was not as common for network security (17%) or application security (19%). However, more surprisingly, 9% of respondents still primarily rely on their cloud service provider to ensure cloud security measures are in place across their environment.

Primary Source of Security

	Cloud Service Provider	One Vendor/Tool	Multiple Vendors/Tools	In-House/ Open Source	None/Don't Know
Cloud Security (Visibility, Compliance, Governance, Identity and Access Management)	9%	29%	33%	26%	3%
Network Security (Web Application Firewall, Microsegmentation)	9%	33%	37%	17%	5%
Application Security (Code Security, Runtime Security, etc.)	9%	35%	34%	19%	4%

Figure 8. Primary Provider of Cloud Security for Different Aspects of Cloud Development, 2023

Even after deploying multiple tools, enterprises have experienced significant security incidents with gaps in response efficacy and efficiency.

Only about 10% of respondents can detect, contain, and resolve threats in less than an hour. An increased number of breaches was reported by 39% of respondents, and more than 30% reported a significant increase in intrusion attempts and unplanned downtime. What's more, 68% of organizations are unable to detect a security incident in less than an hour and, once detected, 69% cannot respond to the threat in under an hour.

Overall, security threats and incidents are getting more difficult to detect and contain.

42%
reported an increase in mean time to remediate

39%
reported an increase in number of breaches

36%
reported an increase in unplanned downtime

HOW APPLICATION DEVELOPERS ARE SHAPING SECURITY

Where collaboration is concerned, 80% of respondents agreed that developers understand their security responsibilities across the development lifecycle.

The same percentage (80%) of respondents reported that security professionals are embedded in their development and operations teams — especially in the design phase.

This year we found that 75% of respondents reported a higher than usual turnover rate in DevOps and 73% reported a higher than usual turnover rate in cloud security roles.

In 2022, 54% of respondents had teams of more than 30 people. This year, only 16% reported teams of 30+ members, while 58% reported cloud security teams of less than 20 people. Many factors likely contributed to this decline in team size, including hiring constraints, the expectation that fewer security team members are required after a significant cloud investment, and the decision to outsource security tasks to manage security service providers (MSSP).

We're seeing deeper level engagement between application developers and security tools/teams, especially in the design phase. But while developers embrace tools and processes that help them code secure applications, there's a limit to how much shift-left responsibility they can and want to handle. As with security professionals, stress appears to be taking a toll. The seamless integration of ease-of-use security tools and teams into the DevOps workflow are important to reduce security friction for application teams.

75% of respondents reported a higher than usual rate of turnover in DevOps roles.

THE PATH FORWARD

As we know, applications were traditionally built as monoliths and placed behind firewalls.

But building, deploying, and running applications in the cloud is a more complex endeavor, especially with the increased agility and efficiency afforded by DevOps. In response, cloud security solutions must provide visibility into, and place barriers at, emergent points of vulnerability. They must meet organizations where they are, catering to their unique needs and priorities.

Our data shows that security teams are looking for an integrated platform that provides visibility across their entire ecosystem. Specifically, more than 80% of respondents said they would benefit from a centralized security solution that sits across all of their cloud accounts and services. What's more, more than 75% of organizations said that the number of point tools they use creates blind spots.

As seen in figure 8, organizations are using between six to ten tools to secure their cloud infrastructures. While this may have its advantages in some areas, our data shows that it's not the most effective way to ensure strong security outcomes.

The protection of cloud workloads requires a comprehensive and proactive approach. It requires investment in 1) technology that's effective and appropriate for where you are on your cloud journey and 2) a significant investment in people, processes, and the ability to break down silos between application and security teams.

Even with best-in-class solutions, good security outcomes can't be achieved without partnership across teams. As technologists, we often forget that what matters most in business is people. In light of increasingly complex cloud environments and expanded attack surfaces, policies and practices that ease friction and distribute responsibilities across teams are essential.

Top Five Priorities for Cloud Security

1. **Data protection**
2. **Application security**
3. **Runtime security**
4. **Vulnerability management**
5. **Identity and access management governance**

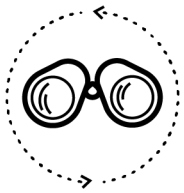
More than 80% of respondents said they would benefit from a centralized security solution that sits across all of their cloud accounts and services.

Recommendations and Best Practices

Palo Alto Networks researchers recommend focusing on these strategic areas in cloud security:

Embed Security Earlier in the Application Lifecycle

Identifying and preventing security issues early in application development helps reduce risks in production by orders of magnitude. Security teams should understand how the organization codes, builds, deploys and runs applications in the cloud. With this knowledge, they can then identify the least disruptive insertion points for security in the CI/CD pipeline. Starting by raising visibility and fix-recommendations for software with known vulnerabilities and container image scanning is a great first step towards getting early buy-in from DevOps or platform teams.



Implement Continuous Cloud Visibility

A pivotal step in making cloud security and compliance easier is eliminating blind spots. Most organizations start with discovering cloud assets, misconfigurations and vulnerabilities. Additionally, it's important to be aware of anomalous or suspicious behaviors that indicate a compromise. Visibility should be continuous and near real time, enabling security teams to answer "who, what, when, and where" for anything happening in their organization's cloud environments.

Adopt Threat Prevention Techniques

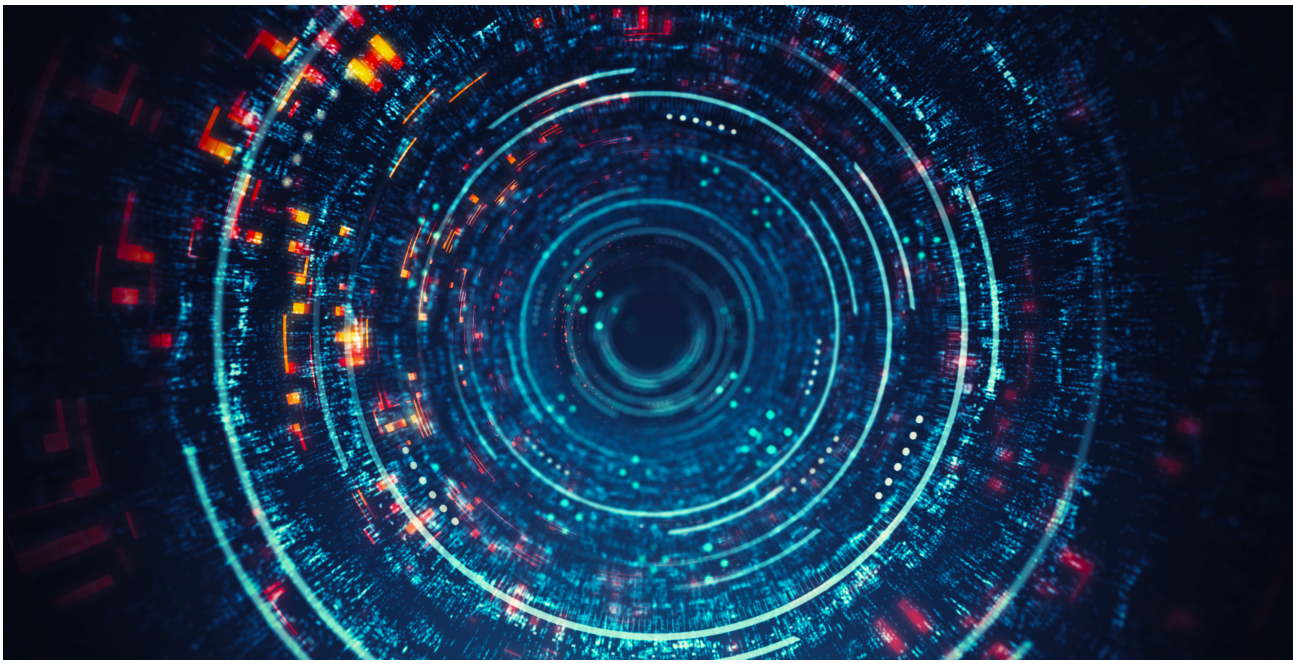
Fixing misconfigurations and known vulnerabilities can significantly reduce the risk of security incidents, but it won't stop insider threats or the undetected breach. Consider adopting threat prevention tactics that can actively block zero-day attacks and contain lateral movement in the event of a breach. Prevention also provides compensating controls during times when developers can't patch known application vulnerabilities. Use preventative techniques that include calculating net-effective permissions across your cloud resources to ensure you follow best practices for least-privilege access for your users. At the very least, organizations should consider applying prevention solutions to their mission critical applications.

Align Your Cybersecurity Tactics with Your Cloud Journey

Security can become a roadblock for cloud migrations and expansions, which is why thinking about the end game is important. Many organizations fall into a trap of adopting a new security technology for each new immediate use case, leading to a sprawl of siloed tools that bog down cloud security teams and leave visibility gaps. Instead, review your organization's cloud adoption goals over the next two to five years (e.g., containerization, serverless, APIs, CI/CD pipelines, open source tools) and seek solutions that meet both current and future priorities.

Consider Tool Consolidation

Unifying data and security controls into a platform approach can go a long way. While siloed tools can cover critical use cases, they don't provide a clear view of risk. By consolidating tools, security teams can automate correlation and tackle the most important security issues across the application lifecycle.



HOW PALO ALTO NETWORKS HELPS

Palo Alto Networks Prisma Cloud platform 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 different cloud providers as needed.

ABOUT

Palo Alto Networks

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

Prisma Cloud

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

PRISMA CLOUD BY PALO ALTO NETWORKS | paloalto NETWORKS

About the 2023 Cover

The cover art for this year's report is an original image taken at Palo Alto Networks' headquarters in Santa Clara, California. Team members Kathleen Qin, Ivan Melia, and Mohit Bhasin stand behind a prismatic glass partition whose surface reflects multiple layers of the headquarters' interior design elements. The image's dimensional, mosaic-like composition is a visual reference to one of the report's key findings–that technical complexity is impeding security and creating blind spots.

Photo Credit: David M. M. Taffet, invisibleman.photography