Techstrong Research

Top Five Cloud-Native Risks

COMMISSIONED BY PRISMA CLOUD

DANIEL KIRSCH
Principal Analyst and
Managing Director

MITCHELL ASHLEY
Principal

CONTENTS

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

Executive Summary

THE PANDEMIC, along with current economic and societal upheavals, has turbo-boosted the enormous, rapid adoption of cloud technologies. Today, nearly 70% of organizations host more than half their workloads in the cloud, up from just 31% in 2020[1]. As cloud migration continues, many organizations struggle with application development security. Our research that includes regularly engaging with and interviewing security, DevOps technical and line-of-business leadership across industries and has identified the top five risks facing organizations as they adopt cloud-native approaches to application development and deployment:

Cloud-Native Vulnerabilities

1. Application vulnerabilities
2. Infrastructure misconfigurations
3. Malware
4. Overprovisioned access
5. Insecure APIs

[1]The State of Cloud Native Security Report 2022

COMMISSIONED BY PRISMA CLOUD BY PALO ALTO NETWORKS

While these challenges are familiar, cloud-native software development requires new protections. Cloud-native development requires you to rethink your approach to security. Adopting a "shift left" approach toward security as well as DevSecOps methodologies is helping top-performing organizations successfully deploy cloud applications and services.

There isn't a single approach to decreasing the risk of cloud-native development. We have developed five best practices that balance the benefits of cloud-native development, including faster development times at reduced costs with security. We recommend:

Best Practices

1. Adopting a team mindset
2. Reducing complexity with a platform approach
3. Choosing cloud-native tools and technology
4. Automating security
5. Gaining visibility across all data and workloads

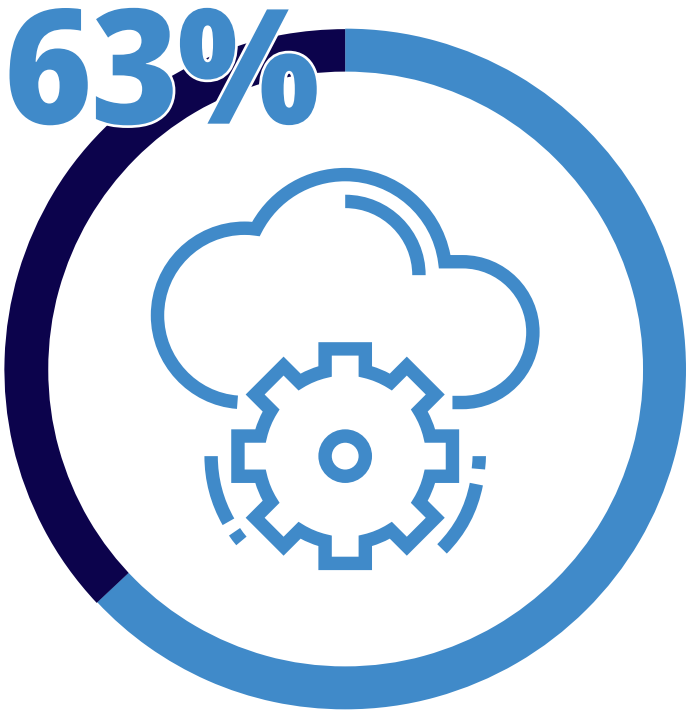
COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

Introduction

Increasingly, businesses are adopting or accelerating cloud-native software development, hoping to gain the speed and continuous improvement needed to drive strategic digital transformation, application modernization, and greater competitiveness. The vast majority of applications are expected to be cloud-native by 2025.

While cloud architectures can deliver application velocity and agility, organizations making the transition are learning a difficult truth: Cloud-native also introduces new risks.

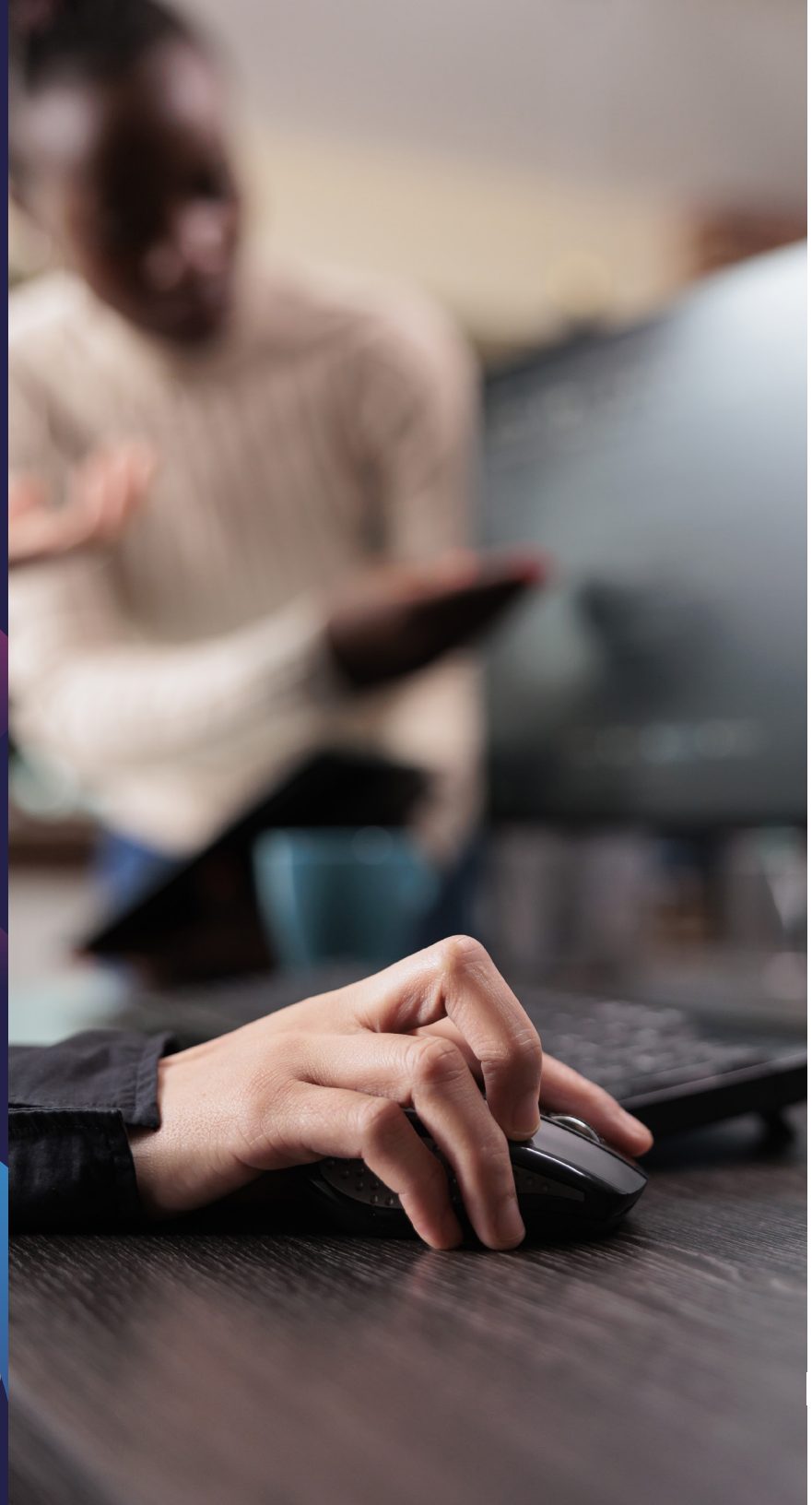
In the cloud, continuous integration practices can shorten cycle times and improve efficiency. But in this dynamic, complex, multi-cloud workscape, which makes heavy use of open source, it's difficult for security teams to keep pace.



of Rapid Expanders who successfully expanded their cloud adoption also integrated DevSecOps principles.

Source: www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2022

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS



COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

Although cloud-native technology is still developing, its security challenges are familiar. Even so, security in this new environment can't be approached simply as an off-premises version of data center security. Continuous and secure application delivery in this new environment demands new security strategies.

Developing modern defenses for cloud-native development starts with recognizing the most common risks, then understanding the crucial role that DevSecOps can play in protecting against them. Indeed, "shifting security left" into the hands of developers is increasingly critical. New industry research has found that best-in-class organizations excel in integrating cloud security touchpoints into the full development life cycle, from build to runtime.

Designing security into applications at every stage helps balance the age-old tension between speed and security. Successful organizations recognize DevSecOps as a powerful opportunity to move away from seeing security as a roadblock to productivity and their chief security officer as "Doctor No."

In this report, we'll identify and discuss the top five cloud-native security risks and what enterprises can do to protect against them. We'll share research on why it's critically important to identify risks early in the DevOps process. Finally, we'll close with approaches and best practices to effectively mitigate these risks to enable safe, secure cloud expansion.

UNDERSTANDING CLOUD-NATIVE SECURITY:

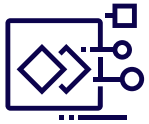
The basics of cloud-native applications

Let's start with a quick level-set of terms and concepts. As the cloud matures and becomes more sophisticated, the way that cloud applications are developed and supported also evolves. Cloud-native applications are software designed with microservices, containers and dynamic orchestration for continuous delivery. Every part of a cloud-native application is housed within its own container. These are dynamically orchestrated with other containers to optimize the way resources are utilized.

Cloud-native applications are:

CONTAINERIZED. A standard way to package applications that is resource efficient. More applications can be densely packed using a standard container format.

DYNAMICALLY MANAGED. A standardized way to discover, deploy and scale (up and down) containerized applications.



MICROSERVICES-ORIENTED. This method decomposes the application into modular, independent services that interact through well-defined service contracts.

This approach radically changes how we think about application creation and management.

CLOUD-NATIVE SECURITY

These strategies mitigate the challenges of non-monolithic cloud architectures ; notably, the lack of fixed parameters, diagnostic difficulties and development velocity. Key elements include inventory and classification, compliance management, network security, identity and Access Management (IAM), data security, workload security and vulnerability management.

CLOUD-NATIVE PROTECTION PLATFORMS (CNAPP)

These provide total, unified visibility across silos, helping DevOps, SecOps and cloud infrastructure teams deliver full-stack security. A single platform responds, protects and automatically mitigates vulnerabilities and misconfigurations across the entire build-deploy-run life cycle. Also known as cloud-native security platforms (CNSPs).

DEVSECOPS

Rather than keeping development, operations and security separate, DevSecOps combines them into a single practice. (Figure 1). Many companies have already developed DevOps practices; DevSecOps is the next step. It begins with 1) a change in culture based on ongoing learning (to raise security awareness with developers who may already be entrenched in DevOps processes) and 2) the empowerment of security experts to determine the best ways to embed security into application development.

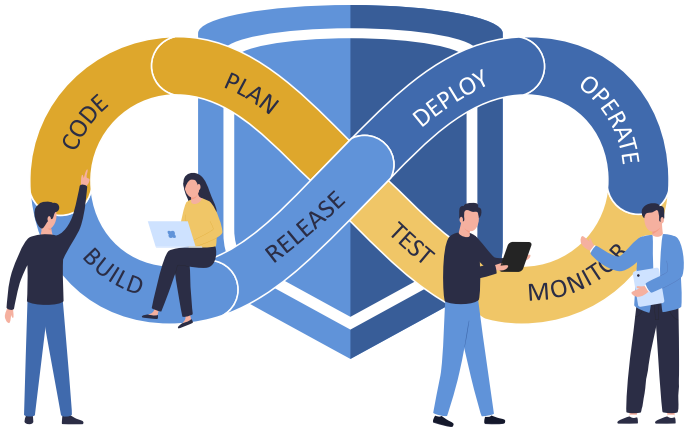
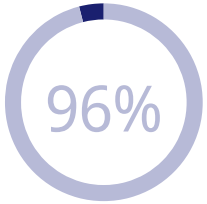


Figure 1

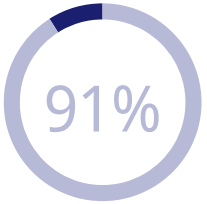
The benefit of DevSecOps is higher-quality, fully tested code, designed securely and delivered more quickly. Properly done, the approach can reduce the risk of vulnerabilities further down in the application development life cycle.

Although DevSecOps is largely about corporate culture and processes, a successful implementation requires technology and tools. Typically, they add automation and integration to smooth application delivery.

The Top Five Cloud-Native Risks



of third-party container applications deployed in cloud infrastructure were found to contain known vulnerabilities



contain at least one "critical" or "high" vulnerability in the images

Application Vulnerabilities

As we've noted, cloud computing environments are increasingly defined and controlled by containers, infrastructure-as-code (IaC) and Kubernetes. With this shift, both DevOps and cloud teams continue to prioritize the identification and remediation of security issues early in the design cycle.

While both groups are "security aware", neither, however, is expert. So there's an increasing need for developer-friendly approaches that help identify security issues in code (application and cloud configurations), while also providing automation and built-in best practices. Lacking these, the biggest risk for many organizations can come from the development process itself and the open nature of cloud-native development and supply chains.

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

Infrastructure misconfigurations

Complex cyber- attacks by criminal and state-sponsored actors get much of the world's attention. But cloud misconfigurations and unpatched software are likely your biggest cloud security threats. The infamous theft of information on 100 million customer loan applications from Capital One, for example, was enabled by intentional misconfiguration of an opensource web application firewall.

Misconfigurations leave the door open for network exploits and ransomware attacks. Think of cloud configurations like the front door to your house, but with a key difference If you skip one of the dozen steps, criminals are ready to rush in. Errors at one stage can cascade and multiply across a chain of dependencies. (Figure 2)

The most common configuration mistake is leaving ports open; any port left open to the internet provides hackers with an attack vector. Other widespread errors include leaving secrets like passwords and encryption keys poorly protected (by using common passwords), not enabling secure backups (to protect from ransomware) and not providing a way to ensure that your security team has visibility into all of your cloud workloads.

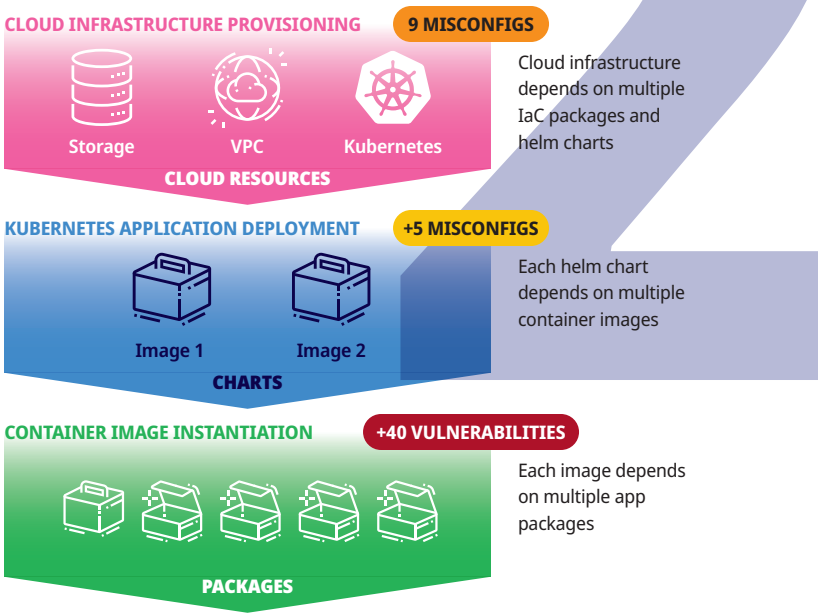
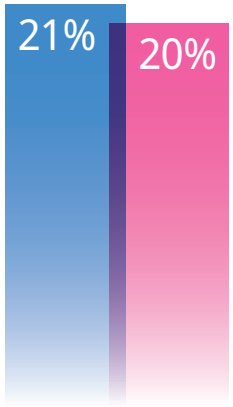


Figure 2: Chain of dependencies in a modern cloud-native application

Although misconfigurations may seem like a mistake easily remedied with a DevOps checklist, fixing them is complicated. And complexity is only increasing, thanks to rapid growth, especially in hybrid and multi-clouds. Even hyperscalers are not immune.



21% of the security scans run against the large SaaS provider's customer's development environment resulted in misconfigurations or vulnerabilities (industry average 20%)

Automation is the only way to help developers avoid the potentially costly mistake of misconfiguring a cloud environment. To be effective, automation platforms should immediately alert DevOps teams to a misconfiguration and prevent common misconfigurations from going into production.

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

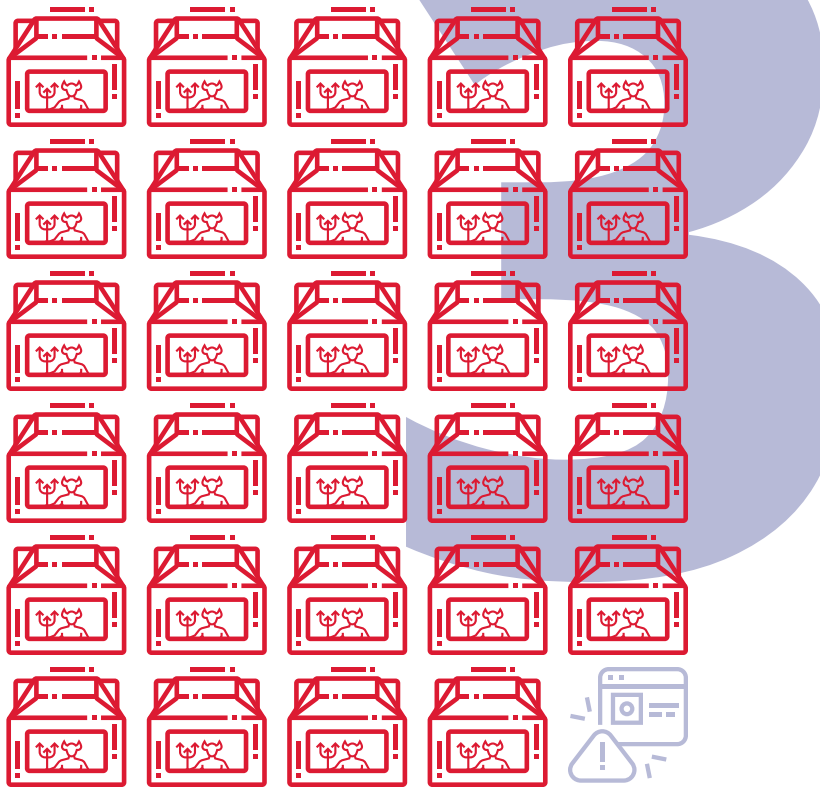
Malware

Malicious software, as enterprises know all too well, has grown in sophistication through the years. Rather than using brute force, threat actors now are willing to lie in wait or traverse complex networks to launch their attacks. Malware isn't new, of course, and most security teams and security operations centers (SOCs) are well-versed in the most common and even obscure malware. But methods continue to evolve in the cloud.

Consider cryptojacking – the illegal use of someone else's computing resources to mine cryptocurrencies. Containers offer attackers a simple, effective way to distribute malicious cryptominers.

A big challenge with spotting potential cloud-native malware is that many security tools are "noisy." That means the platform provides too many alerts to reasonably respond to, creating "alert fatigue." If alerts aren't prioritized, the proverbial "red flashing light" is likely to be missed.

Security teams don't need more alerts – they need threat intelligence that correlates alerts with other network and application activities.



An in-depth look into Docker Hub found 30 malicious images downloaded 20 million times

Overprovisioned access

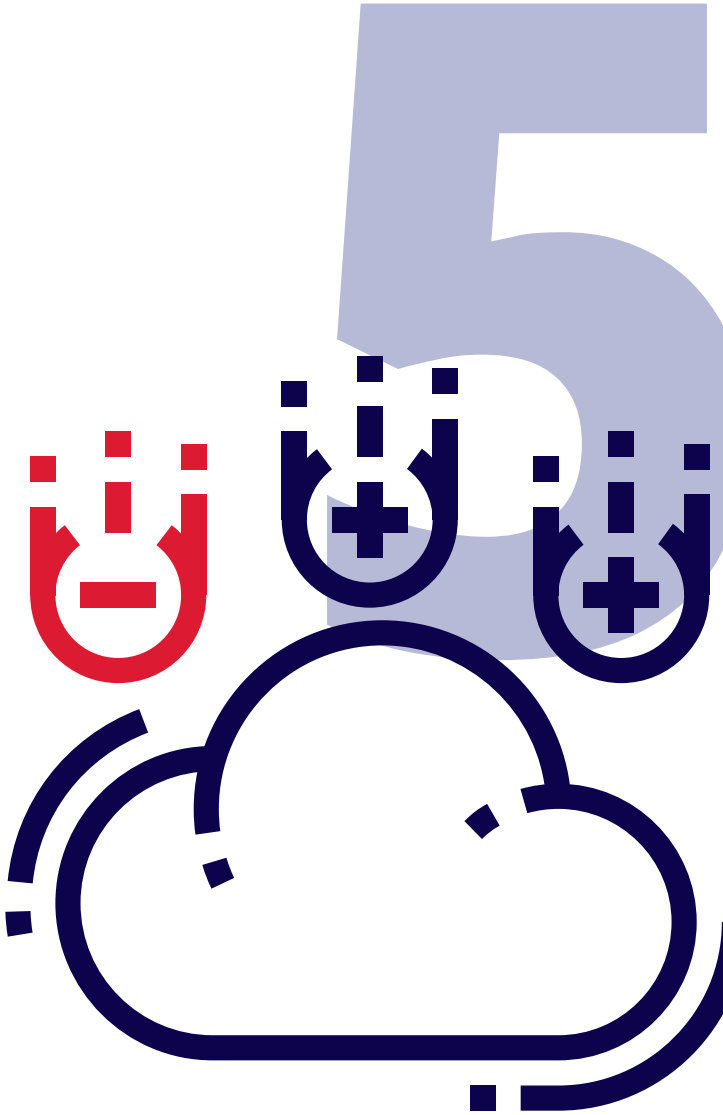
To streamline work, it's common for users to get access to applications, workloads, data and other resources that they don't need. This introduces the idea of role-based access control (RBAC), along with the principle of providing customized privileges. However, business users also need to get their job done. They'll quickly grow frustrated if required to keep asking security for increased access.

Overprovisioned access opens your organization up to two major cloud security threats – malicious insiders and, more frequently, cybercriminal takeovers of insider accounts that have been overprovisioned. We all know where that leads.

By addressing overprovisioned access, your organization can begin to take a zero-trust approach to security. One aspect of Zero Trust is to enable your security organization to ensure that no employee, partner or customer has access to data that you have not explicitly allowed.

One recent global study found that **99% of cloud users, roles, services and resources were granted excessive permissions.**

Insecure APIs



Poor API security across applications and systems puts your organization at great risk. That's because APIs are the lifeblood of the cloud-native and app-based economies.

Failing to adequately manage the security of APIs creates a new host of challenges and questions. Who is using what APIs? Are your APIs updated? Did your DevOps team evaluate the security of your APIs during their selection process? Have you formalized the way your organization is evaluating API security?

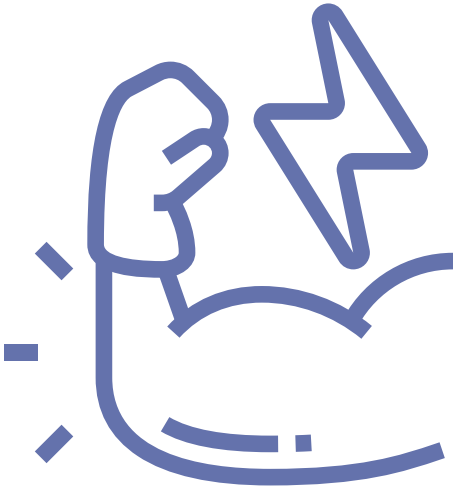
An API that is compromised, unsupported or outdated can offer an easy attack vector for cybercriminals. Vulnerabilities here raise legitimate and serious questions about an organization's approach to application security and about the usefulness of its web application firewalls (WAF) and encryption protocols.

It's increasingly clear: An API breach can lead to the downfall of your entire digital software strategy, to say nothing of your cloud-native development efforts. This criticality is rapidly making — or should be making — API security a top priority for enterprise software professionals and security teams.

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

Best Practices

*Organizations that tightly integrate DevSecOps principles are **over 7X more likely** to have strong or very strong security posture.*



Cloud-native development is on the rise. The global number of cloud-native developers grew to nearly 7 million last year. Analysis by the DevOps Institute shows the cost of fixing top risks at various stages of cloud-native development, including Unit Testing, Full Build, Integration Testing, and System Testing.

Based on Techstrong Research's work with clients, we offer the following as best practices that organizations can take to "shift left" and secure their cloud development pipelines.

1. MORE THAN EVER, TREAT SECURITY AS A TEAM SPORT. Security needs to be involved with development projects at the earliest possible point. There are many software offerings to help with this process, but "shifting security left" requires a culture change, as well. If you don't, you'll likely face one of two consequences: Projects will slow to a crawl as required security measures are bolted on or the schedule will be met at the expense of adequate security.

The shift from traditional structures to DevOps united development, operations and engineering teams. Now, the evolution to DevSecOps requires further expansion of the roster. It's crucial that security architects, engineers and other cybersecurity professionals are also involved in the cloud-native life cycle. As the Head of Technology for Sky, Europe's leading media and entertainment company explained: "Our view of technology has to evolve to ensure it is useful for the people using it because every decision has an almost immediate impact."

2. REDUCE COMPLEXITY AND VENDORS WITH A PLATFORM APPROACH. DevSecOps integration and security automation are necessary components to achieving successful cloud adoption. It's obvious but bears repeating; high cloud spend does not equate to successful cloud development or adoption. Rather, success with DevOps in a cloud-native environment hinges on moving from a tangled web of disjointed solutions to a comprehensive platform. Research shows that consolidation of multiple security vendors leads to successful cloud adoption efforts. Integrated tools can help prevent changes that cause breaks and otherwise mitigate risk by overlaying vulnerabilities, misconfigurations, dependencies and networks, to name a few, into context.

3. USE SECURITY TOOLS AND TECHNOLOGY DESIGNED FOR CLOUD-NATIVE DEVELOPMENT.

Building effective cloud-native applications requires making complex, interlocked decisions about architecture, development and operations. DevSecOps teams require purpose-built tools and platforms that enable external configuration, health and metrics monitoring, service registry and service discovery, dynamic scheduling, multi-cloud implementation and a host of other new practices. Similarly, DevSecOps in cloud-native environments needs the ability to scan container images to identify vulnerabilities, for example – something that conventional tools simply cannot do. Ditto for the ability to scan infrastructure-as-code (IaC) before it is deployed into production. Such tools can use automation to embed security into workflows in DevOps tooling for Terraform, CloudFormation, Kubernetes, Dockerfile, serverless and ARM templates, to cite other examples.

83% of those who were successful using DevSecOps in rapid cloud expansion **used five or fewer vendors**

4. AUTOMATE SECURITY IN YOUR CLOUD-NATIVE ENVIRONMENT. Traditional security reviews break agile development methods and slow the business down. Centralized incident and event management systems look for anomalous data and processes to safeguard the company IT assets. Automation is available everywhere, from configuration management and patching tools to database integrity monitoring and insider threat detection. It's the only way to prevent unintended breaches from happening in the first place.

A new global survey by the DevOps Institute says automation focuses teams on high-value development tasks, while reducing stress and burnout. They advise "automating the heck out of your environment."

Automation is essential to complex distributed systems for rapid development and continuous improvement with

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

frequent releases. As manual efforts are too slow and error-prone to guarantee that, robust automation for a cloud-native application helps keep the app well-tested, secure, reliable and scalable.

5. GAIN CLOUD VISIBILITY ACROSS VENDORS WITH UNIFIED MANAGEMENT. Visibility into all of your cloud-native workloads and data, regardless of vendor, is the only way to ensure that your environment is secure. You need a solution that can use your cloud providers' APIs to provide visibility and control. Not just over your overall cloud infrastructure, but more granular control over containers and serverless elements as well. It's important to choose a solution that isn't tied to one vendor or cloud. While you might be using a single cloud today, you want to be prepared for multi-cloud when the time comes.

About the authors

DAN KIRSCH, managing director and co-founder of Techstrong Research is a consultant, IT industry analyst and thought leader focused on how emerging technologies such as AI, machine learning and advanced analytics are impacting businesses. Dan is focused on how businesses use these emerging technologies to alter their approaches to information security, governance, risk and ethics. Dan provides advisory services directly to leadership at technology vendors that design and deliver security solutions to the market. Dan is a co-author of *Augmented Intelligence: The Business Power of Human-Machine Collaboration* (CRC Press, 2020), *Cloud for Dummies* (John Wiley & Sons 2020) and *Hybrid Cloud for Dummies* (John Wiley & Sons, 2012).

Contact: *dan@techstrongresearch.com*

MITCHELL ASHLEY serves as principal at Techstrong Research where he is part of a team of preeminent experts in digital transformation, DevOps, cloud-native and cybersecurity. In this role, he works with companies to align digital transformation and technology strategies to achieve disruptive goals and high-impact results. Mitch also serves as Techstrong Group CTO, is in demand as a speaker and is widely followed online on his podcasts, his *Analyst Corner* commentary and interviews on the highly popular Techstrong TV streaming video program where he engages with top digital and tech leaders from across the industry.

Contact: *mitchell@techstrongresearch.com*

COMMISSIONED BY
PRISMA CLOUD
BY PALO ALTO NETWORKS

About Techstrong Research

Techstrong Research accelerates the adoption of disruptive technologies that drive business outcomes and provide actionable strategies in rapidly changing markets. We are the only organization serving the needs of IT leaders, practitioners and the industry ecosystem with research, analysis, content, events and education. We bring deep knowledge about today's leading technologies such as DevOps, cloud, data and AI/ML, security/governance initiatives and supporting infrastructure. We offer our customers a holistic business perspective essential to adapt and thrive in the digital economy. The Techstrong Research team has the knowledge, experience and credibility earned by working with hundreds of businesses across many industries to provide consulting, thought leadership and research services.

Techstrong Research is relentlessly focused on the business outcomes of disruptive technologies.