

# How to Take the Friction Out of Cloud Security

The move to hybrid work has accelerated cloud adoption in a range of government organizations. Cloud drives new efficiencies and can help make government more responsive. But cloud security is dynamic and unpredictable. As cyberthreats get more sophisticated, security teams risk falling behind.

Today's security teams spend an average of 145 hours to resolve a security alert, according to the latest [threat report](#) from Palo Alto Networks®. Meanwhile, bad actors can exploit a newly disclosed vulnerability within 15 minutes.

## The Challenge: A Complex Array of Point Products

Cloud security isn't becoming any easier. In an increasingly adversarial environment, it's effectively becoming harder. Risks are everywhere in the cloud, from misconfigurations and vulnerabilities in code, to infrastructure entitlements that allow overly permissive access.

Organizations of all sizes will typically find themselves managing a wide array of disparate solutions as they ramp up applications and processes in the cloud. This approach risks adding complexity and straining already stretched IT talent. Heterogenous tools make the task of safeguarding applications increasingly difficult.

"Having multiple point products creates more complexity, which in turn drives an unmanageable number of security alerts that typically don't help to pinpoint threats or offer any prioritization of greatest organizational risk," said David Kubicki, senior solution architect manager for Prisma® Cloud public sector at Palo Alto Networks.

A talent gap makes the problem worse, as agencies struggle to hire individuals with expertise in a variety of different toolsets. All this in turn leads to insufficient security (or less complete security) because of disjointed policy management.

With agencies across the board struggling to manage the vast number of tools they have within their cloud environments, a better approach is needed.



## The Solution: A Cloud-Native Application Protection Platform

Organizations need a single cloud-native application protection platform (CNAPP) that can protect users and data throughout the development cycle. A CNAPP combines functionality for Cloud Security Posture Management (CSPM), Cloud Workload Protection platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM) and continuous delivery/continuous deployment (CI/CD) security into a unified, end-to-end solution to secure cloud-native applications across the full application lifecycle.

With a robust CNAPP, you can:

- **Protect workloads and applications at all stages.**

A CNAPP makes it possible to apply the same level of protection on both staging environments and production environments. That means having the capability to protect your workloads and applications across the entire development lifecycle.

A CNAPP gives your cloud infrastructure and DevOps teams full-stack security with complete visibility across silos. With a CNAPP, you get a single-platform approach to protect your applications not only at runtime, but throughout development workflows, enabling security teams to find, identify and fix flaws and issues early in the application lifecycle.

- **Consolidate tools and reduce IT workload.** To increase IT efficiency and reduce strain, you need to cut through existing complexity by consolidating tools within a single unified solution.

With a CNAPP, you can reduce the number of alerts for your security personnel, thus freeing up their time and elevating the overall security effort.

- **Deliver end-to-end visibility.** "A CNAPP is a consolidation of tools in a single platform that applies security to the cloud," said Chong Yi, Prisma Cloud account manager for federal civilian agencies at Palo Alto Networks. "That's significant, because you want to have that end-to-end visibility."

A typical attack path might come through the internet, with bad actors exploiting misconfigurations to get to storage where sensitive information is held. With end-to-end visibility into workloads, it's easier to prevent those misconfigurations and keep bad actors at bay.



## Spotlight: DevOps Meets Zero Trust

A recent Palo Alto Networks survey found that 81% of enterprises have embedded security professionals in their DevOps teams to help tackle tasks such as vulnerability management, compliance monitoring, policy enforcement and runtime protection. Organizations must stay attuned to potential friction between development and security teams, which could slow down DevOps processes and undermine confidence in the security architecture.

A Zero Trust approach requires open lines of communication between security professionals and the developers. Too often, siloed efforts get in the way.

One of the benefits of a CNAPP is that you can reduce those silos and enable communication. An intelligent CNAPP can provide vulnerability information during the build process, using tools that developers are most accustomed to seeing. It does this while maintaining security and making your security practitioners feel comfortable during deployment. All this helps communication flow more freely.

By bringing security and DevOps teams close together, a CNAPP makes it easier to build Zero Trust from the ground up. Close coordination helps ensure that robust security controls are applied consistently without getting in the way of application velocity. That's important for agency teams looking to leverage the power of the cloud to develop and deploy new applications in support of critical government missions.

### How Palo Alto Networks Can Help

Prisma Cloud from Palo Alto Networks elevates the security paradigm with a suite of code-to-cloud intelligence capabilities that are tailored to address the multifaceted security challenges of cloud-native applications.

With Prisma Cloud, security teams can save time in securing their applications and data while accelerating digital transformation. Prevent risks and misconfigurations from entering production, reduce your attack surface and establish continuous visibility and control over misconfigurations, privileges, data and vulnerabilities in your cloud environment.

Learn more about what Prisma Cloud can do for you:

<https://www.paloaltonetworks.com/state-of-cloud-native-security>

