PRISMA® CLOUD | paloalto® NETWORKS

Protecting Applications with Code-to-Cloud Intelligence

Generative AI Driving Explosive Growth of the App Economy

The cloud no sooner redefined the app economy and here we are again, witnesses of and participants in a seismic shift brought on by generative AI. By 2030, according to the McKinsey Global Institute, AI could contribute $13 trillion to the global economic output, with a significant portion originating from the application economy.[1] There are already reports of software developers completing tasks 56 percent faster using a GitHub AI Copilot than those not using the tool.[2]

The cloud, of course, continues to offer organizations a scalable, cost-effective platform for application deployment and management—with cloud providers delivering suites of services, effectively democratizing application development. Every modern enterprise now orbits around cloud applications.

Yet, the real momentum of today emerges from the synergy of cloud computing and AI. With cloud technologies now ubiquitous and AI increasingly accessible, enterprises can design applications tailored to their specific business needs. AI excels in sifting through vast amounts of data, unearthing patterns and trends once hidden from human eyes. Such insights pave the way for applications that resonate with both business objectives and customer preferences.

[1] Mckinsey & Company. 2023. *Economic Potential of Generative AI | McKinsey*. www.mckinsey.com. June 14, 2023.
[2] Peter Cihon et al., *The impact of AI on developer productivity: Evidence from GitHub Copilot*, Cornell University, Feb 13, 2023.

The Mounting Challenge to Secure Modern Cloud Applications

The rapid development of cloud applications has been noticed by cyber adversaries. As applications become central to modern business, they draw increased attention from malicious actors. Security teams struggle with the pace of development, which often outstrips the speed at which they can secure their applications. All the while, cyberthreats take on new levels of sophistication, making the task of safeguarding applications increasingly challenging. To put it in perspective, security teams spend an average of 145 hours (approximately 6 days) to resolve a security alert,[3] while bad actors can exploit a new vulnerability within 15 minutes of its disclosure.[4]

Risks are everywhere in the cloud, from misconfigurations and vulnerabilities in code to infrastructure entitlements that allow overly permissive access across systems and resources. The result is an unmanageable number of security alerts that typically don't help to pinpoint threats or offer any prioritization of greatest organizational risk. This leaves security teams in the constant position of making educated guesses on which security issues to work on first.

What You Don't See Should Concern You

Adding to the complexity of cloud security is the fragmentation in visibility and controls. On average, organizations juggle 31 security tools from 13 vendors.[5] This patchwork of point solutions often causes problems. In fact, 76% of organizations admit that the number of tools they use causes blind spots.[6] Noisy alerts pour in from multiple, independent sources, that makes discerning genuine threats from false alarms an incredibly difficult task.

The result is that cloud security has become a data analysis problem. Abundant data exists, but without proper contextualization, visualization and prioritization it's scattered across platforms and tools like a puzzle awaiting assembly. Many tools offer only a narrow view, focusing on specific security issues and providing limited scanning capabilities. Others offer tables of data that, despite their informative nature, miss the crucial correlations and linkages. The result is a broken landscape where security teams grapple for the context to understand the most critical risks to be addressed first, in order to protect their applications.

Fundamentally, the challenge revolves around not just possessing data but interpreting it. It demands the recognition of patterns, identifying contextual relationships between risks, cloud deployment, application criticality, and active threats to accurately prioritize the most critical issues.

The Power of Code-to-Cloud Intelligence

> Without context, a piece of information is just a dot. It isn't until we connect the dots with additional context that information becomes valuable.
>
> **— Michael Ventura, Essayist**

[3]Apr 18, and 2023. n.d. *Unit 42 Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface*, Palo Alto Networks. Accessed October 4, 2023.
[4]*2023 Unit 42 Attack Surface Threat Report*. n.d. Palo Alto Networks.
[5]Dec 13, and 2022. n.d. *What's next in Cyber*. Palo Alto Networks. Accessed October 4, 2023.
[6]*2023 State of Cloud Native Security Report*. n.d. Palo Alto Networks.

As cloud applications become increasingly central to business operations, a singular challenge stands out—the need for a unified, intelligent approach to security, one that spans the entire application lifecycle of code, build, deploy and run.

Code-to-cloud intelligence emerges as the answer, offering the ability to interconnect the signals from development to runtime to deliver valuable contextual security information.

Code-to-Cloud Intelligence Defined

Code-to-cloud intelligence is the ability to connect insights from the developer environment through application runtime to contextualize alerts, prioritize greatest concerns and offer remediations that effectively prevent risks and stop breaches. Recognizing this, it becomes clear that the traditional approach to securing cloud applications is insufficient.

Today's solutions for securing applications during development uncover high volumes of vulnerabilities, many of which are false positives. As individual point products, these application security tools lack the broader context needed to improve the fidelity of their outputs, such as knowing the cloud infrastructure their code will be deployed on. This low signal-to-noise ratio results in unnecessary alerts and overwhelms both developer and security teams.

Conversely, code-to-cloud intelligence empowers teams with a thorough and precise understanding of risks by focusing on exploitable issues, such as code deployed in production, executing on internet-exposed assets, or having access to sensitive data.

Similarly, cloud security teams operating with siloed point solutions spend too much time combing through alerts to identify which issues, or combinations of issues, expose their organization to threats. Moreover, while security teams recognize the priority to protect their organization's critical business applications, they typically lack visibility into these applications because their traditional security tools only have visibility to the cloud resources that host the application.

Code-to-cloud intelligence supercharges security teams with the awareness of the applications they're chartered to protect, including the resource components that comprise the application—the code, open-source and third-party software libraries, cloud infrastructure resources, and API endpoints.

With full contextual understanding of business-critical applications, security teams can effectively prioritize time and resources on the most critical risks. Root cause investigations can be accelerated with accuracy via comprehensive code-to-cloud insights.

With insights on security risks and incidents traced back to their corresponding code assets, cloud security teams can pinpoint organizational owners of at-risk applications and route remediations (e.g., via pull requests) back to their source so that issues are fixed permanently in code.

Code-to-Cloud Intelligence in Prisma Cloud

Prisma Cloud Code-to-Cloud Intelligence addresses challenges faced by security and development teams with innovative capabilities that redefine the expectations of a cloud-native application protection platform (CNAPP).

Building on the foundation of code-to-cloud intelligence, Prisma Cloud elevates the security paradigm with a suite of features tailored to address the multifaceted security challenges of cloud-native applications. With the power of Code-to-Cloud Intelligence embedded in Prisma Cloud, security teams can take a radically new time-saving approach to securing their organizations using these new capabilities.

AppDNA: Act Decisively with Rich Application Insights

Prisma Cloud AppDNA changes the way organizations view their multicloud estates. It discovers and organizes these estates, presenting an intuitive structure that inventories cloud applications and their DNA. This DNA encompasses the cloud services, infrastructure assets, compute workloads, API endpoints, data, and code that constitute these applications. By integrating additional cloud and business context, AppDNA paints a comprehensive picture of which applications are affected by risk, enabling organizations to prioritize remediation actions with precision and insight.

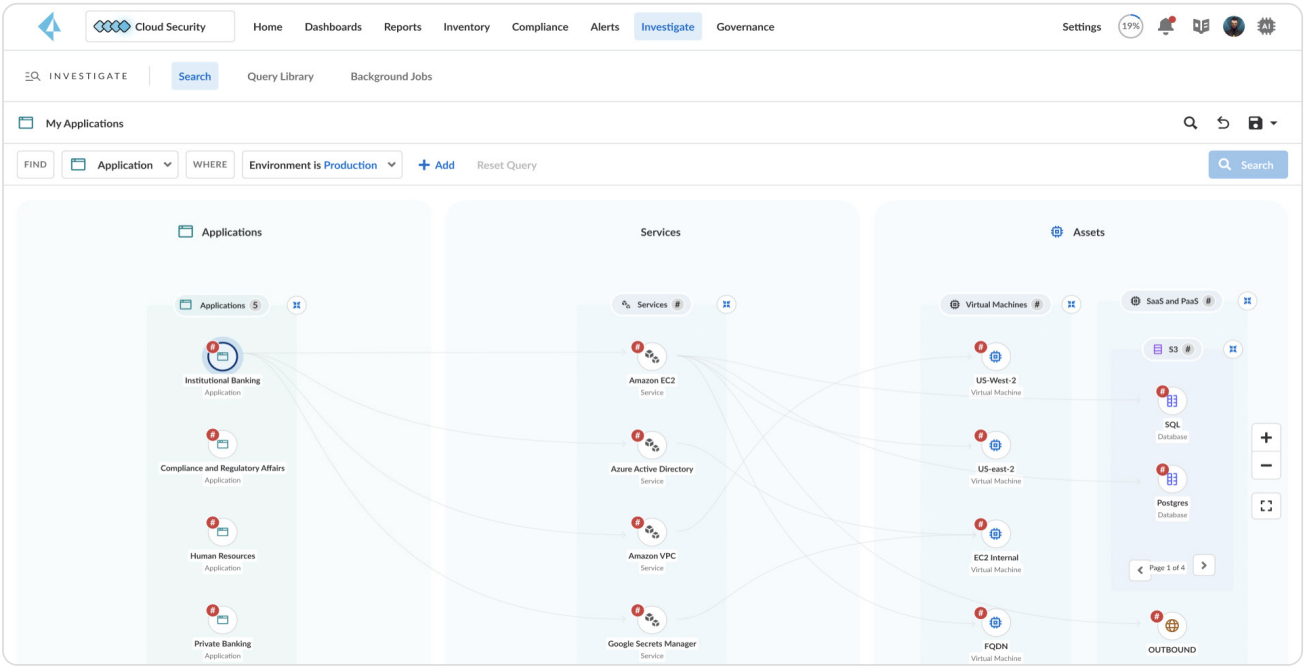

Figure 1: **AppDNA inventories every resource component that makes up the application.**

Infinity Graph: Explore All Angles from Code to Cloud

Navigating the intricate maze of cloud security becomes significantly simpler with Prisma Cloud Infinity Graph, which correlates the security stack across numerous parameters, including misconfigurations, vulnerabilities, exposure, identity and secrets, and sensitive data. By unveiling problematic alert combinations, the Infinity Graph brings insight from interrelated vulnerabilities forming attack paths that potentially lead to breaches. In this, connected alerts become actionable. What's more, Prisma Cloud overlays active compromise attempts on these paths, highlighting active threats and the importance of existing protections. Leveraging code-to-cloud intelligence, Infinity Graph traces discovered risks back to the vulnerable code and gives security teams the contextual details they need for swift and effective root cause analysis.

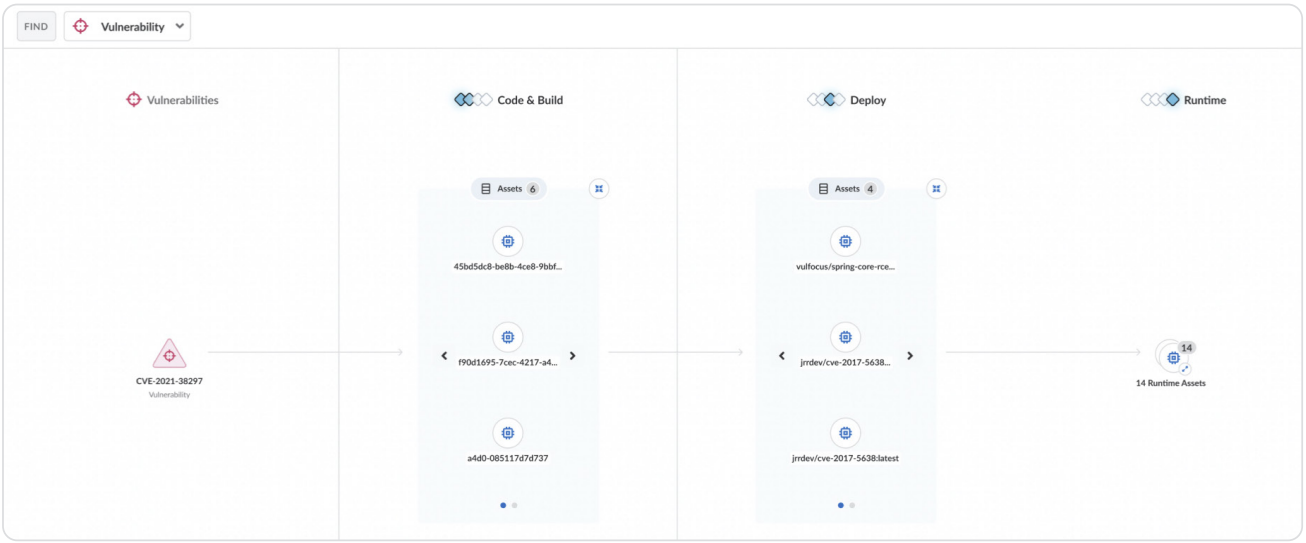

Figure 2: **Infinity Graph correlates the security stack and intuitively models attack paths.**

Code-to-Cloud Remediation: Zero in Quickly to Fix Now in Cloud and Forever in Code

Immediate action is often the difference between a hiccup and a catastrophe. With Code-to-Cloud Remediation, teams can address risks instantly in the cloud. Additionally, by issuing a pull request with the recommended package version or configuration change, developers can review and address the root cause, ensuring the issue will not reoccur in the cloud as software is continuously released to production. Every risk is traced back to its origin, simplifying the remediation process and eliminating the need for endless tickets in search of an owner. A streamlined approach to risk management ensures timely and effective action across all teams.

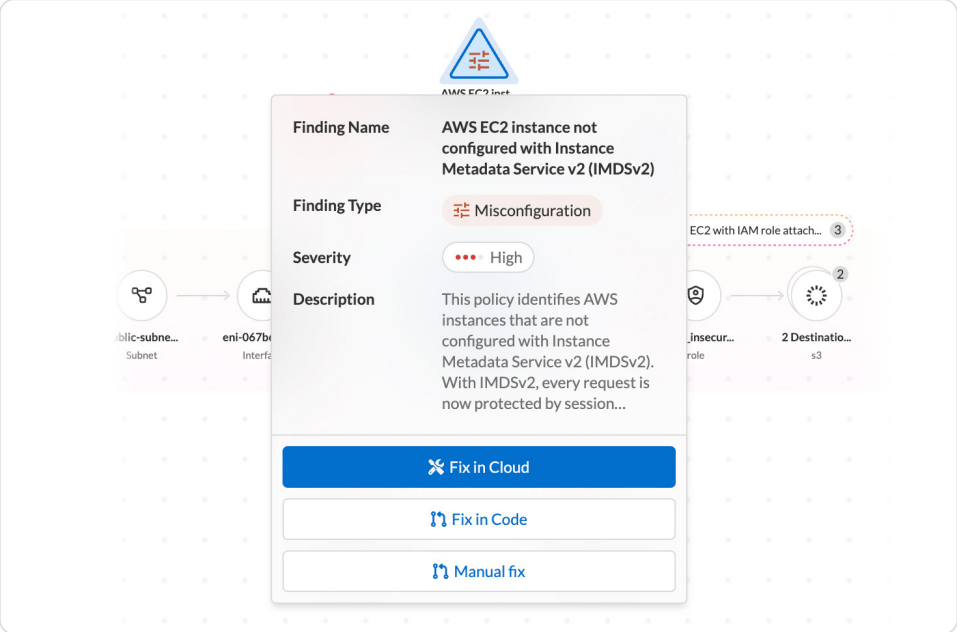

Figure 3: Code-to-Cloud Remediation enables you to easily fix issues in the cloud or open a pull request to fix the issue permanently in the code.

Code-to-Cloud Dashboard

Evidence and context are at the heart of effective decision-making. The new Code-to-Cloud Dashboard offers unparalleled visibility across the application lifecycle, extending even to the software supply chain. But it's more than just a monitoring tool. This dashboard is a powerhouse of analytics, providing in-depth insights at every stage of the software development lifecycle. Whether it's for day-to-day decision-making or reporting to leadership and boards, the dashboard stands as an invaluable tool for organizations, highlighting their risk trends and remediation progress across the application lifecycle.

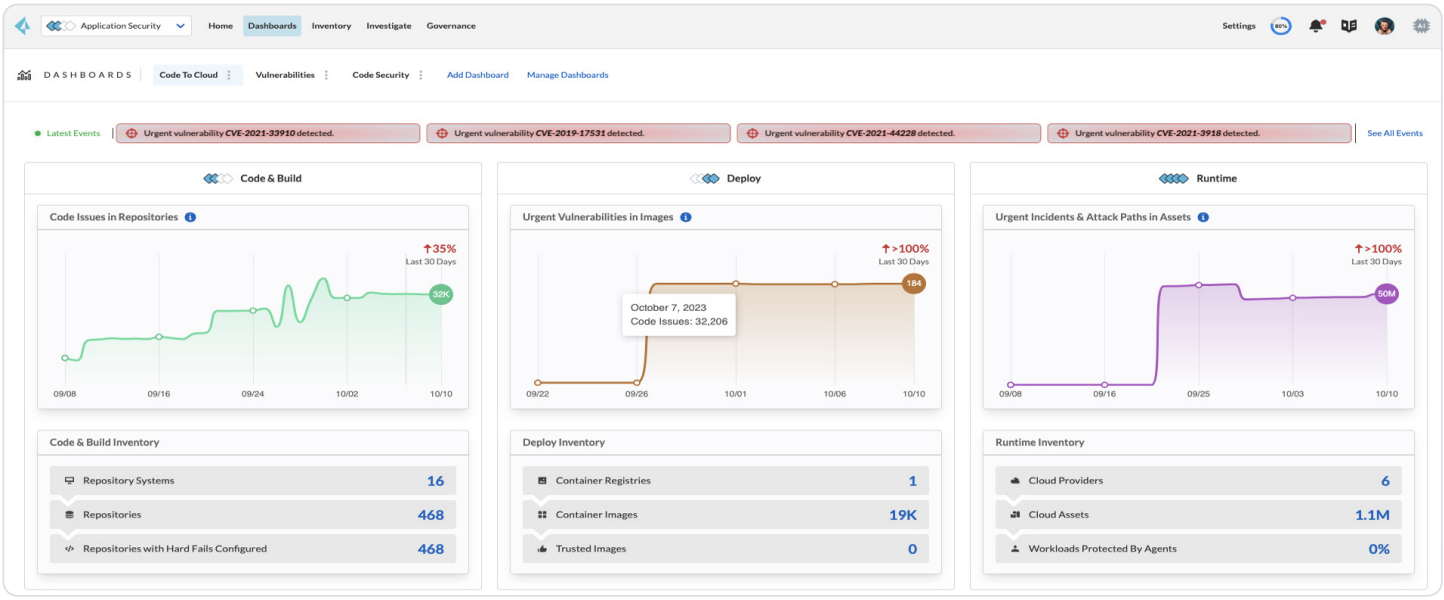

Figure 4: Code-to-Cloud Dashboard provides panoramic visibility across the entire application lifecycle.

The Prisma Cloud Advantage

Code-to-cloud intelligence isn't just another buzzword in the realm of cloud security. It's a paradigm shift, a comprehensive approach that promises to redefine how organizations secure their applications and cloud environments.

Prisma Cloud connects the all-important dots of application risk, security signals and runtime environments across the entire application lifecycle to deliver actionable context. Code-to-cloud intelligence represents a leap in cloud security, setting a new standard for what's possible.

Palo Alto Networks delivers the height of CNAPP excellence in Prisma Cloud. Seamlessly integrating every facet of cloud-native application protection, it offers unparalleled visibility across the entire application lifecycle. From code to cloud, Prisma Cloud's intelligence-driven approach ensures that security is woven into the fabric of your digital operations.

Learn more about Prisma Cloud and Code-to-Cloud Intelligence at

PALOALTONETWORKS.COM/PRISMA

paloalto NETWORKS | Cybersecurity Partner of Choice

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetwroks.com

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087