

# Prisma Cloud Delivers Context-Aware Software Composition Analysis to Secure Deployment of Open Source Software

September 20, 2022

*New SCA module offers proactive vulnerability remediation based on runtime context to achieve seamless code-to-cloud security*

SANTA CLARA, Calif., Sept. 20, 2022 /PRNewswire/ -- Open source software is a critical component of cloud-native applications, allowing developers greater speed and modularity without having to reinvent the wheel each time they code. However, as the [Unit 42 Cloud Threat Report, 2H 2021](#) found, open source software can often contain known vulnerabilities, which can open organizations up to significant risk. Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today introduced the industry's first context-aware software composition analysis (SCA) solution to help developers safely use open source software components. The integration of SCA into Prisma® Cloud further demonstrates why Palo Alto Networks is [the leading provider of cloud-native security](#).



Traditional SCA solutions are standalone products that can produce a large number of alerts but lack the runtime context to help fix vulnerabilities. With the addition of SCA to the Prisma Cloud platform, developers and security teams can proactively surface and prioritize known vulnerabilities that impact the application lifecycle (i.e., code, build, deploy and run). Prisma Cloud SCA delivers deep dependency detection and remediation of vulnerabilities in open source software before applications reach production. It can also help developers prioritize remediation based on software components that are already in use. These capabilities are not possible when SCA solutions are deployed as single point products.

"Developers leveraging open source software should be able to build applications with the confidence they aren't opening the organization up to risk," said Ankur Shah, senior vice president, Prisma Cloud, Palo Alto Networks. "With the average application consisting of [75%](#) open source components, SCA on Prisma Cloud is key to protecting the organization from code to cloud and empowering developers to build with speed."

As a complete cloud-native application protection platform (CNAPP), Prisma Cloud is context-aware at every stage of the application lifecycle to provide a unified view of risk across organizations' cloud environments. Where current approaches to cloud security rely on siloed products that provide intermittent visibility without remediation, Prisma Cloud approaches cloud security with a comprehensive, prevention-first framework. With [188%](#) increase in cloud incident response cases over the past three years, this shift in approach has become mandatory.

A complete code-to cloud CNAPP needs to incorporate the following five key principles in order to keep organizations safe:

- **Security from code to cloud** — protects applications at every stage of the development lifecycle — from code, build, deploy and run.
- **Continuous, real time visibility** — uses real-time and contextual security analysis of cloud environments to help prevent misconfigurations, vulnerabilities and threats.
- **Prevention-first protection** — stopping attacks and defending against zero-day vulnerabilities to drive down mean time to remediation.
- **Choice for every cloud journey** — aligning security needs with current and future cloud priorities by supporting a breadth of cloud service providers, workload architectures, continuous integration and continuous delivery (CI/CD) pipelines, integrated development environments (IDEs), and repositories with a unified platform
- **Cloud scale security** — consistently secures applications as cloud environments scale.

In addition to SCA and to further increase the safety of cloud-native applications, Prisma Cloud introduced a software bill of materials (SBOM) [among other capabilities](#) for developers to easily maintain and reference a complete codebase inventory of every application component used across cloud environments. Implementing SCA and SBOM ensures Prisma Cloud aligns with these principles.

"Buyers looking for cloud-native security solutions need to keep the requirements of microservices security protection in mind. The 'bolted-on' and 'whack-a-mole' approaches are a thing of the past," said Frank Dickson, program vice president, Security and Trust at IDC. "Security should be embedded throughout the application development life cycle. This means that buyers need to fundamentally change their approach to security, although they need to continue to protect their run-time environments, they must also embrace solutions that embed security in the application development process, an approach referred to as 'shift left.' Shift left requires one to think less about security products and more about continuous security processes."

## Availability

The new SCA module and SBOM capability in Prisma Cloud are generally available today.

## Additional Resources

- Read about Prisma Cloud SCA [here](#).
- Learn more about Prisma Cloud CNAPP [here](#).
- Register and join our November event: Code to Cloud Security Hour: The Rise of the CNAPP [here](#)
- Read more about why Forrester named Prisma Cloud a Leader in Cloud Workload Security [here](#).
- Follow Palo Alto Networks on [Twitter](#), [LinkedIn](#), [Facebook](#) and [Instagram](#).

## About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit [www.paloaltonetworks.com](http://www.paloaltonetworks.com).

*Palo Alto Networks, Prisma, and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners. Any unreleased services or features (and any services or features not generally available to customers) referenced in this or other press releases or public statements are not currently available (or are not yet generally available to customers) and may not be delivered when expected or at all. Customers who purchase Palo Alto Networks applications should make their purchase decisions based on services and features currently generally available.*



 View original content to download multimedia: <https://www.prnewswire.com/news-releases/prisma-cloud-delivers-context-aware-software-composition-analysis-to-secure-deployment-of-open-source-software-301627933.html>

SOURCE Palo Alto Networks, Inc.

Brendan Hillan, [bhillan@paloaltonetworks.com](mailto:bhillan@paloaltonetworks.com)