Palo Alto Networks Expands Prisma Cloud to Automatically Secure Unprotected Cloud Workloads and Propels Container Security Forward With Four Critical New Capabilities

April 28, 2021

Prisma Cloud Adds Industry's First Comprehensive Cloud Native Attack Framework to Protect Hosts, Containers and Serverless

SANTA CLARA, Calif., April 28, 2021 /PRNewswire/ -- Palo Alto Networks (NYSE: PANW) today is delivering innovations to Prisma® Cloud to help organizations ensure no workload is left unprotected. The new capabilities also increase automation and detection, simplify compliance checks, and deepen visibility into malware threats for containers and hosts. Additionally, Palo Alto Networks is unveiling the industry's first cloud native attack dashboard that extends the MITRE ATT&CK® framework.

"Organizations currently have large amounts of unprotected workloads and no efficient or unified way to secure them. Often, they are managing multiple, single-purpose security solutions to protect these workload stacks, which can create operational burdens and security gaps," said Varun Badhwar, senior vice president for product, Prisma Cloud, at Palo Alto Networks. "Today's new capabilities further our commitment to deliver comprehensive cloud workload protection across hybrid and multi-cloud environments. DevOps teams can now efficiently build and deploy their workloads and applications rapidly, while helping security teams deliver protection."

The new Prisma Cloud capabilities for cloud workload protection are:

- **Auto-Detection and Auto-Protection for Hosts:** Prisma Cloud now automatically detects unprotected virtual machines (VMs) running on AWS®, Microsoft Azure® and Google Cloud Platform (GCP®), and seamlessly deploys the Prisma Cloud Defender agent to help ensure that VMs are not left unprotected.
- **The Industry's First Comprehensive Attack Framework Spanning Threats to Cloud Native Workloads**: Prisma Cloud's new interactive dashboard extends the MITRE ATT&CK framework to provide a consolidated view of the entire cloud native application portfolio. This helps organizations evaluate their defense against specific threat scenarios, and provides incident response and remediation capabilities. This attack framework was developed by Palo Alto Networks Unit 42 threat research and consulting team.
- **Anti-Malware Capabilities at Runtime and During Continuous Integration and Delivery (CI/CD) Scenarios:** Prisma Cloud now includes Palo Alto Networks WildFire® intelligence to provide an additional layer of runtime protection and deeper visibility into malicious malware threats with new anti-malware and prevention capabilities for host and containers, beginning in the build process before the software is deployed.
- **Simplified Compliance for Hosts, Containers and Serverless Applications**: Prisma Cloud Compliance Explorer simplifies compliance visibility across leading frameworks and CIS (Center for Internet Security), including new updates to the latest benchmarks, which join the exisiting six certifications. In addition, a new user interface delivers a compliance solution for implementing Docker DISA STIG (Defense Information Systems Agency Security Technical Implementation Guide).
- **Open Source License Analysis and Expanded Software Composition Analysis:** Prisma Cloud adds support for scanning code repositories with the twistcli command line interface, as well as new support for scanning GitHub Enterprise repositories. Additionally, Prisma Cloud includes advanced license detection to identify open source licenses in packages, combined with license compliance rules, to monitor and manage usage within an organization.

"Today's enterprises are running their cloud native applications on a wide variety of form factors, including a combination of cloud VMs, containers, Kubernetes, and serverless architectures that all need to be secured," says ESG Vice President and Group Director, Cybersecurity, Doug Cahill. "The latest enhancements to Prisma Cloud deepen their security capabilities for protecting modern applications on both containers and Kubernetes, but also foundational virtual machines from a single, unified solution."

Availability

The new features are available today in Prisma Cloud Compute Edition, with general availability in Prisma Cloud Enterprise Edition by late May.

More Information

For more information, see the blog post.

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 artificial 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.

View original content to download multimedia:http://www.prnewswire.com/news-releases/palo-alto-networks-expands-prisma-cloud-to-automatically-secure-unprotected-cloud-workloads-and-propels-container-security-forward-with-four-critical-new-capabilities-301278907.html

SOURCE Palo Alto Networks, Inc.