

# Palo Alto Networks Launches Strata Cloud Manager, Industry's First AI-Powered Zero Trust Management and Operations Solution

November 8, 2023

*Additional innovations include advanced security capabilities and new Next-Generation Firewalls*

SANTA CLARA, Calif., Nov. 8, 2023 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW) today introduced Strata™ Cloud Manager, the industry's first AI-powered Zero Trust management and operations solution. With these innovations and over 4,400 machine learning models, Palo Alto Networks is well-positioned to prove the combination of AI and Zero Trust can best protect today's customer needs. The world's cybersecurity leader also announced a suite of advanced security capabilities in addition to five new Next-Generation Firewalls to address the use cases of modern enterprises.

## **Anand Oswal, SVP and GM of Network Security at Palo Alto Networks, said:**

"I'm excited about the new capabilities we are announcing today. Strata Cloud Manager will simplify management and operations across our customers' entire network security estate. We continue to innovate with AI and ML in our security services, now stopping advanced attacks, including the first and only instance of a unique attack. This approach effectively prevents patient zero. We are also introducing incredible hardware platforms that offer industry-leading performance with best-in-class security."

## **Redefining Network Security with Strata Cloud Manager**

Inadequate predictive and actionable insights, along with a lack of seamless integration across security tools, can result in security gaps and inconsistent policies that compromise protection and operational experience. [Strata Cloud Manager](#) revolutionizes network security management and operations, bolstering security posture and proactively preventing network disruptions at every enforcement point. With Strata Cloud Manager, security teams can:

- **Ensure continuous network uptime:** With predictive analytics, Strata Cloud Manager helps organizations anticipate capacity bottlenecks and assess deployment health up to seven days ahead, enabling security teams to prevent operational disruptions effectively.
- **Enhance network security with industry best practices:** Leverage AI-powered analysis of policies and real-time compliance checks to fortify network security.
- **Streamline network security management for enhanced efficiency:** For the first time, effortlessly oversee configuration and security policies across all form factors, including SASE and both hardware and software firewalls, ensuring consistent protection and minimizing operational overhead.

## **Sebastian Schubert, Technology Lead, Tui Hotels & Resorts, said:**

"The ability to create one configuration and apply it seamlessly across our entire deployment has been a game-changer. Rollouts and management of firewalls are now streamlined and efficient."

## **Best-in-Class Inline AI-Powered Security**

As part of Palo Alto Networks' [cloud-delivered security services](#), over 60,000 customers benefit from protection against new and advanced threats. These are some of the new capabilities:

- [Advanced WildFire®](#) effectively blocks ever-evolving and uniquely evasive initial attacks by integrating machine learning directly into its cloud-based detection engines. This helps ensure early detection and mitigation, fortifying defense against emerging attacks.
- Industry-first detection capabilities are designed to proactively prevent threats such as meddler-in-the-middle and SaaS platform-hosted phishing attacks. Additionally, [Advanced URL Filtering](#) can anticipate and block a remarkable 88% of malicious URLs a full 48 hours ahead of competing solutions to ensure network security protection.
- The latest AI-powered [Advanced Threat Prevention](#) is purpose-built to counter command-and-control (C2) attacks often propagated via the widely used red team tool Empire. This valuable addition to the advanced threat prevention arsenal now boasts an impressive over 97% success rate in blocking highly evasive C2 attacks.

## **New Next-Generation Firewalls**

Palo Alto Networks announced five new Next-Generation Firewalls to expand addressable use cases, from the most high-traffic networks to remote branches, including ones that require 5G connectivity and others that need to operate in the harshest operational technology (OT) environments. The [new Next-Generation Firewalls](#) include:

- **PA-7500 for blazing fast performance:** Powered by custom ASICs, the PA-7500 delivers industry-leading security and over 1.5 Tbps App-ID™ performance to secure the world's most demanding environments.
- **PA-415-5G for 5G networks:** As the global reach of 5G networks continues to expand, an [estimated](#) 15 billion industrial assets are expected to connect via 5G by 2026. With the advanced firewall solution, organizations gain the flexibility to safeguard their branch offices with comprehensive security for both wired and 5G connectivity, ensuring that their critical assets are protected in this time of rapid digital transformation.
- **PA-450R for the harshest environments:** Industrial organizations can now leverage the ruggedized firewall solution, providing robust connectivity and security for their [OT environments](#), including exposure to extreme weather and wide temperature ranges. This ensures uninterrupted operations and peace of mind in challenging environmental conditions.

Palo Alto Networks also introduced the PA-5445 for securing data centers and large campus locations and the PA-455 for securing branch offices that need Power over Ethernet (PoE).

**John Grady, Principal Analyst, Enterprise Security Group, said:**

"Network security must continue to evolve. Traditional approaches cannot keep pace with today's attack landscape, and sprawling environments have made management much more complex. Palo Alto Networks was an early adopter in leveraging AI across various security services for more effective threat detection. By expanding the use of AI across additional security services, as well as its cloud-based management platform for more efficient and proactive operations, Palo Alto Networks continues to respond to the key pain points organizations face."

To get the full details on Palo Alto Networks new innovations, read the [hardware innovations](#) and [software innovations](#) blog posts.

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 (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022), and HRC Best Places for LGBTQ Equality (2022). For more information, visit [www.paloaltonetworks.com](http://www.paloaltonetworks.com).

Palo Alto Networks, the Palo Alto Networks logo, WildFire, and Strata are 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/palo-alto-networks-launches-strata-cloud-manager-industrys-first-ai-powered-zero-trust-management-and-operations-solution-301981172.html>

SOURCE Palo Alto Networks, Inc.

Bobbi Kimble, Palo Alto Networks PR, [bkimble@paloaltonetworks.com](mailto:bkimble@paloaltonetworks.com)