# Palo Alto Networks Announces PAN-OS 11.0 Nova to Keep Organizations One Step Ahead of Zero Day Threats

November 16, 2022

Nova introduces new innovations to help stop zero-day threats, simplify security architectures, and reduce the risk of costly misconfigurations

SANTA CLARA, Calif., Nov. 16, 2022 /PRNewswire/ -- Cyber threats continue to increase in volume and complexity with threat actors developing new ways to avoid detection — including highly evasive malware. To help organizations outpace these evolving threatsPalo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today announced PAN-OS® 11.0 Nova, the latest version of its industry leading PAN-OS software, unleashing 50+ product updates and innovations. Amongst them are the new Advanced WildFire® cloud-delivered security service that brings unprecedented protection against evasive malware and the Advanced Threat Prevention (ATP) service which now protects against zero-day injection attacks.
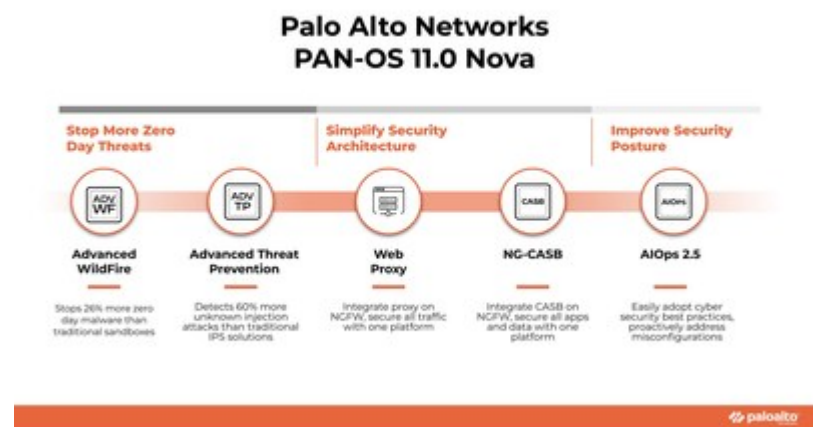
"We've observed a significant increase in unique malware samples over the last year along with an increasing level of malware sophistication. A new approach is required to detect this advanced malware," said Anand Oswal, senior vice president, Network Security, Palo Alto Networks. "PAN-OS 11.0 Nova is a leap forward in network security. It stops 26% more zero-day malware than traditional sandboxes; detects 60% more injection attacks; simplifies security architecture; and helps organizations adopt cybersecurity best practices. The bottom line is that Nova helps keep organizations one step ahead of attackers."

Security against Zero Day Threats

Advanced WildFire: Modern malware is highly evasive and sandbox-aware. To solve this problem, sandboxes need to continuously evolve to thwart analysis-resistant evasion techniques. The new Advanced WildFire service builds upon its custom hardened hypervisor to introduce radical new capabilities, such as intelligent run-time memory analysis combined with stealthy observation and automated unpacking to stay hidden from malware and defeat advanced evasions. These new capabilities enable Advanced WildFire to stop more highly evasive zero-day malware than traditional sandboxes.

Advanced Threat Prevention (ATP): The enhanced ATP service reimagines the intrusion prevention system (IPS) with industry-first inline capabilities for stopping zero-day injection attacks. Injection attacks — one of the top attacks on the OWASP Top 10 Web Application Security Risks" list — attempt to push malicious code into a computing system by exploiting unpatched vulnerabilities in software. Such malicious code executes remote commands that lead to data loss or full system compromise.

To protect against such injection attacks, ATP deep-learning models have been built on high fidelity telemetry data across tens of thousands of exploited vulnerabilities over the last decade. Internal testing has shown that the enhanced ATP service detects 60% more zero-day injection attacks that traditional solutions miss.

Nova not only sets up the foundation for modern day network security by continuously protecting against zero day threats but also raises the bar for how organizations can proactively improve cyber hygiene and simplify security architectures. In addition to Advanced WildFire and Advanced Threat Prevention, notable innovations in the Nova release include:

Simplified and Consistent Security

Web Proxy Support: For customers who need to run explicit proxies in their network due to network architecture or compliance requirements, Nova introduces natively integrated proxy capabilities for Palo Alto Networks NGFWs helping to secure web as well as non-web traffic. Now Palo Alto Networks NGFWs and Prisma® Access support web proxy, allowing customers to deploy consistent network security across campus locations, branches and mobile users, all managed centrally.

Integration of Next-Generation CASB: Palo Alto Networks Next-Generation Cloud Access Security Broker (CASB), natively integrated with Nova and Prisma SASE, now includes all-new SaaS Security Posture Management (SSPM) to help find and eliminate dangerous misconfigurations in 60+ enterprise SaaS apps. Next-Generation CASB now also has support for near-real time data protection in modern collaboration apps and suspicious user behavior detection, which helps to protect sensitive data in modern SaaS apps from compromised accounts and insider threats.

Stronger Cyber Posture

AIOps: Palo Alto Networks AIOps helps reduce misconfigurations that can lead to security breaches. AIOps, launched earlier this year, now

processes 29B metrics every month across 50,000 firewalls, and proactively shares 24,000 misconfigurations and other issues with customers for resolution every month. With Nova, AIOps is even more proactive. AIOps now guards against violations of best practices and enables remediation of inefficiencies in security policies before committing changes, helping organizations strengthen defenses against cyberattacks.

In addition to all the PAN-OS software updates, a new set of 4th generation ML-Powered NGFWs bring these new capabilities to branches, campus locations and data centers at up to 5x higher performance compared to the previous generation. The new hardware firewalls also bring the flexibility of fiber and Power over Ethernet (PoE) to small branches.

PA-445 and PA-415 for small branches: The PA-445 and PA-415 bring the flexibility of fiber and PoE ports to distributed enterprises and small and medium businesses. PoE powers downstream devices such as access points, IP cameras, and IP phones without the need for additional electrical circuits.The PA-445 and PA-415 also bring improved resiliency with dual power supplies and fanless cooling.

PA-1400 Series for large branches: The new PA-1400 Series offers up to 5x performance and up to 7x the session capacity compared to the previous generation. The PA-1400 Series is ideal for protecting large branch locations and small enterprise campuses, with support for PoE and fiber ports.

PA-5440 for large campus locations and data centers: We are launching the highest performing fixed-form factor in 2RU, the PA-5440. This platform offers 2x the performance of the previous generation PA-5260, and is ideal for protecting large campus locations and data centers.

"Attackers continue to develop new ways to evade traditional defenses, while security teams struggle to defend organizations with point solutions that are complex to deploy and operate," said John Grady, ESG senior analyst. "Palo Alto Networks PAN-OS 11.0 Nova addresses these critical challenges by stopping zero-day threats in real-time, simplifying security architectures, and improving cyber hygiene."

Availability
PAN-OS 11.0 and most of the security services will be available in November. New ML-Powered NGFW platforms will be available in December, and SSPM will be available on the NGFW platforms in January. Most security services including Advanced WildFire will be compatible with previous versions of PAN-OS.

Additional Resources

- Follow Palo Alto Networks on Twitter, LinkedIn, Facebook and Instagram
- Launch event

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 (2022), Comparably Best Companies for Diversity (2021) and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Prisma, PAN-OS 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.

C View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-announces-pan-os-11-0-nova-to-keep-organizations-one-step-ahead-of-zero-day-threats-301679776.html

SOURCE Palo Alto Networks, Inc.

Josh Weinberg, jweiberg@paloaltonetworks.com