



Palo Alto Networks Expands the Preventive Strengths of Its Traps Advanced Endpoint Protection Offering

May 2, 2017

Multi-Method Prevention Approach Delivers Protection Against Ransomware and Other Advanced Threats, Now With Support for macOS and Android Devices

SANTA CLARA, Calif., May 2, 2017 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced enhancements to its Traps™ advanced endpoint protection offering that strengthen its malware and exploit prevention capabilities and extend support to more operating systems, including macOS™ and Android™ (beta).

A verified AV-replacement for organizations subject to HIPAA regulations or PCI DSS standards, Traps employs a multi-method prevention approach to blocking both known and unknown malware as well as exploits before they compromise endpoints.

Despite increased investment in endpoint security, cyber adversaries continue to compromise endpoints at a rate that outpaces organizational investments. Legacy and next-generation AV point products have made attempts to close this gap, but they have merely replaced one ineffective malware detection method with another without significantly advancing their ability to identify and prevent exploits and unknown malware.

The enhancements announced today as part of Traps version 4.0 address these challenges, with the addition of support for macOS and Android (beta), plus several new prevention modules designed to detect and stop ransomware and other advanced threats.

In addition, when implemented in conjunction with other elements of the Palo Alto Networks Next-Generation Security Platform, customers can now correlate endpoint and network security events and threat intelligence information via Panorama™ network security management to mitigate the risk of cyber breaches across endpoints, firewalls, cloud and SaaS applications.

QUOTES

- "Signature-based endpoint security simply cannot provide effective protection against the new wave of cyberattacks targeting endpoints. Given the acute problem presented by the "Patient Zero Effect," new approaches are a must. Built from the ground up to address modern endpoint security needs, Palo Alto Networks Traps provides modern endpoint protection that can be implemented as either an independent, standalone solution or as a part of an integrated security ecosystem with the accompanying integration synergies that their Next-Generation Security Platform can provide. Palo Alto Networks Traps commands consideration for organizations seeking modern endpoint threat prevention capabilities."
 - Frank Dickson, research director, Worldwide Security Products, IDC
- "Today's dynamic cyber threat landscape demands that global organizations implement new strategies and technology to prevent cyber breaches, such as endpoint security that enables companies to replace legacy technology that can be ineffective and cumbersome. The Palo Alto Networks endpoint offering tackles breach prevention in a unique manner by identifying and blocking exploit techniques as well as identifying known and unknown malware to meaningfully decrease the time it takes to identify and stop new threats."
 - Jeff Wilson, senior research director, Cybersecurity Technology, IHS Markit
- "Our customers are increasingly having to respond to business and employee demand to grant access to sensitive applications and data via non-Windows and mobile devices. Because of this, both our current and prospective customers will find great value in the latest updates to Traps. With its added macOS and Android support and integration with the Palo Alto Networks Next-Generation Security Platform, we are able to service a wider cybersecurity strategy and embrace a more holistic approach to preventing cyberattacks by securing endpoints, networks and cloud environments."
 - Bryan Norman, chief executive officer, Norlem
- "Traps unique approach preemptively stops attacks by blocking the techniques that attackers rely upon, including never-before-seen attacks. The advancements announced today extend protections to macOS and Android, while adding to the attack techniques that can be prevented, to include macro- and script-based attacks, fingerprinting techniques, and kernel privilege escalation. These protections harness and add to the power of our platform to prevent advanced and never-before-seen threats from infiltrating the enterprise, at any point, and render them ineffective."
 - Lee Klarich, executive vice president, Product Management, Palo Alto Networks

Key new advancements introduced include:

- **Support for macOS and Android (beta):** Traps now secures macOS systems, replacing legacy AV with a multi-method approach to prevention. Protection for Android devices is also available via a community access beta program.
- **Protection from malicious macros:** Prevent macro-based attacks often used by ransomware and other advanced attacks by preemptively blocking known and unknown malicious macros embedded in Microsoft® Office documents.
- **Prevention of script-based attacks:** Prevent vulnerable processes like browsers and Office applications from launching sensitive tools like PowerShell and scripting engines.
- **Exploit kit fingerprint protection:** Disrupt attacker attempts to identify and target vulnerable endpoints by blocking their profiling tools.
- **Kernel privilege escalation protection:** Block advanced attacks targeting the operating system itself.

LEARN MORE

- [Traps Advanced Endpoint Protection Version 4.0](#)
- [Register to attend the webcast, Prepare for the Imminent Shifts in Endpoint Attacks](#)
- [Palo Alto Networks Next-Generation Security Platform](#)

About Palo Alto Networks

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.

Palo Alto Networks, PAN-OS and

the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdiction throughout the world. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.

To view the original version on PR Newswire, visit: <http://www.prnewswire.com/news-releases/palo-alto-networks-expands-the-preventive-strengths-of-its-traps-advanced-endpoint-protection-offering-300449359.html>

SOURCE Palo Alto Networks, Inc.

Brittany Stagnaro, Palo Alto Networks, 408-425-6302, bstagnaro@paloaltonetworks.com