Palo Alto Networks Raises the Bar for Endpoint Security With Updates to Traps Advanced Endpoint Protection Offering

August 3, 2016

LAS VEGAS, Aug. 3, 2016 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced new functionality, including significant machine learning capabilities for real-time unknown malware prevention, to its Traps™ advanced endpoint protection offering. These updates further strengthen the malware and exploit prevention capabilities of Traps and alleviate the need for legacy antivirus products to protect endpoints, such as laptops, servers and VDI instances.

Many organizations deploy a number of security products and software agents on their endpoint systems, including one or more traditional antivirus products. Nevertheless, cyber breaches continue to increase in frequency, variety and sophistication. Traditional antivirus products struggle to keep pace and invariably fail to prevent these attacks on endpoints.

An alternative to legacy antivirus point products, Traps uniquely combines the most effective, purpose-built malware and exploit detection methods to prevent known and unknown threats before they can successfully compromise an endpoint. By focusing on detecting and blocking the techniques at the core of these attacks, Traps can prevent sophisticated, targeted and never-before-seen attacks.

As a component of the Palo Alto Networks Next-Generation Security Platform, a natively integrated and automated platform designed to safely enable applications and prevent cyber breaches, Traps both shares with and receives threat intelligence information from the Palo Alto Networks WildFire™ cloud-based malware analysis environment. Threat intelligence information is passed to WildFire by each component of the security platform, and Traps uses this information to block threats on the endpoint no matter where they originated.

The new functionality announced today, which includes static analysis via machine learning and trusted publisher capabilities**,** will allow Traps to detect and immediately prevent malware that has never been seen.

Quotes

- "The sophistication and frequency of cyberattacks are growing too quickly for legacy antivirus tools that rely on malware signatures to keep pace. The Palo Alto Networks Traps offering takes an innovative approach to endpoint security, keeping endpoints more secure despite a growing landscape of cyberthreats and reducing the resources required by IT teams to track and install security patches."
  - **Rob Westervelt, research manager, Security Products, IDC**
- "Antivirus point products give organizations a false sense of security, because while they technically make users compliant with regulatory and corporate governance requirements, they do not protect against today's advanced cyberthreats. To do that, organizations must adopt a cybersecurity platform that prevents malware from infiltrating the enterprise at any point, including the endpoint, even if it has never been seen before."
  - **Lee Klarich, executive vice president, Product Management, Palo Alto Networks**

The latest version of Traps, version 3.4, will be available by the end of August on the Palo Alto Networks Support Portal and will include the following updates:

- **Static analysis via machine learning** examines hundreds of characteristics of a file to determine if it is malware. Threat intelligence available through the Palo Alto Networks WildFire subscription is used to train a machine learning model to recognize malware, especially previously unknown variants, with unmatched effectiveness and accuracy. This new functionality allows Traps to rapidly determine if a file should be allowed to run even before receiving a verdict from WildFire.
- **Trusted publisher identification** allows organizations to automatically and immediately identify new executable files published by trusted and reputable software publishers. These executable files are allowed to run, cutting down on unnecessary analysis and allowing them to execute without delay or impact to the user.
- **Quarantine of malicious executables** immediately removes malicious files and prevents further propagation or execution attempts of the files.
- **Grayware classification** allows enterprises to identify non-malicious, but otherwise undesirable, software and prevent it from running in their environment.

Learn More

- **Read the Traps 3.4 blog post**
- **Register for the upcoming webinar, Protect Yourself From Antivirus**
- **Read the white paper, *Protect Yourself From Antivirus***
- **Palo Alto Networks Traps Advanced Endpoint Protection**

- **Palo Alto Networks WildFire Cloud-Based Malware Analysis Environment**
- **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.

Logo - http://photos.prnewswire.com/prnh/20150527/218856LOGO

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/palo-alto-networks-raises-the-bar-for-endpoint-security-with-updates-to-traps-advanced-endpoint-protection-offering-300308178.html

SOURCE Palo Alto Networks

Brittany Stagnaro, Americas PR & AR Manager, Palo Alto Networks, 408-425-6302, bstagnaro@paloaltonetworks.com