Palo Alto Networks Raises the Bar on Battling Sophisticated Cyber Attacks

January 14, 2014

SANTA CLARA, Calif., Jan 14, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the leader in enterprise security, today announced enhancements to its enterprise security platform that increase advanced threat detection and prevention capabilities for its customers worldwide. Most significantly, this includes enhancements to the Palo Alto Networks WildFire™ service that enable quick discovery and elimination of previously unknown malware, zero-day exploits, and advanced persistent threats (APTs).

(Logo: http://photos.prnewswire.com/prnh/20130508/SF04701LOGO)

Cyber criminals are employing new stealth methods to evade traditional security measures, such as stateful firewalls, intrusion prevention systems and anti-virus (AV) systems. These legacy approaches often address only a single threat vector across a limited range of network traffic, resulting in a higher attack penetration rate and costly human incident response.

To better detect sophisticated attacks, a highly automated and scalable "closed loop" approach is required. One that begins with positive security controls to reduce the attack surface; inspects all traffic, ports, and protocols to block all known threats; rapidly detects unknown threats; then, automatically employs new protections back to the front line to ensure previously unknown threats are known to all and blocked.

The Palo Alto Networks enterprise security platform is pioneering this approach; it starts with its next-generation firewall as the core enforcement vehicle within the network, and is extended by the advanced detection and analysis capabilities delivered by the WildFire service, which is now used by more than 2,400 customers worldwide. New advancements include:

- **Extended file visibility** – all common file types, including PDFs, Office documents, Java, and APKs, operating systems, and applications (encrypted or not) are now detected, sandboxed and filtered.
- **Zero-day exploit detection –** using behavioral analysis, this signature independent capability in the WildFire cloud quickly identifies exploits in common applications and operating systems and distributes the intelligence to subscribing customers in as little as 30 minutes to prevent future attacks.
- **Discovery of malicious domains** – blocks the critical command-and-control phase of an advanced attack by building a global database of compromised domains and infrastructure.
- **Single "pane of glass" view into incident response data** – in a single view, security administrators have access to a wealth of information on malware, its behavior, compromised hosts, and more, so that incident response teams can quickly address threats and build proactive controls.

These advancements increase unknown threat detection capabilities at each step in the attack lifecycle. Combined with automated blocking and in-line enforcement, the new capabilities can dramatically reduce the number of threats that penetrate an organization and require human incident response. And, in the unlikely event a threat does penetrate an organization, incident response teams have relevant data in a single view to take quick action.

QUOTES

- "The Palo Alto Networks security platform with WildFire gives us an extra layer of security we didn't have before – extra inspection and comfort that we can stay ahead of breaches by not just detecting them, but also by easily blocking them. By having our firewall, URL filtering, threat prevention natively integrated and managed from a single dashboard – instead of multiple niche products, we have a clearer picture of our threat landscape. Ultimately, the platform gives us what we need to effectively detect, analyze, block, and, more importantly, quickly remediate issues."
  - **Phil Cummings, Security Administrator, Health Information Technology Services-Nova Scotia (HITS-NS)**
- "Quickly detecting and eliminating previously unknown threats across all applications is key to protecting an organization from today's advanced threats; only Palo Alto Networks offers its customers the closed loop capabilities to most efficiently and effectively stop sophisticated threats."
  - **Lee Klarich, senior vice president of product management, Palo Alto Networks**

Availability

The enhancements are accessible via Palo Alto Networks PAN-OS™ version 6.0 – the operating system that is the heart of the Palo Alto Networks platform, which will be available for all Palo Alto Networks customers with valid support contracts. These new advancements will also be spotlighted at the Palo Alto Networks Ignite user conference, March 31 – April 2, Las Vegas, NV; to register, visit: https://www.paloaltonetworks.com/content/campaigns/ignite/ignite-2014/home.html.

To learn more about Palo Alto Networks security platform and WildFire service, visit: https://www.paloaltonetworks.com/products/features/apt-prevention.html.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is leading a new era in cybersecurity by protecting thousands of enterprise, government, and service provider networks from cyber threats. Unlike fragmented legacy products, our security platform safely enables business operations and delivers protection based on what matters most in today's dynamic computing environments: applications, users, and content. Find out more at www.paloaltonetworks.com.

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, Palo Alto Networks, (408) 638-3280, jjsmith@paloaltonetworks.com, or Tim Whitman, Voce Communications, (617) 897-8255, twhitman@vocecomm.com