Palo Alto Networks® Announces Agreement to Acquire Cyvera

March 24, 2014

Combination Creates Game-Changing Enterprise Security Platform that Spans Network, Endpoint, and the Cloud

SANTA CLARA, Calif., March 24, 2014 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), today announced a definitive agreement to acquire Cyvera, a privately held cybersecurity company located in Tel-Aviv, Israel. Under the terms of the agreement, Palo Alto Networks will acquire all of the outstanding capital stock of Cyvera for an aggregate purchase price of approximately $200 million. The acquisition is expected to close during the second half of fiscal 2014, subject to customary closing conditions and regulatory reviews.

Named a cool vendor in security by Gartner in 2013 ("Cool Vendors in Security: Infrastructure Protection 2013")*, Cyvera, which has 55 employees, has developed a highly innovative offering that protects enterprises from cyber threats by using a unique approach to block unknown, zero-day attacks on the endpoint.

The addition of this unique capability to the Palo Alto Networks enterprise security platform will extend customers' ability to safely enable applications and protect users against known and unknown cyber threats on any device, across any network.

QUOTES:

- "This event marks a key milestone in our strategic enterprise security vision. It extends our next-generation security platform with a very innovative approach to preventing attacks on the endpoint. It enables us to accelerate the delivery of the market's only highly integrated and automated enterprise security platform spanning network, endpoints, and the cloud. For customers, this translates into the most sophisticated and automated threat prevention for their entire organization."
  - Mark McLaughlin, President and CEO of Palo Alto Networks

- "Much like Palo Alto Networks set out to disrupt the network security market with its next-generation security platform, we founded Cyvera to revolutionize protection for the endpoint – one of the most vulnerable frontiers for cyber attacks. We are pleased to join the Palo Alto Networks team and together help enterprise customers tackle the advanced threats they face today."
  - Uri Alter and Netanel Davidi, co-founders and co-CEOs of Cyvera

Cyvera Prevents Attacks at the Right Time and Place

Zero-day cyber attacks represent one of the greatest threats to enterprises, governments, and service provider organizations that rely on a vast array of systems, applications, and devices to run their business. These cyber attacks often exploit a vulnerability known only to the attacker. While there are literally tens of thousands of vulnerabilities an attacker can potentially target, there is a significantly smaller number of exploit techniques they may use to exploit that vulnerability.

While patching software can provide an element of protection, it does little to protect organizations against vulnerabilities that have not yet been discovered by the software manufacturer. Simply detecting the presence of malware is also insufficient since malicious activity may have already been initiated and evasion tactics employed to evade detection. In order to stop zero-day attacks in their tracks, it's critical to understand the exploit techniques attackers employ. Cyvera has developed a unique method of performing this real-time prevention against all core attack techniques at the endpoint during the exploitation phase, before the malware has a chance to run.

Advanced Threats Demand Highly Integrated, Automated, and Scalable Platform Approach

Today's sophisticated attacks increasingly rely on a combination of tactics and threat vectors to penetrate an organization and require a new approach to security. Most organizations still rely on legacy point technologies that address only specific types of attacks, phases of an attack, certain devices, or certain network segments. Because of the singular nature of these technologies, they are ill-equipped to detect and prevent today's advanced cyber attacks.

To address these challenges, Palo Alto Networks developed a new approach: one that begins with positive security controls to reduce the attack surface; blocks all known threats; rapidly detects unknown threats through analysis and correlation of abnormal behavior; then automatically employs advanced exploit prevention mechanisms and policies back to the front line to ensure previously unknown threats are known to all and blocked. This approach is designed to prevent threats from penetrating an organization and greatly reduce the need for costly human remediation.

Adding the unique Cyvera capabilities extends the Palo Alto Networks enterprise security platform to perform next-generation security functions across the network, endpoint, and the cloud.

To learn more about the Palo Alto Networks security platform:

- Visit our website
- Register for the Palo Alto Networks Ignite user conference, March 31 – April 2

Investor conference call information

Palo Alto Networks will host a conference call for analysts and investors to discuss details of acquisition at 8:00 a.m. Eastern time / 5:00 a.m. Pacific time. Open to the public, investors may access the call by dialing (877) 474-9503 or (857) 244-7556 and entering the passcode 82968997. A live audio webcast of the conference call along with supplemental financial information will also be accessible from the "Investors" section of the company's website at investors.paloaltonetworks.com. Following the webcast, an archived version will be available on the website for one year. A

telephonic replay of the call will be available two hours after the call and will run for five business days and may be accessed by dialing (888) 286-8010 or (617) 801-6888 and entering passcode 32682574.

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.

* Gartner, Cool Vendors in Security: Infrastructure Protection, 2013, Ray Wagner, Neil MacDonald, et al, April 23, 2013. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

SAFE HARBOR

This press release contains "forward-looking" statements within the meaning of Section 27A of the Securities Act and Section 21E of the Exchange Act that are based on the beliefs and assumptions of Palo Alto Networks and on currently available information. Forward-looking statements include information concerning the expectations, beliefs, plans, intentions and strategies of Palo Alto Networks relating to its pending acquisition of Cyvera. Such forward-looking statements include statements regarding expected benefits to Palo Alto Networks, Cyvera and its respective customers; the impact of the pending acquisition on Palo Alto Networks' competitive position; and plans regarding Cyvera and Cyvera personnel. These statements reflect the current beliefs of Palo Alto Networks and are based on current information available to Palo Alto Networks as of the date hereof, and Palo Alto Networks does not assume any obligation to update the forward-looking statements to reflect events that occur or circumstances that exist after the date on which they were made. The ability of Palo Alto Networks to achieve these business objectives involves many risks and uncertainties that could cause actual outcomes and results to differ materially and adversely from those expressed in any forward-looking statements.

There are a significant number of factors that could cause actual results to differ materially from statements made in this presentation, including the failure to achieve expected synergies and efficiencies of operations between Palo Alto Networks and Cyvera; the ability of Palo Alto Networks and Cyvera to successfully integrate their respective market opportunities, technology, products, personnel and operations; the failure to timely develop and achieve market acceptance of combined products and services; the potential impact on the business of Cyvera as a result of the acquisition; the ability to coordinate strategy and resources between Palo Alto Networks and Cyvera; the ability of Palo Alto Networks and Cyvera to retain and motivate key employees of Cyvera; Palo Alto Networks' limited operating history and experience with integrating acquired companies; risks associated with Palo Alto Networks' rapid growth, particularly outside the United States; rapidly evolving technological developments in the market for network security products; and general market, political, economic and business conditions. Additional risks and uncertainties are included under the captions "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations," in the company's quarterly report on Form 10-Q filed with the SEC on February 24, 2014, which is available on the company's website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. Additional information will also be set forth in other filings that the company makes with the SEC from time to time. All forward-looking statements in this presentation are based on information available to the company as of the date hereof, and Palo Alto Networks does not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made or to update the reasons why actual results could differ materially from those anticipated in the forward-looking statements, even if new information becomes available in the future.

Logo - http://photos.prnewswire.com/prnh/20130508/SF04701LOGO

SOURCE Palo Alto Networks

Jennifer Jasper-Smith, Head of Corporate Communications, 408-638-3280, jjsmith@paloaltonetworks.com, Kelsey Turcotte, Vice President of Investor Relations, 408-753-3872, kturcotte@paloaltonetworks.com