Palo Alto Networks Broadens Technology Partner Program with New Authentication, Security Risk Management, Network Monitoring And Availability Partnerships

November 13, 2012

SANTA CLARA, Calif., Nov. 13, 2012 /PRNewswire/ -- Palo Alto Networks™ (NYSE: PANW), the network security company, has announced new partnerships within its Technology Partner Program – a program committed to delivering integrated solutions that fundamentally improve network security for enterprises. These newly announced partnerships further the company's commitment to providing interoperability between its Next-Generation Firewall (NGFW) platform and leading technologies in authentication and access control, security risk management, and network monitoring and availability.

"These partnerships center around arming enterprises with validated solutions of our industry's most innovative technologies," said Chad Kinzelberg, vice president of Business and Corporate Development for Palo Alto Networks. "This particular set of partners is focused on helping customers deploy their Next-Generation Firewall in highly mobile and virtualized environments that require secure access, proactive risk management and unparalleled visibility into the network. "

Strong Authentication and Access for the Mobile Workforce

Palo Alto Networks has strengthened its alliance with authentication partners to enable its mutual customers to take advantage of flexible and secure authentication platforms for internal and remote users accessing corporate applications and data from any location. New authentication and access technology partners include:

RSA – this collaboration ensures interoperability between Palo Alto Networks Next-Generation Firewalls with RSA SecurID® hardware, software and smartphone authenticators. This multi-factor authentication platform from RSA is engineered to provide additional strength and security before allowing access to corporate applications and data.

SafeNet – this partnership ensures interoperability between Palo Alto Networks Next-Generation Firewalls with SafeNet's multi-factor Authentication solutions to ensure authenticity of users accessing the enterprise network. To address varying threat levels, SafeNet's versatile authentication solutions provide mutual customers with the right combination of authentication methods.

Swivel – this partnership enables customers to deploy a variety of easy-to-use strong authentication methods based on Swivel's Authentication Platform. Swivel's mobile-based authentication is available on all mobile platforms and acts as the second-factor authentication using the unique PINsafe algorithm to generate one-time codes.

Bradford Networks – this partnership leverages user and device information obtained by Bradford Networks Network Sentry from a non-corporate device, such as employee, contractor or guest owned laptop, tablets, and smartphones, enabling the Palo Alto Networks Next-Generation Firewalls to apply granular security policies to these devices to mitigate potential threats.

Security Risk Management to aid compliance

New partnerships with security risk management solution providers ensure that mutual customers have access to a broader set of network security information and data for more complete risk analysis, compliance reporting and policy and device management. New security risk management partners include:

RedSeal – this partnership makes it possible to better pinpoint weaknesses and risk through complete end-to-end security visualization, predictive network threat modeling and metrics for situational awareness and compliance gaps. RedSeal collects information from Palo Alto Networks Next-Generation Firewalls and other networking devices to create a navigable topology map for network modeling, risk analysis and continuous audit and control monitoring.

Skybox Security – this partnership prevents cyber attacks by integrating information from Palo Alto Networks Next-Generation Firewalls with predictive analytics offered by Skybox solutions, which further identifies ways to block risky access and vulnerabilities before they can be exploited. In addition, the integration provides signature configuration and reporting on next-generation firewall feature sets such as integrated Intrusion Prevention Signatures (IPS), and complete support for next-generation access and rule compliance at the user and application level.

Network Monitoring and Availability

New partnerships in the network monitoring and access segment assist mutual customers in ensuring comprehensive network visibility and intelligence as well as uninterrupted access during network interruptions. These new partners include:

Lancope – this partnership provides visibility and threat intelligence across the internal networks through market-leading NetFlow analytics and reporting. Lancope StealthWatch System consumes NetFlow records from Palo Alto Networks Next-Generation Firewalls to deliver in-depth insight needed to detect and remediate network and security problems.

Interface Masters – this partnership ensures interoperability between Palo Alto Networks Next-Generation Firewalls and Interface Masters Niagara bypass switch to ensure continuous network monitoring, availability, and mitigation under planned or unplanned device failures and interruptions to network services.

Garland Technology – this partnership ensures interoperability between Palo Alto Networks Next-Generation Firewalls and Garland Technology's line

of portable, modular and integrated bypass switches to ensure continuous network monitoring, availability, and mitigation under planned or unplanned device failures and interruptions to network services.

Partner Quotes

RSA: "Enabling secure authentication is a critical component to ensuring that applications are safely enabled," said Sean Brady, director of Product Marketing in the RSA Identity & Data Protection group. "Our interoperability partnership signifies the continued commitment that Palo Alto Networks has in providing enterprises with strong authentication for its NGFW technology."

SafeNet: "Today's decentralized business environments demand a new approach to securing high value data," said Andrew Young, vice president of Product Management and Authentication, SafeNet. "In order to ensure that the data remains secure, username and one time password approaches are no longer sufficient. By combining Palo Alto Networks Next-Generation Firewalls with SafeNet's strong, two-factor authentication, enterprises can meet strict compliance requirements with an elegant solution that ensures the utmost network protection."

Swivel: "Following the launch of Swivel Secure in the US earlier this month, we are delighted that Palo Alto Networks has chosen to work with Swivel to ensure interoperability of Swivel authentication platform with its Next-Generation Firewall," said Fraser Thomas, vice president International for Swivel Secure. "As Swivel continues to gain traction in the US in 2013, we look forward to working with Palo Alto Networks to develop our relationship further."

RedSeal: "RedSeal Networks and Palo Alto Networks are getting a step ahead of the competition by delivering integration that provides customers with previously unattainable capabilities to visualize and control network security – ultimately for the protection of critical business assets," said Parveen Jain, CEO of RedSeal Networks. "RedSeal continues to expand its integration with third-party network and security devices, enabling customers to identify risk and predict threat paths throughout the network down to the most granular level."

Skybox Security: "We are pleased to partner with Palo Alto Networks to provide support for next-generation firewall management processes," said Gidi Cohen, CEO of Skybox Security. "Skybox enables organizations to quickly and securely migrate to Palo Alto Networks Next-Generation Firewalls by validating the deployment plan and optimizing legacy rule sets before implementation to ensure accuracy. Once deployed, Skybox streamlines policy management for both traditional and next-generation firewalls, and integrates Palo Alto Networks' capabilities with a complete security risk management ecosystem."

Bradford Networks: "BYOD is now an unstoppable force across the industry; however, the proliferation of consumer devices such as smartphones and tablets accessing the network creates new challenges for IT teams tasked with managing access to enterprise resources," said Vincent Ma, vice president of business development for Bradford Networks. "The partnership between Bradford Networks and Palo Alto Networks adds mobile device perspective, including the user, device type and its location, to provide companies with full visibility and control over corporate or personally owned devices connecting to their networks –and enabling a complete and secure BYOD strategy."

Lancope: "By combining Palo Alto Networks Next-Generation Firewalls with market leading NetFlow analysis and reporting from Lancope's StealthWatch System, enterprises gain pervasive visibility and threat context across the internal network," said Mike Potts, president and CEO of Lancope. "Widely deployed across Global 2000 enterprise networks, StealthWatch is a key component of the defense in depth strategy, enabling rapid incident response to minimize costly downtime and limit potential damage."

Interface Masters: "Interface Masters is pleased to partner with Palo Alto Networks to provide a fully tested plug-and-play next-generation firewall that works seamlessly with leading bypass to protect Gigabit, 10 Gibabit and 40 Gigabit networks," said Ehud Yuhjtman, president of Interface Masters. "The combined solution addresses network operators requirements for high availability, hitless network connectivity protection, fully secure network management and comprehensive event notifications."

Garland Technology: "We are excited to be part of Palo Alto Networks Technology Partnership program," said Chris Bihary, CEO and Co-owner of Garland Technology. "Our products work very well together since we are an enabling technology for inline deployment of Palo Alto Networks Next-Generation Firewall. Garland's bypass TAP technology is the access point for connecting next-generation firewalls actively in-line for Gigabit, 10 Gigabit, and 40 Gigabit Networks without having to worry about network downtime, maintenance, or troubleshooting."

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks' products are used by more than 9,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

SOURCE Palo Alto Networks

Mike Haro, Director of Corporate Communications, Palo Alto Networks, 408-438-8628, mharo@paloaltonetworks.com