New Palo Alto Networks Aperture Safely Enables SaaS By Preventing Data Exposure And Threat Risks

September 15, 2015

SANTA CLARA, Calif., Sept. 15, 2015 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced availability of Aperture, a new security-as-a-service offering to help organizations safely enable and strengthen security for sanctioned SaaS applications, such as Box, Dropbox, Google Drive, and Salesforce.

Typically accessed by users via both corporate and personal devices, SaaS applications provide productivity and collaboration benefits for organizations; however, these applications and the often sensitive data stored in the public cloud present unique security challenges and risks, such as accidental data exposure by users. To prevent this exposure and ensure threats do not propagate through these SaaS applications, granular visibility and control of sanctioned SaaS applications with security policies applied to all data and users is essential.

Aperture – based on technology acquired from CirroSecure in May 2015 – gives security teams this visibility and control of sanctioned SaaS application activity, and provides a detailed analysis of usage by user and device to easily determine if there are any data risks or compliance-related policy violations. In addition to granular policy controls, Aperture is integrated with the Palo Alto Networks WildFire™ cloud-based malware prevention offering to identify known and unknown malware and prevent a SaaS application from becoming an insertion point for advanced threats into an organization's computing environment.

QUOTES

- "Global organizations are transitioning to new models of productivity and collaboration, powered by mobile-first, cloud-based solutions. With this new approach, IT leaders must adopt security policies that protect business critical information while still enabling employees to be agile and connected. We're incredibly excited to be working with Palo Alto Networks to advance content security in the cloud and transform the way today's leading enterprises work."
  - Chris Yeh, senior vice president, Product at Box
- "Until now, this combination of visibility, analysis, and contextual control of SaaS applications hasn't existed and it forced many organizations to shoulder the risks associated with sanctioning the use of SaaS applications. Now, the granular control provided by Aperture, along with malware protection through WildFire, can help organizations enjoy the productivity benefits of sanctioned SaaS applications while reducing the risk of data exposure and cyberthreats compromising their networks."
  - Lee Klarich, senior vice president, product management at Palo Alto Networks

Secure SaaS applications with visibility, analysis and control
Aperture, which complements the Palo Alto Networks Next-Generation Firewall that identifies and controls access to unsanctioned applications, allows IT teams to control sanctioned SaaS applications and associated data by examining and controlling how data is shared while preventing malware from being introduced.

Aperture, a cloud-based, device-agnostic offering that requires no agents, has little impact on the user's experience or changes to the network infrastructure. If a use violation occurs, Aperture enables quick enforcement of security policies to quarantine folders and data.

Key features of Aperture include:

- **Complete visibility across all user, folder and file activity** – Helps organizations transition from a position of speculation to one of knowing what is happening at any given point in time.
- **Retroactive analysis and control of data and threat exposure** – Enforcement dating back to the creation of the SaaS account itself.
- **Deep content inspection and usage analytics** – Quickly classify data and determine if there are any data risks or compliance-related policy violations.
- **Granular, context-aware policy control** – Drive the enforcement and quarantine of folders and data as soon as a violation occurs.
- **Advanced threat protection** – Block known malware, and identify and block unknown malware.

For more information about Palo Alto Networks Aperture, visit: https://www.paloaltonetworks.com/products/aperture.html

For more information about Palo Alto Networks WildFire, visit: https://www.paloaltonetworks.com/products/technologies/wildfire.html

For more information about the Palo Alto Networks Next-Generation Security Platform, visit: https://www.paloaltonetworks.com/products/platforms.html

Availability
Aperture is a subscription-based security-as-a-service offering now available in North America through authorized channel partners of Palo Alto

Networks. It is expected to be available in EMEA and APAC by the first half of CY2016.

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

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

To view the original version on PR Newswire, visit:http://www.prnewswire.com/news-releases/new-palo-alto-networks-aperture-safely-enables-saas-by-preventing-data-exposure-and-threat-risks-300142906.html

SOURCE Palo Alto Networks

Tim Whitman, Voce Communications, 617-721-5994, twhitman@vocecomm.com