Palo Alto Networks Expands CASB Offering With New Cloud Security Capabilities

October 3, 2017

Added Capabilities for Amazon EC2, IAM and Amazon S3 Protect Against Sensitive Data Loss; Prevent Malware Propagation and Security Misconfigurations

SANTA CLARA, Calif., Oct. 3, 2017 /PRNewswire/ -- Palo Alto Networks® (NYSE: PANW), the next-generation security company, today announced that its Cloud Access Security Broker (CASB) offering, Aperture™ SaaS security service, now provides application protections for several Amazon Web Services (AWS) solutions, including Amazon Elastic Compute Cloud (Amazon EC2), AWS Identity and Access Management (IAM) and Amazon Simple Storage Service (Amazon S3).

The new protections address sensitive data loss, enable monitoring for risky or suspicious administrator behavior, and provide additional protection against security misconfigurations and malware propagation. When combined with the preventive capabilities of the Palo Alto Networks Next-Generation Security Platform, these advancements will enable organizations to achieve even more protection for AWS, as well as address critical cloud security needs to deliver the most complete application and data security for cloud environments. Additionally, Aperture support for Office 365 and Google applications has been enhanced to include cloud-based email services and G Suite Marketplace applications.

Data and applications reside everywhere: on the network, on endpoints, and in the cloud. As part of the migration to the cloud, many enterprises are adopting a multi-cloud strategy that includes storing large amounts of business-critical data within cloud environments, which requires advanced protections that complement basic native cloud offering controls to achieve comprehensive and consistent security.

Palo Alto Networks Aperture controls enterprise SaaS applications and associated data by examining and controlling how data is shared, all without impact to user experience or changes to network infrastructure. If a policy violation occurs, Aperture enables quick enforcement of security policies to quarantine folders and data while immediately alerting security teams of suspicious behavior.

QUOTE

- "Our Aperture service secures business-critical data residing within today's most important cloud-based enterprise SaaS applications. With extensive capabilities across our security platform and our latest application protections for Amazon Web Services, our customers benefit from complete visibility and granular control, instant classification, and enforcement across users, folders, and file activities, enabling them to prevent cyber breaches and protect their data no matter where it resides."
  - Lee Klarich, executive vice president, Product Management, Palo Alto Networks

Key new Aperture advancements introduced include:

- **Support for AWS:** Aperture now provides additional in-cloud security controls to prevent improper use while enabling malware protection and data governance policies via integration with Amazon EC2, IAM and Amazon S3.
- **Support extended to Office 365 Exchange:** Aperture now adds the ability to scan email content and attachments for compliance violations, malware, user impersonation and data exposure within Office 365; this capability also complements the company's existing integration with Proofpoint, offering customers increased visibility and comprehensive protection against advanced cyberthreats via email.
- **Controls for new productivity and file-sharing apps:** Aperture already offers protection for a number of business-critical SaaS applications, such as Box, salesforce.com, Office 365 and many others; in addition to Amazon EC2, IAM and Amazon S3, Aperture now supports several other applications, including Citrix ShareFile®, Atlassian Confluence, G Suite Marketplace applications, Jive®, and Microsoft® Office 365 Exchange Server®.
- **Policy control for G Suite Marketplace applications:** Aperture can now apply policy control across Marketplace applications, protecting organizations from targeted phishing and malware attacks, or unwanted data sharing, through the Google G Suite Marketplace.
- **SIEM integrations with new API and log forwarding capability:** Customers can now configure Aperture to interface with syslog servers and API clients, allowing them to push event information to external syslog servers or access event information from the Aperture service via a REST API.
- **Monitoring for suspicious user behavior:** Aperture now supports the ability to alert administrators if suspicious activity is detected within SaaS applications.

LEARN MORE

- **Complete New Features Guide**
- **Aperture SaaS Security**
- **SaaS Applications Supported by Aperture**

- **Read the blog – Introducing Expanded Public Cloud Security Capabilities with Aperture Our CASB Security Offering**
- **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.

View original content with multimedia:http://www.prnewswire.com/news-releases/palo-alto-networks-expands-casb-offering-with-new-cloud-security-capabilities-300529575.html

SOURCE Palo Alto Networks, Inc.

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