

# Palo Alto Networks and VMware expand strategic partnership

Palo Alto Networks and VMware have announced an expansion of their strategic partnership to address mobile security needs.



Mobile computing is transforming the ways organisations do business. Users no longer stop working once they leave the office, and they need secure access to business information at any time, from anywhere, and from any device. This introduces new security challenges for organisations by exposing them to new risk vectors and creating a need to protect business information and applications accessed via employee-owned devices, while also respecting the privacy of personal information and traffic.

To address these challenges, Palo Alto Networks and VMware will integrate their enterprise security and mobile management technologies to give organisations a rich and unique combination of mobile device management (MDM) with advanced threat prevention for secure enterprise BYOD support. This builds upon endeavours started in 2014 when the companies announced a software-defined data centre reseller agreement and network security and network virtualisation solutions.

## A positive mobile experience

"Employees love the flexibility that using their mobile devices for business provides them, but IT teams often struggle to enforce security policies without compromising usability. Integrating our Next-Generation Firewall, WildFire and GlobalProtect technologies with the AirWatch platform addresses the concerns of both parties, giving users a positive mobile experience while existing security policies are enforced," said Lee Klarich, Senior Vice-President of Product Management, Palo Alto Networks.

"In a world of rising mobile threats Palo Alto Networks and VMware are building upon the comprehensive AirWatch mobility

platform to provide another layer of security, automation and ease of management for customers around the globe," added Noah Wasmer, Vice-President, End-User Computing, VMware.

The Palo Alto Networks Next-Generation Firewall, WildFire and GlobalProtect technologies, coupled with the AirWatch by VMware Enterprise Mobility Management platform, can help customers enforce security policy to protect networks from unauthorised or infected devices, provide the appropriate level of access to apps and data for mobile users, and enable mobile devices to be properly configured for business use and connection to a global threat intelligence service to identify and eradicate malicious content.

Detailed capabilities include:

- **Malware detection:** Palo Alto Networks WildFire security subscription service identifies known and previously unknown mobile malware. By integrating the intelligence provided by WildFire, users can identify infected applications and take immediate and automated action for security and containment, such as creating an application blacklist;
- **Network protection:** Organisations need to make sure only approved devices are used with sensitive applications and networks; this is accomplished with Palo Alto Networks GlobalProtect Host Information Profile (HIP), a direct tie between information about the mobile device, its configuration and what data and applications the device can access;
- **VPN and network security:** Palo Alto Networks GlobalProtect provides a secure connection between AirWatch managed mobile devices and the Palo Alto Networks Next-Generation Firewall at the device or application level utilising per-app VPN. This allows consistent inspection of traffic and enforcement of network security policy for threat prevention, wherever the user goes.

The Palo Alto Networks GlobalProtect iOS VPN app deployed by AirWatch. Additional integration components have targeted availability in the second half of 2015.

For more, visit: <https://www.bizcommunity.com>