

One of the Most Sensitive R&D Installations in the World Secures Network, Consolidates Security Functions, and Saves Money with Palo Alto Networks® Next-generation Cyber Security

BACKGROUND

As one of the premier government research and development (R&D) organizations for national security in the world, this organization needed to secure some of the country's most sensitive weapons information. With over 5,000 employees and a relatively small real estate footprint, they were convinced that they could consolidate their multi-vendor approach into a singular next-generation cyber security platform. Given its mission, the importance of the information to be secured could not be underestimated. Palo Alto Networks was a natural fit.

CONSOLIDATION: MORE HAD NOT MEANT MORE SECURE

The government R&D facility had relied on three different vendors for three distinct cyber security functions. They did not believe it was necessary to maintain such a complex cyber security architecture to provide the security they needed. In fact, they were disappointed and unconvinced that the solutions were providing sufficient security for the organization. The Cyber Operations team had tested the Palo Alto Networks platform and felt confident the platform could perform these same functions and get better threat visibility.

IMPROVED THREAT VISIBILITY WITH REDUCED COMPLEXITY AND COST

Palo Alto Networks proved the Cyber Operations team right. Not only did they improve their threat visibility with the consolidation of the firewall, IDS/IPS and URL filtering into the singular platform, they in turn reduced the complexity of their previous multi-vendor architecture, and reduced their costs. Such consolidation naturally also adds the benefits of reducing operational overhead with fewer devices to manage, further reducing power, heating and other costs. In fact, their renewal costs for two of the previous solutions virtually covered the entire cost of the Palo Alto Networks deployment.

Palo Alto Networks security platforms are unique because they natively bring together all network security functions. Predictable, multi-Gbps performance is delivered via dedicated, function-specific processing for networking, security, content inspection, and management.



ORGANIZATION:

U.S. Government Research & Development (R&D) Organization

INDUSTRY:

Government

CHALLENGE:

Improve the facility's cybersecurity.
Reduce costs.

SOLUTION:

PA-2050s, PA-5050 and PA-3050s with URL filtering, Threat Prevention, WildFire and Panorama for management

RESULTS:

- Improved threat visibility and protection
- Reduced number of vendors and devices and therefore complexity
- Reduced costs
- Achieved full application visibility and control
- Reduced operational overhead with fewer devices to manage, less power and heat consumption and costs

“Not only did they improve their threat visibility with the consolidation of the firewall, IDS/IPS and URL filtering into the singular platform, they in turn reduced the complexity of their previous multi-vendor architecture, and reduced their costs.”

NEXT-GENERATION SECURITY FOR ONE OF THE WORLD'S MOST SENSITIVE NETWORKS

Today, this super-secret government facility is very happy with the threat visibility that Palo Alto Networks gives them. They are planning for their next deployment, that of the WF-500 platform which provides unknown threat—including Advanced Persistent Threat (APT)—identification and prevention in a private cloud option on their own network to identify and deliver on-board protection.

For this sensitive government installation, it was imperative they have the utmost security protection. Palo Alto Networks was proud to deliver. The reduced footprint, reduced complexity, and cost savings were the much-appreciated ancillary benefits that, along with their cyber security, continue to yield rewards.



4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

Copyright ©2014, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN_CS_USGOV-RD_031814