

Government Agency Strengthens their Security Posture with Machine Learning Driven NGFWs

Swish Data and Palo Alto help agency increase security, prevent cyberattacks, safeguard classified and sensitive data, and optimize security operations.

This government agency is responsible for administering the United States' lawful immigration system. Their sole focus is the administration of benefit applications. With 19,000 government employees and contractors working at more than 200 offices across the world, the agency enhances the security and efficiency of national immigration services. Like all government agencies, they must maintain a strong security posture. With numerous security solutions to choose from, this agency solicited help from Swish Data, a provider of IT solutions and services for government agencies. Swish's recommendation, based on the agency's needs and environment, was Palo Alto Networks®. The company's reputation and the prior success of Palo Alto deployments throughout the agency's parent organization were among the reasons for this recommendation but there were also specific needs that the agency had. Strata, Palo Alto's industry-leading network security suite, perfectly addressed those needs.

Background

This agency generates seven terabytes of log data per day. They process thousands of applications, petitions, and benefit requests with much of this information being shared with state and local governments, foreign governments, and authorized organizations. Their IT environment is extremely diverse and cuts across many sectors, stakeholders, organizations, processes, and systems. Security and privacy of users, applications, and data, regardless of location, are critical to the agency fulfilling its mission.

The Problem

With malware proliferating at a rate of 1,000 new threats every five minutes and variants identified five minutes later, the agency needed a network security solution that would enable them to stay ahead of tomorrow's threats.

Only a Next Generation Firewall (NGFW) powered by machine learning (ML) could deliver the level of intelligent network security that the agency required.

Security deployments can be complex and overload IT teams with complicated security rules and mountains of data from numerous sources. This agency was looking for ease of management, administration, and implementation. Specifically, they needed a single pane-of-glass that would provide visibility into network traffic, logs, and threats. Due to their vast, diverse environment, the agency also needed the ability to manage firewalls agency-wide and to apply common rules across multiple devices.





The Solution

The Strata network security suite leverages the augmentation of Palo Alto's standalone NGFW's existing automation capabilities with the power of ML, enabling the agency to take a proactive, cloud-based approach to network security through a FedRAMP approved platform. Strata provides the agency with complete visibility across their network, from a single pane-of-glass, as well as automated response capabilities for enhanced ability to react. Swish recommended that the agency also subscribe to Palo Alto's Wildfire®, a cloud-based analysis service that is a prevention engine for highly evasive zero-day exploits and malware. The service employs a unique approach that combines dynamic and static analysis, ML and a bare metal analysis environment to detect and prevent even the most evasive threats while leveraging threat indicators from other federal entities on the FedRAMP approved platform.

To protect users accessing external websites, the agency subscribed to Palo Alto's URL Filtering. Attacks that leverage web browsing to deliver threats are more pervasive than ever and URL Filtering prevents these as well as credential-phishing pages. This service is a native component of Palo Alto's Next-Generation Security Platform so there is no additional operational burden.

Focusing on the agency's need for ease of management, Swish also recommended Palo Alto's Panorama™ network security management solution. Panorama includes easy-to-implement, consolidated policy creation and centralized management features. This allows the agency to configure, deploy and manage their firewalls centrally with an efficient rule base, and gain insight into network-wide traffic and threats. With URL Filtering controlled through Panorama, the agency can enforce policy across thousands of endpoints from a single pane-of-glass with instant effect.

Summary

Aware of the many cybersecurity solutions available, this government agency called on Swish to help them make the best decision for their needs and environment. Swish recommended Palo Alto's Strata, the first cybersecurity solution to incorporate ML into a NGFW. For easy implementation, maintenance, and management of their numerous firewalls, Swish recommended that the agency subscribe to Panorama network security management and to protect their users who access the web via networked devices, URL Filtering. Today, national and federal government departments worldwide count on Palo Alto Networks® and Swish to prevent successful cyberattacks, safeguard classified and sensitive data, and optimize security operations.

Swish is a Service-Disabled Veteran-Owned and HUBZone certified Small Business provider of technology solutions and engineering services to the U.S. Federal Government with a focus on high-quality outcomes for our clients. Swish's focused practice areas include Cybersecurity, Performance Engineering, IT Modernization and DevSecOps. To learn more, please visit: www.swishdata.com

1420 Spring Hill Road Suite 320 McLean, VA 22102

P 703.635.3324 / F 703.852.7904 / E info@Swish.com