CASE STUDY

US Federal Agency Boosts Security

A key US federal government agency had information siloed between the agency's headquarters, security operations center, and various field locations. This made it challenging to enforce security and IT policies across a decentralized network and led to numerous unknown, unmanaged and vulnerable Internet-connected assets.

paloalto® NETWORKS | CORTEX XPANSE™ BY PALO ALTO NETWORKS

Problem

A key US federal government agency had information siloed between the agency's headquarters, security operations center, and various field locations. This made it challenging to enforce security and IT policies across a decentralized network and led to numerous unknown, unmanaged and vulnerable Internet-connected assets.

Solution

The agency worked with Xpanse to define its global inventory of Internet-connected assets. It identified numerous exposures (including unprotected FTP and Telnet instances) and remediated them before attackers could exploit them. The agency now uses the Xpanse Platform powered by Expander on an ongoing basis to discover, monitor, and track Internet assets across all agency locations.

Outcome

The agency decreased critical exposures by over 58% and reduced the number of insecure certificates by 44% over a two-year period and is driving toward full remediation. Because they had a complete, current, and accurate asset inventory, the agency's headquarters and security operations center could finally enforce policies across the entire agency and raise its overall cybersecurity posture.

The Challenges of a Distributed Network

A major cabinet-level federal agency that manages projects related to science, technology, and infrastructure needed a better way to manage Internet-connected assets and services and monitor and enforce policies across a distributed network. Because the agency employs over 100,000 people and 85% of its workforce is contractors, it was easy for new infrastructure to be spun up outside of sanctioned IT processes. This meant the agency had a complex network where the security and IT operations teams had incomplete visibility and thus incomplete ability to defend the agency's network

The challenges at the agency came at a time when cyberattacks against US agencies and infrastructure have been ramping up. Attacks on the US electrical grid, the US Office of Personnel Management, and major US contractors like Boeing have all happened in recent years. In response to these escalating attacks, the US has a defined National Cyber Strategy that includes a focus on defending forward and moving to "halt malicious behavior at its source." A key part of this initiative that spans across government agencies is securing federal networks and critical infrastructure. The agency chose the Xpanse Platform to tackle these challenges head-on and boost its cybersecurity posture.

Identifying and Reducing Exposures

Once the agency engaged with Xpanse, one of its first tasks was to solve the problem of the security team having responsibility for a network it didn't have full ability to monitor and manage. At the time, it was the established practice across the agency for semi-autonomous field sites to make their own risk acceptance decisions without adhering to centrally decreed security policies. This paved the way for Internet-facing vulnerabilities that the security team didn't know about and thus could not remediate. In its initial IP address list audit, Xpanse showed that the agency had 40% more IP addresses than it knew about and was actively monitoring.

The security team used Xpanse Expander to independently identify assets and exposures across the entire network perimeter of the agency, and enforce remediation actions at the individual field sites. In one case, a particular field site used a series of networked security cameras extensively. The field site had a legitimate business use case for the cameras, but was unaware that the cameras' factory default configuration included File Transfer Protocol (FTP). These FTP instances were not encrypted or actively managed, and could have been accessed by unauthorized, malicious actors on the Internet. In addition to exposed FTP, there were field sites with publicly exposed Telnet servers, which are unencrypted remote access protocols that are a favorite target of attackers. Xpanse discovered these exposures and empowered the agency's security team to work with the field sites to properly configure, manage, and protect these devices and services.

With the Xpanse Platform, the agency gained total visibility into its global Internet attack surface. The security team no longer had to accept responsibility without visibility or authority — it could now discover, monitor, and track Internet assets and exposures across the entire organization, resulting in a heightened security posture. Leveraging Expander from August 2017 to April 2019, the agency decreased critical exposures by over 58% and reduced the number of insecure certificates by 44%, and is driving toward full remediation.

With a significantly reduced attack surface and automatic discovery and monitoring of new Internet-connected assets and exposures, the major US agency is more secure and able to focus on its mandate in service of the American people.

With continuous discovery and monitoring of assets as well as any communications between those assets and the Internet, Accenture has a secure foundation to continue delivering exceptional service to its customers in the digital age.

3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com