CASE STUDY

Fortune 100 Financial Services Company Reduces Attack Surface with Cortex Xpanse

Like most large financial institutions, this Fortune 100 financial services company has a complex network. From M&A activity to cloud development to securing critical suppliers, it was challenging for the company to identify and monitor all of its internet-connected assets. And without a complete and accurate IT asset inventory, it was even more challenging to secure those assets.

paloalto® NETWORKS | CORTEX® XPANSE™ BY PALO ALTO NETWORKS

Problem

A Fortune 100 financial services company has a complex network, and it is a challenge for the company to identify and monitor all of its internet-connected assets. It needs a complete an accurate IT asset inventory, covering M&A activity to cloud development to securing critical suppliers, in order to secure those assets.

Solution

The company uses Cortex® Xpanse™ as its central source of truth for all assets connected to the public internet. With automatic discovery and monitoring of its internet connected assets, its IT operations and security teams can more effectively monitor for exposures and reduce the company's attack surface.

Outcome

Working with Xpanse, the company identified and removed a previously unknown Remote Desktop Protocol (RDP) server exposed on the public internet. It also eliminated more than 20 critical exposures and reduced the number of publicly accessible services from more than 1,200 to 175. These actions eliminated potential entry points for attackers and improved the company's cybersecurity posture.

COMPLEX NETWORKS REQUIRE GLOBAL VISIBILITY

The Fortune 100 financial services company is a veritable giant in its industry. It's one of the 25 largest banks in the United States.

One big contributor to the company's success has been its business development strategy, which has resulted in a number of high-profile acquisitions over the past decade. But this business expansion meant that IT and security teams had to grapple with a new challenge: integrating the networks and technologies of its new subsidiaries. With thousands of new internet-connected assets to integrate and manage the lifecycles for, they knew it could be all too easy for some assets to get missed. And without a complete, accurate, and current internet asset inventory, they couldn't be sure they were securing all of their assets appropriately.

REDUCING EXPOSURES IN THE CLOUD AND BEYOND

The company partnered with Xpanse to tackle this challenge head-on. The company began using Xpanse Expander to discover, monitor, and track all of its internet-connected assets, including IP addresses, domains, and certificates. It also uses Xpanse Behavior to monitor for any risky or out-of-policy communications, like banned communications to Office of Foreign Assets Control-designated countries, cryptocurrency mining, and use of Tor, or peer-to-peer sharing services. When the security team gets an alert from Behavior, they are able to remediate the issue almost immediately and put systemic changes in place that would prevent the problematic behavior from surfacing again in the same place.

Using Expander's cloud module, the security team discovered a previously unknown system that exposed a remote desktop protocol server on the public internet. The RDP server in question connected to automatic blinds at the headquarters building of an acquired company. The Fortune 100 financial services company had taken ownership of the building during the acquisition, but due to the complex financial terms of the deal, it was prevented from getting global visibility into all building subsystems, even post-acquisition.

Building control systems are common attack vectors because they often aren't under active management by IT or IT security teams, but rather by facilities or operations teams that routinely lack cybersecurity expertise. The discovery of this RDP exposure was only possible because of Xpanse's internet-wide visibility and ability to correctly attribute internet-facing assets back to the company.

Apart from this RDP exposure, the company has remediated more than 20 critical exposures with the help of Xpanse, including 16 audio and video teleconferencing systems, and eliminated or replaced hundreds of non-compliant certificates in its internet-facing infrastructure. The company has also reduced the number of its publicly accessible services on the internet from more than 1,200 to 175, greatly reducing its overall attack surface.

With a significantly smaller attack surface and automatic discovery and monitoring of new internet-connected assets and exposures, the company is able to carry forward its mission of delivering the best possible financial products and services to customers.

paloalto NETWORKS | CORTEX XPANSE BY PALO ALTO NETWORKS

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

cortex-xpanse-fortune-100-financial-services-company-reduces-attack-surface-with-cortex-xpanse-cs-051421