CUSTOMER SUCCESS STORY

Global Bank Hardens Defense with AI to Counter Network-Based Adversaries

How does one stop advanced threats? It's not that easy when you're in the financial services industry. Financial organizations experience thousands of attacks targeting employees every day as well as advanced threats targeting their critical infrastructure, systems and applications.

The risks involving these attacks become even greater for global banking organizations. These large financial entities need to ensure their security controls keep pace with the onslaught of digital threats. Strategies to defend the perimeter with layers of defense in depth, which worked well in the past, are no longer reliable. Current events show us that attackers penetrate these financial networks at an increasing rate. This brings high-vulnerability banking applications, SWIFT financial networks and ATMs within the reach of bad actors.

Cyberdefenders know that it is almost a certainty that an adversary will penetrate an internal network. The challenge today is to rapidly detect them within the networks and then shut them down. Today, your strategy must evolve to meet these tough adversaries.

Legacy security tools are often not capable of detecting all of these incoming threats. Most of these systems utilize rules to set the boundary between activity that is acceptable and activity that should generate an alert. If the boundary conditions are set too tightly, then adversaries will penetrate the network. If the boundary conditions are set too loosely, then the volume of alerts is usually unmanageable. This leaves it up to the security teams to spend scarce resources investigating a multitude of false positive activity indicating potential attacks, which wastes time and distracts from real threats that have not been found.

COMPANY

Fortune Global 1000 Company

INDUSTRY

Financial Services

ENVIRONMENT

50,000 employees in North America, Europe, Asia and Latin America

CHALLENGE

- Stop advanced threats that bypass existing perimeter security controls
- Improve visibility of attacks already inside the network

VMWARE FOOTPRINT

VMware NSX® Network Detection and Response™

RESULTS

- Deployed NSX Network Detection and Response in blocking mode to stop malicious web traffic and email content before it enters the global network
- Deployed NSX Network Detection and Response to identify lateral movement
- Validated the AI-powered detection and response from NSX Network Detection and Response

One leading financial services company included on the Fortune Global 1000 list deployed various defense-in-depth technologies to counter this problem. These solutions included a next-generation firewall (NGFW), a web proxy, an anti-spam mail filter, and an intrusion prevention system (IPS). But even together, these and other utilities failed to provide an adequate level of visibility and protection. They were concerned that attackers could penetrate the network and remain undetected for unacceptably long periods of time. The security operations center (SOC) team and the suite of products they deployed could not keep up with the volume of alerts generated by existing tools. They no longer had confidence in those tools' abilities to accurately detect all of the threats targeting the bank.

The financial services firm needed a more capable solution to help meet and defeat the advanced threats targeting their network. It was important for the chosen solution to provide the necessary protection without disrupting business-critical operations. After considerable research, they decided to deploy a technology utilizing AI-based detection and response technology. This would substantially save their SOC team time in rapidly identifying the active and dangerous threats potentially already within their networks.

The solution

The bank chose VMware NSX Network Detection and Response based on its proven threat detection and response capabilities, powered by supervised and unsupervised machine learning. They used NSX Network Detection and Response to detect malicious content hidden within incoming emails, thereby serving as a supplement to their mail server security and anti-spam tools. NSX Network Detection and Response was initially deployed in monitoring mode only, but was switched by their security team to blocking mode after the AI-powered solution demonstrated high accuracy and broad detection capabilities.

The bank used NSX Network Detection and Response to detect malicious web traffic that bypassed their NGFW and web proxy. As with the first stage, the organization ultimately set NSX Network Detection and Response to blocking mode after initially configuring it to only monitor for threats. They did this after they validated that NSX Network Detection and Response would not impact legitimate traffic. NSX Network Detection and Response also demonstrated high competence in detecting sophisticated threats engineered to evade detection by next-generation products, such as fileless malware and polymorphic keyloggers such as Emotet.

The financial services firm then used NSX Network Detection and Response to detect lateral movement in the network by any existing or new threats. These network-resident threats were constantly being introduced by visiting contractors and employees compromised by phishing attacks (perhaps via their personal email or, in some cases, by visiting malicious websites from home). NSX Network Detection and Response reduces false positives by up to 90 percent. This high accuracy was extremely important to enable the blocking of internal traffic and reduce the time required by the security team to investigate many spurious alerts.

The results

The financial services firm currently has NSX Network Detection and Response deployed throughout their global network. The security team values the flexibility and scalability of NSX Network Detection and Response, which enables them to deploy across their global network for maximum protection. NSX also provides the organization with unparalleled visibility into the complete series of intrusions that cover the MITRE ATT&CK techniques. For example, NSX has allowed the firm to see every stage within any given attack—whether a user clicked on the email or executed the attachment, what happened after the attachment executed, whether the compromised host established communication with an external host, whether the attack involved additional accounts or hosts, and which datasets were accessed.

> "VMware NSX Network Detection and Response helps us sleep better at night—we know that NSX will detect it."
>
> FORTUNE GLOBAL 1000 COMPANY

Such visibility has also significantly reduced the organization's time to respond. Their reliance on the more accurate assessments provided by NSX Network Detection and Response to actively block threats before they enter the network has drastically reduced the number of threats entering their network. And the NSX high-fidelity analysis has freed security professionals from the burden of following up on false positives generated by other tools. Indeed, the financial services firm has already validated the low false positive rate from NSX Network Detection and Response, which has inspired peace of mind in the solution's capability to detect and stop legitimate attacks without affecting business operations.

Looking ahead to the cloud

The financial services firm is also in the initial stages of migrating some of their workloads to the public cloud. NSX Network Detection and Response will be able to keep pace with the organization during this migration because it delivers the same AI-powered network detection and response protection against threats trying to enter or operate within the cloud environment as it does with on-premises networks. The bank will be able to benefit from unmatched visibility and protection of their entire network, on premises and in the cloud, from a single management console.

Harden your defense today

Attackers use different paths to compromise and move around your network. It is critical for a threat detection solution to monitor them all and deliver complete visibility into the entire attack chain, without burying your security team in false positives. The AI-powered security from VMware NSX Network Detection and Response provides unmatched protection from threats that cross your network perimeter as well as move laterally inside the network for both on-premises and cloud environments.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com