GOVERNMENT RESEARCH FIRM SLASHES DETECTION AND REMEDIATION FROM DAYS TO MINUTES WITH FIREEYE

KEY COMPONENTS

- FireEye Network Threat Prevention Platform (NX Series)
- FireEye Email Threat Prevention Platform (EX Series)
- FireEye Endpoint Threat Prevention Platform (HX Series)
- FireEye Central Management (CM Series)
- FireEye Multi-Vector Virtual Execution™ (MVX) engine

As a federally funded research and development center (FFRDC), this organization works on long-term technical research projects in areas such as defense, space, and energy. The center routinely finds itself in the crosshairs of nation-state cyber-spies seeking lucrative scientific research data.

BUSINESS CHALLENGE

The entity's Cyber Security team's main focus is on detecting adversaries and preventing or minimizing data theft. It had evolved a layered defense solution that included firewalls, encryption, and anti-virus (AV) software, but adversary tactics were becoming more sophisticated. Targeted malware circumvented signature-based anti-virus tools and there was no defense when employees fell victim to an email phishing scam or visited a compromised website. As the workforce became more

COMPANY	Federally Funded Research and Development Center (FFRDC)
Industry	Research and Development
Description	Government funded entity, with 1,200 employees
Challenges	• Detecting adversaries and preventing or minimizing data theft • Adversary tactics becoming more sophisticated • Targeted malware circumventing signature-based anti-virus tools • Increased risk with more mobile workforce, through lack of visibility into off-network machine activity
Solutions	• FireEye Network Threat Prevention Platform • FireEye Email Threat Prevention Platform • FireEye Endpoint Threat Prevention Platform • FireEye Central Management • FireEye Multi-Vector Virtual Execution™ (MVX) engine
Benefits	• Reduced detection and response from days to minutes • Minimized disruption, and decreased remediation costs • Optimized adminstration overhead through centralized reporting

FireEye

mobile, the risk increased because the team lacked visibility into off-network machine activity.

The center had developed its own custom investigation and forensics tool, but it was not scalable beyond a handful of machines. The impact of downtime on employees caused by remediation efforts also was significant, sometimes requiring hours and even days to complete. The team also had no traceability from network detection to the endpoint, limiting its ability to prioritize and scope incidents or track and report on key metrics. The organization needed a better detection and incident response solution.

SOLUTION

In 2011, the center purchased the FireEye® Network Threat Prevention Platform and FireEye® Email Threat Prevention Platform to detect initial intrusion attempts through web drive-by downloads and spear-phish emails more quickly. FireEye was selected because of the company's Multi-Vector Virtual Execution™ (MVX) engine, which is able to detect never-seen-before (signature-less) malicious files and URLs and quarantine them. The combination of NX Series and EX Series, deployed in TAP mode and managed through the FireEye® Central Management, enabled the identification and analysis of suspicious files detected on the network and blocking of communication between hosts and malicious websites. The spread of a spear-phishing attempt can now be traced within minutes; allowing identification of other message recipients, and outreach to targeted mailboxes to remove known-bad emails and attachments.

The organization added the FireEye® Endpoint Threat Prevention Platform in 2013, which enhanced the ability to trace intruder activity found on the network all the way to the endpoints. With an average of 30 advanced attacker alerts daily, the HX Series helps prioritize the handful that need further investigation and remediation, limiting the scope of response to just the affected machines. Fed by global dynamic threat intelligence (DTI) provided by NX Series and EX Series as well as 3rd party indicators, HX Series shows which employees actually clicked on a malicious link or were the recipient of a web drive-by attack. HX Series also scans machines that are off-network to proactively look for signs of attacker activity. With a mobile workforce, the ability to detect compromises, contain the machine, and instruct remote users on appropriate action has proven valuable in preventing data theft and attack escalations. This combination of network, email, and endpoint security enables the government research firm to:

Detect and Stop Advanced Attacks on Multiple Fronts: FireEye Network Threat Prevention Platform detects and dynamically analyzes traffic emanating from or going to suspicious URLs, while FireEye Email Threat Prevention Platform analyzes the contents and file attachments of emails. When threats are confirmed, communication is blocked and malicious files are quarantined.

Identify Affected Endpoints and Contain an Attack in Minutes: FireEye Endpoint Threat Prevention Platform continuously monitors endpoints using indicators from FireEye and 3rd party products to locate compromised hosts on- or off-network. Containment of endpoints interrupts attacks in progress while allowing for immediate investigation.

Aggregate and Correlate Events to Identify Blended Attacks: FireEye® Dynamic Threat Intelligence provides the latest information about attacker tactics gathered around the globe, while FireEye Central Management correlates malicious URLs with the originating emails and the intended victims to reveal the attack lifecycle.

BUSINESS BENEFITS

By deploying FireEye network, email, and endpoint security products together with Dynamic Threat Intelligence and the Central Management, the company is able to implement a broader defense that detects attacks earlier in the lifecycle. By correlating data and information across the security ecosystem, events detected on the network can be traced to compromised endpoints and immediately contained. The Cyber Security team can then prioritize remediation efforts and reduce impact across the organization.

Some of the specific benefits the organization has already realized include:

Rapid Detection and Response: FireEye immediately quarantines malicious files, alerts when emails with suspicious URLs reach a mailbox, and enables the team to retrieve those emails from recipient Inboxes. Continous monitoring of hosts on- and off-network detects actor activity on endpoints, with the ability to contain a system and remediate remotely.

Reduced Disruption & Remediation Costs: Having visibility and traceability of activity on the network all the way to the endpoint and with few false positives, the team can optimally scope and prioritize incident response. It can triage an incident without having to take over each employee's machine for an hour or more. Incident response is faster, more accurate, and results in less downtime.

Centralized Reporting: Consolidated security information provides better reporting of key metrics, such as frequency, type and method of advanced targeted attacks and system-level incident and remediation trends. This helps the team communicate the organization's security posture to executives.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye