CUSTOMER STORY

Asian Media Company Enhances Protection Across Multi-OS Environment

FireEye Network Security Brings Cross-Infrastructure Visibility and Improved Team Efficiency

FACTS AT A GLANCE

INDUSTRY

Media

SOLUTIONS

- FireEye Network Security

BENEFITS

- Operating system agnostic technology protects hybrid environment dominated by macOS devices
- Visibility and control across entire infrastructure simplify security operations
- Real-time monitoring of network traffic minimizes exposure to malicious activity
- Actionable intelligence from global FireEye community enhances security posture

CUSTOMER PROFILE

This media company's local language newspaper is the largest in its country. Founded many decades ago, the company has evolved into a 24/7 media outlet that utilizes print, broadcast and online channels to deliver both news and entertainment.

One regional media company has ensured that residents across its country have access to information about politics, the economy, society and entertainment through its printed newspaper, the most popular in the nation. As a high-profile media source enjoyed by millions with an internal network of 1,500 end users, the company's attack surface is a prime target for cyber criminals.

The organization's chief technology officer (CTO) commented, "Advanced attackers have multiple motivations for targeting our company, including exploiting our brand's popularity, damaging our reputation, stealing our unpublished stories or even negatively influencing our coverage of political issues."

The media outlet typically receives over 1,500 spam and phishing emails per day; approximately one for every reporter, writer, editor, analyst, administrator and executive employed by the company. To secure its environment, the organization was relying on a firewall, intrusion prevention system and antivirus software solution from an assortment of vendors.

However, this combination of technology generated an overwhelming number of alerts and offered little help filtering out false positives. "We knew gaining more accurate visibility across our network was crucial to strengthening our overall security and enhancing the effectiveness of our team," recalled the CTO.

> “Implementing FireEye Network Security addressed key vulnerabilities in our infrastructure that the other solutions missed.”
>
> — Chief Technology Officer, regional media company

Holistic Security Begins with Threat Visibility

Updating the organization’s network defenses required a solution capable of providing deep visibility into a hybrid environment that is 90% comprised of devices running the macOS® operating system. The company also needed a solution that could operate without requiring a dedicated full-time security professional.

The CTO conducted individual proofs of concept (POCs) on solutions from three leading security providers—including FireEye—to evaluate their performance.

Within a week of starting the POC on FireEye Network Security, they detected three infected machines and four instances of dormant malware that had evaded the company’s legacy security measures. “We also learned that the compromised endpoints were attempting to make previously undetected communication back to command-and-control servers. FireEye experts immediately reported the activities to our team and blocked the devices before anything further could occur,” recounted the CTO.

The POC irrefutably demonstrated the unique ability of FireEye Network Security to identify malicious activity in the media outlet’s environment. The CTO elaborated, “Deploying FireEye technology confirmed my suspicions that there was the possibility of a gap in our defenses: Many of our security tools were designed to only protect against Microsoft Windows®-based threats. Implementing FireEye Network Security addressed key vulnerabilities in our infrastructure that the other solutions missed.”

Fueled by Actionable Intelligence

FireEye Network Security analyzes network traffic in real time, efficiently identifying threats like callbacks from an infected client and DNS queries to blacklisted IP addresses. To better leverage its fixed resources, the company engaged a local FireEye managed security services provider to help deploy and monitor the solution. The CTO reported. “The impact was immediate. Once anything malicious is detected, FireEye Network Security creates a rule to block the activity and deploys countermeasures across the entire infrastructure.”

A Collaborative Future

Envisioning future possibilities to evolve the organization’s security posture, its CTO revealed, “Now that I’m confident our network has this level of protection, I am excited to shift attention to further cultivating the skills of our team members, with the ultimate goal of creating our own autonomous security operations center.”

He reflected, “It is important to us to be part of the global FireEye community; sharing threat intelligence around the world gives us the ability to collaborate with other companies to combat attacks, irrespective of where they might first occur. It’s impossible to be truly 100% secure but together we definitely are stronger.”

To learn more about FireEye, visit: **www.FireEye.com**

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

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.