FIREEYE™

CUSTOMER STORY

Prominent Stock Exchange Continues to Rely on Protection from FireEye

FACTS AT A GLANCE

INDUSTRY

Finance

SOLUTIONS

- FireEye Network Security
- FireEye Endpoint Security
- FireEye Central Management
- FireEye Managed Defense
- FireEye Network Forensics Platform
- FireEye Investigation Analysis System
- FireEye Threat Analytics Platform
- FireEye Platinum Priority Plus Support

BENEFITS

- Seamless multi-vector protection throughout diverse global infrastructure
- Intuitive, centralized monitoring and management of entire environment
- Real-time threat detection, rapid investigation and mitigation

CUSTOMER PROFILE

Prominent global stock exchange

This exchange's high-profile makes it a prime target for cyber criminals. A principal security specialist for the organization commented, "We are at the hub of the world's financial ecosystem; not only do we handle enormous dollar volumes but any disruption can have a massive global impact and the potential to create widespread destabilization. Back in 2010 we reached the conclusion that we needed to reinforce our unified threat management measures for our internal systems; traditional security solutions were not proving sufficiently robust in keeping us ahead of the escalating threat curve."

A globally known name needs world-class security

The exchange's extensive infrastructure contains a wide range of hardware components, operating systems, and applications. "To even be considered as a viable option, any solution had to be able to cope with the full diversity of our environment; including Windows, UNIX, Linux, and Mac OS-based platforms," noted the security specialist.

The exchange takes a holistic approach to its IT environment: Project teams collaborate to come up with a broad set of requirements, including the definition of security defenses. The security specialist recalled, "We strategized on exactly what was needed to provide comprehensive protection for our environment. We'd heard about the growing reputation of FireEye solutions across the industry and were enthusiastic to verify what was being said.

"We've been in partnership for well over half a decade, and FireEye has continued to stay at the front of the pack through the innovation and agility of its solutions."

—**Principal security specialist,** prominent global stock exchange

We assembled a selection of FireEye platforms to create a proof of concept and – after confirming that the performance actually exceeded expectations – we rolled the solutions straight into production."

Today, the exchange has implemented multiple components from the FireEye security portfolio, including:

- FireEye® Network Security (NX) solutions to protect from web-based cyber attacks
- FireEye® Email Security products (EX) to block email attacks
- FireEye® CM series to centralize management of the FireEye defenses
- FireEye® Managed Defense for managed security services
- FireEye® Network Forensics Platform (PX series) for accelerated identification and resolution
- FireEye® Investigation Analysis System (IA series) facilitating deep research capabilities
- FireEye® Threat Analytics Platform (TAP) enabling improved response times to attacks
- FireEye® Platinum Priority Plus Support for priority access to Level 2 Advanced Engineering support

Multi-vector attacks require multi-layered defenses

The exchange's security specialist reflected, "The FireEye solutions are doing exactly what we need them to do. Running everything inline, we experience near-zero false positives, instantly block malware and are able to resolve most valid alerts in less than two hours."

The FireEye Platinum Priority Plus Support program covers both hardware and software, and provides a targeted response time of under one minute, delivered through email, live chat, web, and telephone support channels. "Platinum support is just excellent; I get instant response, even over a weekend. I really view my Platinum engineers as an extension of my own team; they are very consultative and are a constant source of great advice," stated the security spokesperson.

"I'm also a big fan of the CM series console: Managing everything in an environment of our magnitude and complexity could turn into a nightmare but the console gives us an intuitive interface to administer the entire ecosystem and correlate alerts from all the connected platforms. It enables me to view our whole deployment on one piece of glass, which is really great for our global enterprise. It has proved to be especially effective when we do shift changes; the incoming team can instantly see the status of every appliance and every layer across the entire infrastructure."

While exchange's entire security stack is very complex, having multiple protection solutions from a key vendor brings additional benefits. The security specialist expounded, "I'm a confirmed advocate of multi-layered protection, and having the tiers provided by the same company means that there are no gaps, no dropped balls. As a FireEye client for many years, it's clear that the integrated FireEye applications continually excel with handling threats that move across different domains and threat vectors. Irrespective of threat origin—be it email, website, or network—I have the confidence that things won't slip through the cracks."

"FireEye Network Forensics Platform and Investigation Analysis complement our perimeter defenses with strong research capabilities, enabling us to rapidly investigate and remediate attacks."

—**Principal security specialist,** prominent global stock exchange

Combining agility and innovation

The portfolio of FireEye solutions and services provides seamless, multi-vector protection throughout the global infrastructure and each individual element provides the exchange with best-in-class protection.

"Every component from FireEye stands on its own merit. For example, the NX Series gives us great deployment flexibility and local dynamic rule generation; both invaluable to us. The EX Series also gives us numerous options for implementation and it automatically communicates with the NX platforms to ensure that they are always synchronized," observed the specialist.

"The FireEye Threat Analytics Platform capabilities allow us to report on overall system health for managed services and expedites the rapid delivery of security-related updates across our worldwide infrastructure. It also links in to FireEye's global intelligence network that connects millions of virtual machines embedded in every industry and every location: this gives us immediate notification of threats and automatic access to remediation intelligence gathered from those events."

He continued, "FireEye Managed Defense provides the exchange with sophisticated threat validation and proactive pursuit of any signs of potential compromise. We added the FireEye Network Forensics Platform and Investigation Analysis system to complement our perimeter defenses with strong research capabilities, enabling us to rapidly investigate and remediate attacks."

The exchange's security specialist concluded, "The sophistication and numbers of threats are always escalating, and things change on a minute-by-minute basis. It would be naïve to ever claim to be 100% secure but the agility of the FireEye solutions contributes to my level of comfort in knowing that we consistently have best-in-class protection in place."

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.

FIREEYE™