CASE STUDY

FireEye

Top Law Firm Protects Clients' Interests by Deploying FireEye Web MPS to Combat Advanced Malware and Targeted APT Attacks

SECURITY REIMAGINED

KEY COMPONENTS

- FireEye Web Malware Protection System 4000 Series appliance

This law firm has built its reputation on crafting creative trial strategies and has amassed an impressive record for winning cases. The daily substantial volumes of information handled by the partnership imposes a heavy responsibility, the firm's Director of IT, elaborated, "By the very definition of our business, all of our data is highly sensitive. It is a company-criticalimperative to ensure that all possible precautions are taken to safeguard the integrity of the information with which we are entrusted."

The Evidence is Clear

The original IT security infrastructure relied heavily on mainstream firewall products to provide perimeter protection for the network. The Director of IT commented, "We never had a specific issue with running just a firewall, but we were cognizant of other law firms being

COMPANY	New York-based Law Firm
INDUSTRY	Legal
DESCRIPTION	This New York-based law firm specializes in delivering legal expertise to financial services firms and other multinational corporations. In addition, it is well known for its commitment to providing pro bono services to assist disadvantaged, disabled and deserving clients.
CHALLENGE	• Identify a security solution to elevate the protection of the company's infrastructure beyond levels typically provided by traditional signature-based technologies. Viable candidates needed to provide next-generation protection, and be easy to install, without degrading existing network traffic throughput.
SOLUTION	• Deployment of FireEye Web Malware Protection System (MPS) 4000 Series appliance.
BENEFITS	• The FireEye Web MPS appliance was rapidly configured into the infrastructure and provided immediate visibility into the characteristics and integrity of network traffic. An imperceptible impact on network performance and sophisticated real-time malware detection capabilities culminated in the test appliance becoming a per manent fixture in the firm's IT security environment.

"We thought that the FireEye appliance was fantastic: The power of its malware detection technology was the ultimate decision maker for us."

— **Director of IT,** Law Firm

hacked and were aware of the potential for data leakage instigated by zero-day malicious code."

He continued, "We were literally on the verge of signing a deal with another vendor when I had a call from a FireEye sales representative. I was sufficiently intrigued by what FireEye had to offer that I placed the original order on hold and agreed to perform a proof of concept with the FireEye appliance."

The evaluation was conducted over a period of 30 days. The Director of IT recalled, "The appliance was easy to install and we felt that the technology gave us unique benefits that weren't available from any other vendor. The FireEye Malware Protection System was the only product that focused on real-time interpretation of the specific intent of potentially malicious code, versus the rigid signature-based approach—and difficult to administer heuristic-based techniques—that everyone else offered."

The law firm halted discussions with the competing vendor and purchased a FireEye Web Malware Protection System (MPS) 4000 Series appliance to protect its flagship New York office. The FireEye Web MPS appliances continually scrutinize, isolate and confirm zero-day malware and targeted attacks using a unique multi-phase analysis engine that executes potentially malicious code in a full-featured virtual execution engine.

Case Proven

The FireEye appliance was originally deployed in a monitor-only mode, but the firm's evaluation team quickly gained the confidence to transition to an inline configuration. The Director of IT described, "Before the move inline we manually addressed each alert, and were able to confirm an extremely low false-positive rate. This gave us the confidence to go inline and we immediately benefited from having call-backs automatically blocked and zero potential for data exfiltration."

As with any device placed directly in the path of large volumes of network traffic, the impact on throughput performance was a major consideration. However, the Director of IT quickly dismissed the concern, "Having researched the FireEye appliance's specifications, we were comfortable that there would be no adverse effects on network throughput. I would be very hesitant to do this with most equipment, and am aware that several security-related boxes from other vendors have severe issues with restricting bandwidth."

He concluded, "We absolutely feel more secure than we did prior to deploying the FireEye appliance. Having the device protecting our infrastructure gives us the confidence that we are blocking malicious code and the assurance that no data is being inappropriately sent outside of our network."