FireEye

Case Study

A Leading Law Firm Relies on FireEye to Protect Highly Sensitive Client Data

Key Components

- Multiple FireEye Web Malware Protection System (MPS) 4000 and 7000 Series Appliances
- FireEye Malware Protection Cloud (MPC)
- FireEye Central Management System (CMS)

With an international reputation and many high-profile clients, this prestigious law firm represents a prime target for malicious Web-based assaults. Despite having a best-in-class suite of next-generation intrusion prevention, anti-virus, and firewall solutions, the rapidly evolving sophistication of cyber threats motivated the firm to look for an elevated level of protection.

The Director of Information Technology explained, "We wanted to be equipped to block malicious traffic both into and out of our environment, rather than just being alerted when a machine had become infected. We needed to know that there was a mechanism in place to actively prevent information from being compromised."

Company	Leading Multi-National Law Firm
Industry	Professional Services
Description	Headquartered in North America, with offices in Europe and Asia, this multi-national law firm offers a full-service portfolio of corporate law and litigation services to clients. With lawyers and professionals numbering into four digits, the firm is one of the oldest and most respected in the nation.
Challenges	• Remove limitations of existing signature-based protection • Identify effective, easy-to-deploy, low-operational overhead solution • Tailor solution to match traffic requirements at each location
Solution	Deployment of multiple FireEye Web Malware Protection System 4000 and 7000 Series appliances, FireEye Central Management System, and FireEye Malware Protection Cloud.
Benefits	• Virtual Execution engine detects and blocks unknown threats, which otherwise easily bypass traditional signature-based protection • Immediate isolation of potentially malicious elements allows orderly remediation of threats • Multiple configuration options allow optimally sized appliances to be selected for each location • Ease of deployment results in nominal operational impact • Appliances are administered centrally using intuitive graphical dashboard that provides infrastructure-wide integrated view of all activities

FireEye

Case Study

"Since deploying the FireEye Web Malware Protection System we've seen explicit evidence of malware trying to invade our environment, but because the appliances have eliminated any ability of the malicious code to execute and communicate, we know the threat cannot perform its intended function."

— Director of Information Technology, multinational law firm

A wide range of potential solutions was evaluated. The IT Director recalled, "We examined a lot of different products, including Damballa, and contacted many reference accounts to gain insights from actual users of the various solutions. Based on our findings, we selected the Web Malware Protection System (MPS) appliances from FireEye."

Capturing Zero-Day Malware

"One of the compelling aspects of the FireEye solution is the ability to detect potentially malicious code or objects as soon as they arrive. Anything suspicious is isolated and executed in its own virtual environment to establish intent. At no point during this process is inbound or outbound communication permitted. We've also found that the number of false positives generated is entirely nominal."

Instead of relying on a heuristic estimation of risk, the multi-phase Virtual Execution (VX) engine examines potential zero-day malware and targeted attacks by executing suspected malware in a full-featured virtual environment to determine root intentions. This approach eliminates the typical weakness of only detecting malware that correlates to a previously cataloged signature. Because the VX engine detonates code against a range of browsers, plug-ins, applications, and operating environments, a FireEye Web MPS appliance is frequently credited with being the first in the world to detect a new malware strain.

The IT Director observed, "We're hearing about malicious code that is written to specifically target one particular company; if that is the case, there is no chance that any of the signature-based products will be of the slightest help. Having protection that doesn't rely on signature or pattern matching provides us with a very significant advantage."

A Comprehensive Solution

To fully benefit from the advanced detection capabilities, the law firm joined the global Web MPS user community in utilizing the FireEye MPC to dynamically share malware security intelligence.

FireEye Web MPS appliances were deployed at each of the law firm's North American offices. The Director commented, "Because FireEye offers a variety of different sized Web MPS appliances, we were able to select a configuration for each location that optimally reflected traffic volumes. I also really appreciated the ease of implementation; the impact was nominal. I am very impressed!"

FireEye Web MPS management, reporting, and data sharing duties at the firm are handled by the network-based FireEye CMS. The intuitive graphical dashboard presents a system-wide view of all relevant activities, including real-time alerts and the ability to perform detailed analysis of threat characteristics to determine next steps.

The IT Director commented, "We do not provide 24/7 support coverage, but knowing that potentially malicious code is automatically isolated means that we can handle any threats in an orderly fashion during normal operational hours."

He summarized, "Since we've had the FireEye appliances installed, I absolutely do feel more secure."