

Fortune 500 Company Chooses FireEye in Competitive Evaluation

Summary

Company	Fortune 500 Company
Industry	Hi-Tech
Description	Multinational IT software and services company
Challenge	Supplement existing firewalls, antivirus and intrusion prevention systems to mitigate exposure to advanced malware threats like zero-day and targeted APT attacks.
Solution	FireEye Web Malware Protection System Appliance
Benefits	Malware infiltration threat mitigated by lab-proven, best-in-class malware protection solution, providing verified industry-leading speed and accuracy of detection.

A member of the Fortune 500, this US-based multinational IT software and services company had revenues in excess of \$5 billion in 2010. Understanding that traditional firewalls, antivirus and intrusion prevention systems were not sufficient to provide effective coverage against today's advanced malware threats, the company's CISO initiated a project to identify solutions to address the vulnerability.

Potential contenders – including Damballa and McAfee – were brought into the company's lab environment that mirrored the diverse deployment infrastructure, containing a variety of Linux, HP-UX, Solaris and Windows-based platforms. Volumes of regular network traffic were combined with a selection of actual zero-day malware code samples to evaluate the detection capabilities of each solution. The CISO elaborated, "We released the malware code inside of our isolated lab and initially looked at two factors to be representative of each solution's effectiveness; what was detected, and how quickly the detection occurred."

"I'm dumbfounded that beyond FireEye nobody else appears to have a solution that addresses the biggest threats that we face."

– Fortune 500 Company Chief Information Security Officer

Instantaneous Detection

The pragmatic evaluation revealed some dramatic results. The CISO stated, "The FireEye appliance absolutely, unquestionably dominated the competition! (McAfee was not even a real contender.) It was actually very disappointing that no one could get anywhere-near to the performance delivered by the FireEye solution." Other companies like next-generation firewall vendor Palo Alto Networks and intrusion prevention systems vendor SourceFire were initially considered but quickly dismissed as not viable because of being focused on completely different areas from FireEye – neither stop zero-day or targeted APT threats.

In order to have a token comparison point, the company then performed a more intensive evaluation of the FireEye Web Malware Protection System (MPS) appliance against a unit from Damballa. The CISO recalled, "We conducted what became known as 'the bakeoff' however, we always felt that it was not a true peer-to-peer comparison: The FireEye approach is to perform a true real-time binary analysis of the traffic, but the Damballa solution focused on looking for more obvious indications of a problem."

He continued, "The FireEye Web MPS appliance was able to provide ostensibly instantaneous detection of any zero-day code that we injected into the lab test environment. With Damballa, the same malicious modules were able to establish themselves and execute whatever they were designed to do, before we finally got an alert sometimes up to a week later!"

Speed and Accuracy

In parallel with proving its speed of detection, the FireEye solution was equally adept in its accuracy. The CISO described, "With the notable exception of FireEye the false-positive rate was a massive issue with every solution we tested. In one instance, for every valid hit [positive-positive] we got literally a thousand false-positives! With Damballa for every correct hit, we got maybe three false-positives. The FireEye appliance's false-positive performance also stood out because we didn't see any."

Using a standard data-breach, annual loss expectancy calculation, even a highly conservative estimation of the savings to be gained from purchasing a FireEye solution proved to be compelling enough to make the investment. The first FireEye Web Malware Protection System was installed in late 2010.

Since the bakeoff, the company has continued to monitor the malware threat deterrent landscape very closely. The company's CISO commented, "We repeatedly test our deployed security components in the lab and keep a close eye on the marketplace; and while other vendors are constantly trying there is still no one closing the gap on FireEye."

"FireEye is continually innovating and staying ahead of the competition in delivering solutions that address the most current and insidious threats. The malware threat-scape is continually changing and evolving; which means that our protection needs to move at least as fast to keep ahead. The success rate we see from FireEye is a clear demonstration of the company's ability to do this."

Key Components:

FireEye Web Malware Protection System Appliance

FireEye is the world leader in combating advanced malware, zero-day and targeted APT attacks that bypass traditional defenses, such as Firewalls, IPS, AV, and Web gateways!

© 2011 FireEye, Inc. All rights reserved. FireEye, Inc. and all FireEye, Inc. products are either trademarks or registered trademarks of FireEye, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. -- CS.F50092011