Case Study

Financial Services Company Chooses FireEye After Competitive Comparison

Summary

Company	S&P 500 Company
Industry	Financial Services
Description	Multinational financial services company
Challenge	Provide protection against Web-based threats that elude traditional firewalls, antivirus and intrusion prevention systems.
Solution	FireEye Malware Protection System Appliance
Benefits	Operationally-proven solution fills void in security portfolio to provide verified industry-leading accuracy of detection and mitigation.

A member of the S&P 500 Index®, the company has almost 10,000 employees serving financial services markets throughout North America, Latin America and Europe. Primarily focused on business customers, its broad portfolio of products are commonplace components in the toolsets of the world's leading financial institutions.

The inherent sensitivity of financial information imposes a significant responsibility on all parties entrusted with its safekeeping. The company's Chief Security Officer (CSO) elaborated, "The security of each client's information is fundamentally important to us. If there is even the merest hint of suspicion that customer details have been compromised in any way, we risk erosion of the foundation of trust on which our company is built."

> **"I definitely feel that we're getting extreme value for the money. The FireEye solution is filling a huge gap that existed in our security architecture."**
> *– S&P 500 Company Chief Security Officer*

Closing the IT Security Gap

The company had identified Web-based threats as a likely major vector for data theft. With the perpetual escalation of Web-based threats and their increased sophistication this mandated the need to continually evaluate the effectiveness of deployed security defenses. The CSO described, "We had a very robust suite of traditional tools, such as firewalls, intrusion prevention systems, antivirus and Web gateways. However, we knew there was a gap in our protection against zero-day malware-based attacks. Our research showed that we needed a solution that wasn't subjected to the limitations of conventional signature-based analysis."

The company had a longstanding relationship with Damballa Inc. The CSO recalled, "Having evaluated the Damballa product, we just didn't feel confident that it gave us the level of protection that we were looking for. When we expanded our search, one name in particular kept being mentioned as a leader in the field, and that was FireEye."

He continued, "We had talked to Palo Alto Networks, but didn't feel comfortable with their approach: We are not a big believer in over-loading firewalls with tasks they were not originally designed to perform because they provide sub-par results in those areas."

We examined the Secure Web Gateway product from M86 and the IPS product from Sourcefire to round out the evaluation process and found them inadequate to address our needs. Today's Web-based threats evolve too quickly and are far too sophisticated to be detected by the approaches these companies offered."

Real World Evaluation

Having decided that a FireEye solution would potentially meet all required criteria, the company deployed a FireEye Web Malware Protection System (MPS) series 7000 appliance into their production environment for evaluation. Despite being installed inline, no discernable impact on network latency was observed. For comparison purposes, a competing Damballa product also was placed into the diverse infrastructure to examine the same traffic. The two solutions were tested side-by-side for a period of six weeks.

"We wanted to evaluate the solutions in a real world environment to see how they performed. We used fundamental evaluation criteria, such as what was detected, how quickly things were detected, and the levels of accuracy to measure effectiveness. We looked closely at which product legitimately found threats, versus generating false-positives," stated the company's CSO.

The results proved to be overwhelming. "We irrefutably saw a substantially higher caliber of results from the FireEye appliance over Damballa, and the statistics were very easy to substantiate. The FireEye solution found at least two to three times the number of legitimate threats than Damballa, even though Damballa generated far greater volumes of alerts; in the vast majority of cases, these proved to be false-positives."

Accuracy

The detection capabilities of the FireEye Web MPS appliance were so exacting that not a single false-positive was generated. The CSO commented, "This was fantastic for us. We're interested in quality, not quantity. There was a huge gap between FireEye and Damballa: The instances of threats found by the FireEye solution were real and because the FireEye appliance was deployed in-line, these attacks were blocked before entering the corporate network to compromise the hosts. Our resources are limited so having the level of detection accuracy and being able to stop the attacks at the gate meant that we didn't have to re-image the compromised system, which was a huge operational cost savings for us."

Key Components:

FireEye Web Malware Protection System

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.SP50092011