FireEye™

Case Study

A Large Multi–Program National Laboratory Stays Ahead of Next–Generation Malware By Deploying FireEye Web Malware Protection System

Summary

Company	Multi-Program National Laboratory
Industry	Government
Description	U.S. National Laboratory tasked with advancing scientific discoveries in the disciplines of energy, the environment and national security.
Challenge	Need to continually enhance effectiveness of protection against escalating global cyber threats such as advanced malware, zero-day and targeted APT attacks that target sensitive data.
Solution	Deployment of FireEye Web Malware Protection System 7000 Series appliance.
Benefits	Rapid appliance deployment facilitated dramatic increase in speed of threat detection, notification and resolution. Appliance accuracy and low false positive rates have elevated usability and productivity, without adding network or security management overhead.

Chartered with enhancing the scientific foundations of a broad spectrum of national programs for fundamental research and innovation, this multidisciplinary laboratory is at the very center of ensuring that the lives of U.S citizens can be conducted in an environment that is safe, secure and sustainable. On a daily basis, the Laboratory handles a huge portfolio of national secrets and sensitive data, making it a prized target for highly motivated and sophisticated cyber criminals. Given this role, the organization places great emphasis on providing an uncompromising and robust infrastructure to support the stringent requirements of its own team of world renowned scientists and engineers. To achieve this, the Laboratory employs seasoned security experts to ensure that all aspects of the facility remain impervious to the most insidious and malevolent of assaults.

"FireEye is stellar! We were able to clearly demonstrate what the FireEye appliance was doing for our response times and for our abilities to expediently remediate and protect the environment from advanced malware, zero–day and targeted APT attacks."

– Laboratory Lead Analyst, Cyber Defense Team

FireEye™

Case Study

Staying One Step Ahead

To guard against the ever-escalating threat of malicious attacks the Laboratory deployed a comprehensive range of enterprise-class security protection components, including firewalls, intrusion prevention systems, and anti-virus solutions. As part of its due diligence to stay ahead of the increasingly sophisticated tactics of today's criminals, such as zero-day and targeted APT attacks, the Laboratory's cyber defense team procured a FireEye Web Malware Protection System (MPS) appliance, the FireEye Web MPS 7000 Series, to complement the preventative measures that were already implemented.

The FireEye Web MPS 7000 Series is specifically designed for large networks and offers integrated inbound and outbound blocking of zero-day malware. The suite of FireEye Web MPS network security appliances prevents signature-evading threats from exploiting system weaknesses in order to exfiltrate sensitive data. Because the FireEye Web MPS appliances are typically implemented inline, the use of fast-path blocking inhibits known inbound attacks and malware callbacks. A full-fledged virtual execution engine (VX Engine) accurately detects zero-hour attacks in suspicious code and Web objects and promptly halts their progress.

FireEye Provides the Winning Edge

The FireEye team was able to pass the stringent legal, contractual and technical prerequisites for working with a sensitive National entity. Taking just one day to implement a full-scale pilot to monitor network traffic, it showed immediate positive results. Within a few hours of having the FireEye solution installed, alerts were generated by malicious code that was not being detected by any of the existing cyber defense tools. A key aspect of the implementation for the Laboratory has been the significant reduction in time between the introduction of a potential threat into the environment and the creation of a notification announcing its presence. In similar circumstances, more traditional defenses can take multiple days before generating a comparable alert.

One of the Laboratory's cyber defense team members, a fifteen-year network security industry veteran, stated, "Working with the FireEye team has been great. Its support model is outstanding. In fact, it is probably one of the most responsive vendors that I have ever worked with." Through its thorough multistage testing of suspicious code, the FireEye Web MPS appliances restrict alerts to legitimate issues. This accuracy promotes usability and productivity.

Key Component

FireEye Web Malware Protection System 7000 Series 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!

FireEye, Inc. | 1390 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com