The FireEye Malware Analysis appliance automates zero-day exploit analysis within pre-configured, full-fledged Windows® virtual machines.

FireEye Malware Analysis

Modern Malware Forensics

The FireEye Malware Analysis appliance provides automated analysis of Modern Malware and advanced persistent threats embedded in suspicious files, binary executables, and Web pages. FireEye features an advanced, multi-phase analysis engine within an enterprise-class security appliance that can automate and batch threat analysis. It provides system-level OS and application changes, such as file system, memory, and registry modifications including Mutex object creation, SSDT hooking and UAC changes. FireEye is uniquely able to provide malware forensics on zero-day exploits targeting truly unknown vulnerabilities in pre-configured, full-fledged Windows virtual machines. The Malware Analysis appliance reports on the full 360-degree view of the attack, from the initial exploit to malware execution path and callback destinations. By using pre-configured installs of Windows environments, administrators can quickly analyze suspicious samples targeting unknown OS and application vulnerabilities.

Pre-configured Environments to Analyze OS and Application Attacks

Unlike sandbox emulation environments that can be detected by hostile code, FireEye appliances feature technology that has virtualized PC hardware running full-fledged versions of Microsoft® operating systems, browsers, and other 3rd party applications. These pre-installed, instrumented Windows®-based virtual machines free administrators from time-consuming setups and baselining of virtual environments for malware analysis. In addition, beyond OS or heuristic application modeling, FireEye tests suspected files, binaries, and Web pages against a cross-matrix of browsers, applications, and operating systems to confirm malicious URLs, infectious PDFs, and malware payload executables.

At the core of each security appliance is the FireEye Malware-VM™ and Malware-Callback™ technologies, a multi-stage malware analysis capability that combines aggressive capture heuristics with deep packet inspection within instrumented virtual machines. The virtual machine analysis stage performs both static analysis to catalog information about the binary/URL as well as dynamic analysis when it executes the binary or loads the Web page. It is able to determine arbitrary code execution and when an exploit is confirmed by the virtual machine, malware forensics and outbound transmissions are captured and cataloged for use by researchers and within the Malware-Callback filters to block outbound data exfiltration attempts. With deep instrumentation, the FireEye malware analysis engine is uniquely able to trace the full execution path of zero-day and known attacks as well as providing details on custom malware communication protocols.

KEY FEATURES & BENEFITS

- Automated, batch analysis of suspicious files and URL destinations
- Confirms zero-day exploits and catalogs system-level changes and outbound transmissions
- Eliminates deployment headaches and tuning overhead
- Packet captures of malicious URL session and code execution
- Bulk submission of suspicious files via SCP or a list of URLs

MALWARE-VM & MALWARE-CALLBACK FILTERS

1. **Confirm** malicious PDF, EXE, or URL & analyze its full execution path
2. **Fingerprint** the attack and record malware callback destinations
3. **Share** malware forensics to FireEye MAX Cloud Intelligence subscribers
4. **Determine** callback transmission types to criminal servers

FireEye®

FireEye Malware Analysis

PRODUCT DATASHEET

Inbound and Outbound Threat Protection

In addition to offering a secure, encapsulated sandbox mode, FireEye offers a live, on-network mode for full malware lifecycle analysis. Today's stealth malware has circumvented conventional security technologies by utilizing an infection lifecycle in which the first malware attack is just the first step to fully own the endpoint. With a live, on-network mode, FireEye makes it is possible to witness and analyze the Modern Malware infection lifecycle that targets organizations for the purpose of cybercrime, cyber espionage, and cyber reconnaissance.

FireEye inspects not only inbound traffic for malware attacks, but also outbound traffic across multiple protocols to provide a full understanding of the intent and goals of malicious software. This integrated approach enables comprehensive threat analysis against OS, Web-based, and application threats that attack across multiple vectors to penetrate the network. Once dropper malware is confirmed, callbacks are traced to the criminal server enabling capture and download of further malware samples.

Global Network to Share Local Malware Intelligence

In order to share the benefits of the real-time malware forensics gathered by the local analysis engines, FireEye has built a worldwide Malware Analysis and Exchange (MAX) cloud to distribute the auto-generated security forensics about Modern Malware and its covert callback channels. The MAX Cloud Intelligence network is essentially an Internet cyber crime watch system to provide subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations in real-time to prevent data exfiltration, alteration, and destruction.

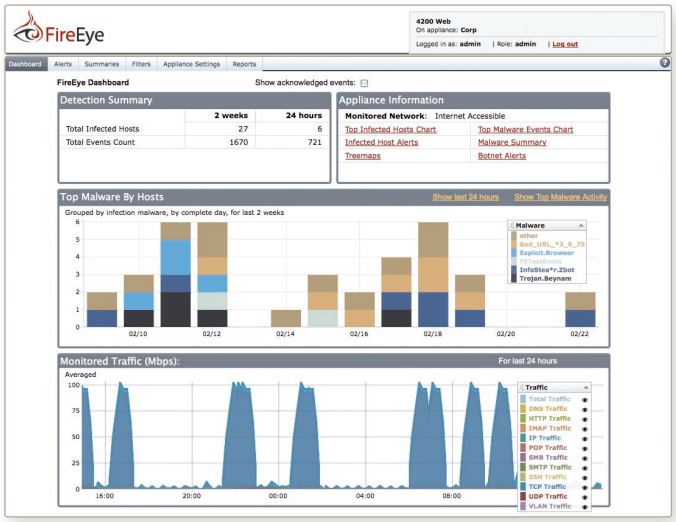
By pre-configuring virtual analysis environments and eliminating the need for tuning heuristics, it saves administrators setup time and configuration headaches. The appliance offers a clientless, network-based appliance for a quick deployment. This is an easy-to-manage, cost effective solution that analyzes Modern Malware without adding network and security management overhead.

Advancing the State-of-the-Art For Malware Analysis

FireEye has significantly advanced the state-of-the-art for malware forensics, and has now made it possible to accurately automate and analyze Modern Malware in real time. With inbound attack analysis and outbound malware transmission tracking tied into a global security exchange cloud, administrators have a clientless solution that is easy to deploy and maintain to analyze today's modern threats.

SPECIFICATIONS

Form Factor	1U Rack-Mount
Weight	23 lbs, (10.4 kg)
Dimensions	17.25"W x 21.75"D x 1.75"H (43.8 x 55.3 x 4.5 cm)
Enclosure	Fits 19-Inch Rack
Interfaces	(2) Active 10/100/1000 BASE-T Ports
AC Input Voltage	100 ~ 240 VAC Full Range
AC Input Current	4.8 - 2.0 A
Power Supply/RAID	Single / No
Frequency	50-60Hz
AC Power	400 W Max
Ambient Temp	40 °C



About FireEye, Inc.

FireEye, Inc. is the leader in malware protection systems and next generation network threat prevention solutions that safeguard valuable data and networks against Modern Malware infiltration and theft in commercial enterprises, higher education, and government institutions. The FireEye Malware Protection System is the industry's first solution that completely breaks the Modern Malware infection lifecycle by stopping inbound, zero hour, targeted attacks, outbound data exfiltration callbacks, and dynamically inoculating networks from future attacks through both local and global intelligence. FireEye finds and blocks the 90% of Modern Malware attacks that conventional defenses miss, at network speeds and near-zero false positive rates, delivering an extremely low security TCO. FireEye is based in Milpitas, Calif. and backed by Sequoia Capital, Norwest Venture Partners, JAFCO Ventures, DAG Ventures, Juniper Networks, and In-Q-Tel.

FireEye

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035
+1 (877) FIREEYE (347.3393) info@fireeye.com

www.FireEye.com