DATASHEET

FireEye Malware Analysis & Exchange Network

Web Malware & Botnet Security System

The FireEye Malware Analysis & Exchange (MAX) Network is a real-time data exchange for Web malware intelligence and botnet threat data to enhance customers' preemptive protection against the ever-changing threats. The FireEye Analysis & Control Technology (FACT) engine that powers every FireEye security appliance automatically generates dynamic malware intelligence to protect the local network against zero-day Web malware and botnet threats. By joining the MAX Network and sharing malware intelligence, participating FireEye appliances become even more efficient.

Previously confirmed Web malware, botnets, and OS attacks are no longer required to undergo the FACT engine's virtual victim machine analysis reducing alert response time. FireEye appliances can join the MAX network to receive as well as report the latest data on Web malware locations, command and control (C&C) coordinates, signatures, port/protocol abuse info, and malware propagation tactics. Customers can connect into the MAX Network by using a single CLI command on their FireEye appliances.

Global Proliferation of Web Malware & Botnets

Web malware is the primary method to build botnets, which are massive groups of compromised, remotely controlled machines used to steal customer data, perpetrate online fraud, and take intellectual property. Botnets are a widely dispersed threat making them particularly difficult to combat solely in the service provider 'cloud' or only locally within organizational networks and endpoints. Rather, a coordinated local and global security mechanism is required.

KEY FEATURES & BENEFITS

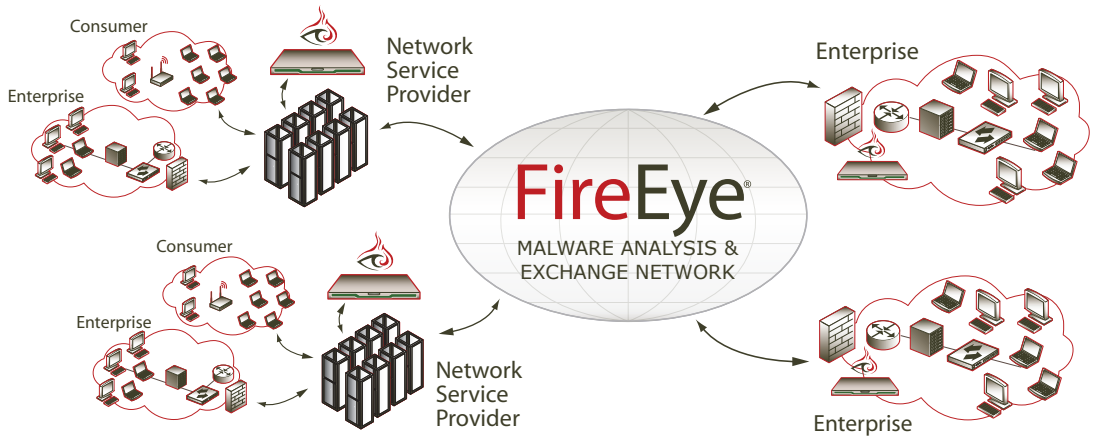
- Global malware intelligence network
- Pull-based data feed on Web malware & botnets
- Prevent malware proliferation within the network
- More efficient FACT engine detection

Using Global Intelligence to Protect Local Assets

FireEye provides anti-malware protection through FireEye appliances connecting into the FireEye MAX Network service. The FireEye MAX Network is a globally deployed discovery and analysis service offering subscribers with the most current malware intelligence to complement on-premise anti-malware FireEye security appliances. The MAX Network analyzes and disseminates:

- Web malware attack profiles (signatures, network behaviors)
- Botnet C&C fully qualified locations (IP address, protocol, ports)
- Malware call-back destinations (IP address, URL)

The FireEye MAX Network is formed from interconnected FireEye appliances deployed at enterprises and service providers around the world. These appliances receive and report malware analysis intelligence. This systematic approach prevents infections before they exploit customer data, intellectual property, and enterprise resources for cybercrime profits.



The FireEye MAX Network is a global, multi-enterprise alliance of enterprises, services providers, and research organizations fighting against Web malware and botnets. IT professionals can benefit from FireEye's global network and technology visibility to help identify and understand emerging malware threats. FireEye increases network security and restores IT control over the network by discovering and blocking call-back communications as well as derailing malware and botnet proliferation attempts.

FireEye Analysis & Control Technology (FACT)

FireEye appliances use a multi-stage analysis engine called the FireEye Analysis and Control Technology, or FACT for short. FACT detects zero-day Web malware and botnets by analyzing real-time Web and network traffic flows. When malware is confirmed within a virtual victim machine, FireEye appliances alert administrators about attack details and repel attacks via integration with existing security enforcement infrastructure.

FireEye offers a global malware intelligence exchange network that enhances local analysis to quickly and precisely identify, understand, and stop emerging Web malware and botnet threats.

The FACT Engine features:

- Multi-stage detection eliminates false positives
- Virtual victim machine analysis
- Fingerprints malware & outbound call-backs

First FireEye identifies potentially malicious code using signatures, outbound call-back coordinates, advanced heuristics, and anomaly detection to cast the widest net possible.

Next, FireEye appliances confirm malware and eliminate false positives using virtual victim machines to 'taste test' network traffic.

FireEye virtual victim machines are transparent to attackers, as the appliance is deployed out-of-band while capturing and replaying live network activity in an isolated environment. Virtual victim machines combine virtualization with patent-pending instrumentation to analyze memory, CPU, network interface, and other aspects of control flow within the virtual PC. Parallel virtual victim machines operate to analyze for zero-day Web malware and botnets and run on Microsoft® Windows® operating systems.

Finally, FireEye appliances alert administrators and can optionally share the malware intelligence data gathered via the FireEye Malware Analysis & Exchange (MAX) Network. Members receive zero-day malware signatures, call-back coordinates, and botnet intelligence for more efficient FACT engine performance.

About FireEye, Inc.

FireEye, Inc. is the leader in anti-malware and anti-botnet protection, enabling organizations to protect critical intellectual property, computing resources, and network infrastructure against Web malware and botnet infiltration. Today's most damaging attacks are perpetrated through Web malware that forms into highly organized botnets, or networks of remotely controlled, compromised machines. FireEye delivers a complete solution that is designed from the ground up to detect and protect organizations from advanced Web malware and botnets through global and local intelligence and analysis. The company is backed by Sequoia Capital, Norwest Venture Partners, JAFCO, SVB Capital, DAG Ventures, and Juniper Networks.

www.fireeye.com
+1 (877) FIREEYE (347.3393)
info@fireeye.com

FireEye, Inc.
1390 McCarthy Blvd
Milpitas, CA 95035