The FireEye MAX Network is a real-time exchange for malware threat data to maximize preemptive protection against broad and targeted attacks.

FireEye Malware Analysis & Exchange Network

Malware Protection System

The FireEye Malware Analysis & Exchange (MAX) Network is a real-time exchange for malware threat data to maximize preemptive protection against a dynamic cyber threat. Within locally deployed FireEye appliances, the FireEye Analysis & Confirmation Technology (FACT) engine automatically generates real-time malware intelligence to protect the local network against zero-day malware and advanced persistent threats. The FACT engine fingerprints zero-day malware and captures its callback IP address, communication protocol(s), port(s), and other details. Through the MAX Network, subscribers get real-time updates of global threats to their local network.

Global Network to Share Local Malware Intelligence

The FireEye MAX Network is formed from interconnected FireEye appliances deployed within customer networks, technology partner networks, and service providers around the world. FireEye has built a worldwide Malware Analysis and Exchange (MAX) network to share and efficiently distribute the auto-generated malware security intelligence, such as its covert callback channels. The MAX Network is essentially an Internet cyber crime watch system to provide subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations to prevent data exfiltration, alteration, and destruction. Real-time detections of inbound targeted attacks take place in the local FireEye network appliances. It performs outbound callback analysis based on its local callback database and further maximizes the detection of modern malware infections by subscribing to the global MAX Network.

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

FireEye has significantly advanced the state-of-the-art for malware protection, and has now made it possible to accurately stop modern malware in real time. With inbound attack detection and outbound malware transmission filtering tied into a global security exchange network, administrators have a clientless solution that is easy to deploy and maintain to provide modern protection against today's modern threats.

KEY FEATURES & BENEFITS

- Global distribution of targeted modern malware intelligence
- Pull-based data feed on Trojans, bots, and advanced persistent threats
- Prevents modern malware infiltration within the network
- Real-time updates to cut off outbound malware transmissions and stop data exfiltration

FireEye®

FireEye Malware Analysis & Exchange Network

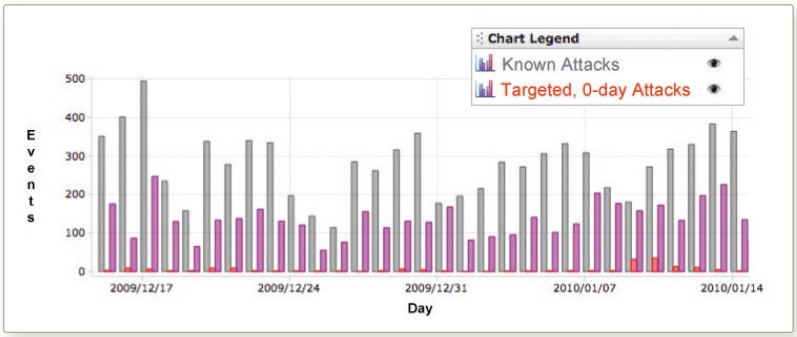
PRODUCT DATASHEET

Understanding the Malware Intelligence Service

The global MAX Network is a service providing subscribers with the latest malware intelligence produced by the FACT engine complementing on-premise anti-malware FireEye security appliances. The MAX Network provides subscribers:

- Modern malware attack profiles (MD5's of malware code, network behaviors)
- Fully qualified malware callback destinations (IP address, protocol, ports)
- Malware communication protocol characteristics

This maximizes FireEye's ability to accurately pinpoint stealth malware that have circumvented conventional security technologies and to stop the proliferation of modern malware targeted at your organization for the purpose of cybercrime, cyber espionage, and cyber reconnaissance.



MAX Network attack graph for a customer site over a one-month period

Disrupting the Modern Malware Lifecycle

FireEye inspects inbound traffic for malware attacks as well as outbound traffic across multiple protocols to identify compromised systems transmitting your data to criminal servers. This integrated approach enables the most comprehensive threat protection against modern malware that attack across multiple vectors to penetrate the network. The initial compromise of a system could be a social engineering attack like a spear-phish email with a URL or malicious PDF. Once the dropper malware is installed, it calls back out to upload stolen data and download further malware payloads. With both inbound and outbound threat protection, FireEye can protect against the entire modern malware lifecycle and goes beyond simple signature matching or rudimentary packet analysis.

With the MAX Network, FireEye security appliances address the operational concerns of IT security by providing additional accurate, real-time malware detections to help restore IT control over the network while eliminating the headaches associated with false positive analysis. The MAX Network completes the story for an easy-to-manage, cost effective solution that maximizes modern malware protection without adding network and security management overhead.

About FireEye, Inc.

FireEye, Inc. is the leader in malware protection systems, enabling organizations to stop information and resource theft due to modern malware. Based on a real-time, multi-phase analysis engine and outbound callback filtering, FireEye network security appliances find and block zero-day and targeted attacks that have circumvented conventional defenses and prevent infected systems from transmitting sensitive information out of the network. For the first time, enterprises have a cost effective, complete and integrated defense against modern malware in an easy-to-deploy network appliance. By doing so, FireEye puts organizations ahead of attackers while lowering administrative and risk management costs and empowering users to safely take advantage of the Internet, Web 2.0 and other emerging capabilities. The company is backed by Sequoia Capital, Norwest Venture Partners, JAFCO, SVB Capital, DAG Ventures, and Juniper Networks. For more information, contact (408) 321-6300 or email: info@fireeye.com. Visit us at www.FireEye.com.

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

www.FireEye.com