FireEye™ | 4200

Network Malware Control System

The FireEye 4200 network malware control system stops malicious attacks and prevents your customer data and intellectual property from being stolen. The FireEye 4200 analyzes real-time network activities, ensuring that targeted malware, botnets, zero-day attacks, and other network-borne malware do not compromise your client or server computing environments.

- **Unparalleled accuracy stopping stealthy malware and botnet infiltration**
- Prevents customer data and intellectual property theft
- Secures both Windows® client and server environments

Malware has evolved into crimeware

Crimeware is stealthy, targeted malware used for illicit purposes and financial gain. It is designed to mutate rapidly and spread quietly to circumvent traditional security technologies. Common criminals as well as organized crime are actively funding and building this next-generation malware to break into your network using known and undisclosed vulnerabilities.

Traditional security has hit the wall

Modern crimeware has relentlessly advanced in sophistication, technology, and scale rendering traditional security technologies largely obsolete. While crimeware has been on an exponential growth curve, traditional security has remained architecturally stagnant. This is all contributing to a rapid proliferation of remote control malware targeted at enterprises for the express purpose of making money.

FireEye stops targeted malware

The FireEye 4200 is unparalleled in its ability to accurately identify malicious attacks, including targeted attacks specific to a particular enterprise network. It secures against both widespread and targeted malware without relying on external updates or analysis. The FireEye 4200 is a self-sufficient system performing continuous threat analysis using its FACT engine. After definitively confirming a targeted malware attack, the FireEye 4200 can be setup to block the attack, quarantine the infected machine, and alert administrators of the incident.

Security

- FireEye Attack Confirmation Technology (FACT) engine using virtual victim machine analysis
- Windows client and server protection
- Infection-based network access control
- Network access auditing and logging

Attack Prevention

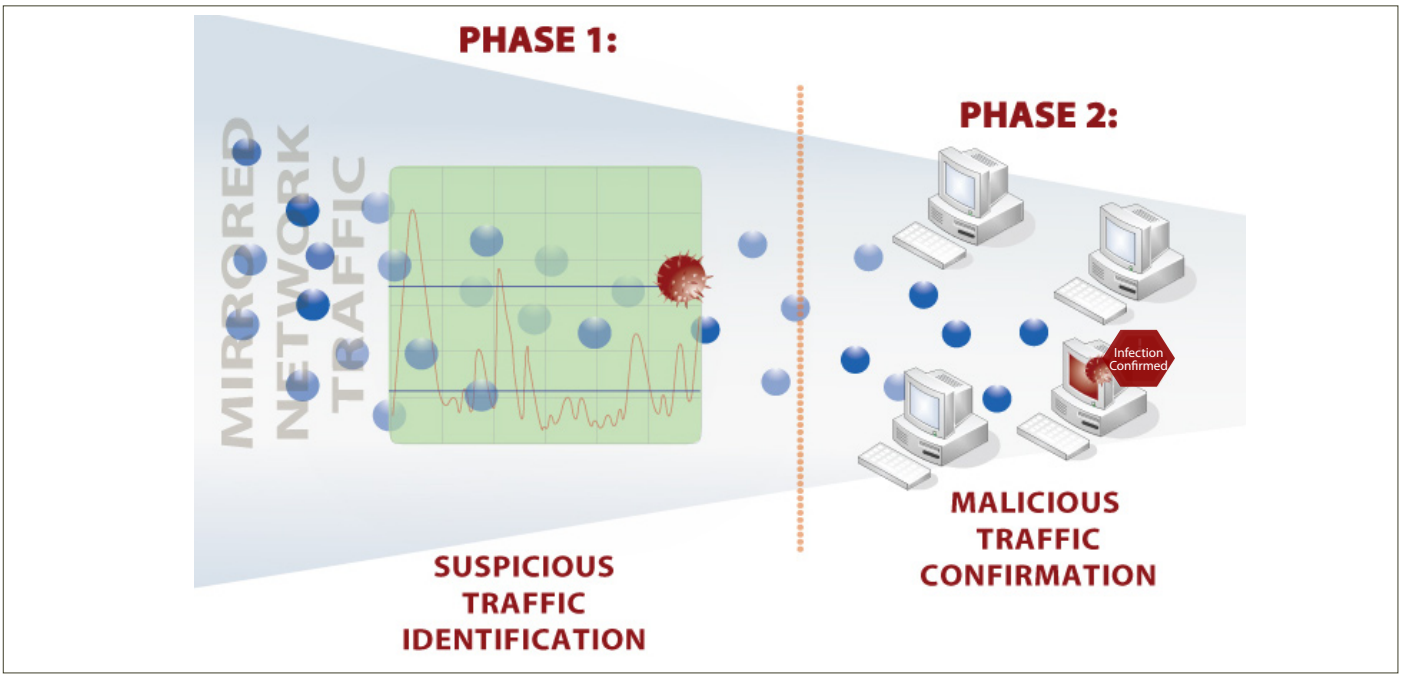
- Switch-based VLAN reassignment & ACL re-configuration
- Traffic filtering and packet-level scrubbing
- Integration with Aruba mobility controllers and other 3rd party equipment

Management

- Local or centralized management options available
- Deploys out-of-band alongside wireless controllers, VPN concentrators, and network switches

The FireEye 4200 FACT engine – Unearthing stealthy malware

The FACT engine forms the core of the FireEye 4200. The FACT engine protects against targeted malware by analyzing real-time network traffic flows as they attack virtual victim machines. When an attack is confirmed within a virtual victim machine, the FireEye 4200 instantly takes protective measures against the attack as well as records and catalogues attack details.



The FACT engine flags all suspicious network activities—then uses virtual victim machines to confirm if a targeted malware attack is underway.

Specifications	
Form factor	*1U rack-mount*
Weight	*37lbs, (16.78kg)*
Dimensions	*17.25"W x 21.75"D x 1.75"H (43.82x 55.25 x 4.45 cm)*
Enclosure	*Fits 19-inch rack*
Interfaces	*Six 10/100/1000 BASE-T ports (Copper)*
Performance rating	*1 Gbps*
AC input voltage	*90 ~ 264 VAC full range*
AC input current	*2.1 Amps*
Frequency	*50-60Hz*
AC power	*400 W max*
Ambient temperature	*27 °C*

Features	Benefits
FireEye Attack Confirmation Technology (FACT)	• Offers fully accurate network malware detection using an infinite supply of virtual victim machines in the network to scan real-time traffic flows for malicious content
Server protection pack	• Protects Windows Server environments from stealthy malware that seeks to compromise and take remote control of the server computing environment
Infection-based network access control	• Features continuous analysis of wired, wireless, and remote access machines to ensure machines infected with targeted malware, zero-day attacks, and other exploit software cannot gain a foothold in the enterprise network
Network access auditing and logging	• Provides a non-disruptive method of baselining an organization's machine posture state as well as meeting security audit and compliance requirements for safe machine network access
Crimeware prevention mechanisms	• Includes methods such as VLAN/ACL reassignment, dynamic inline packet-level scrubbing, as well as 3rd party enforcement integration with Aruba™ mobility controllers
Local or centralized management options	• Locally managed or with the FireEye CMS, administrators can set, update, and upgrade appliance configurations on an individual or group basis

Find out more

For a more information, visit us at www.fireeye.com, call 877-fireeye (347-3393), or email fireeye@fireeye.com.

About FireEye, Inc.
FireEye, Inc is the leader in malware control, providing protection for the network against crimeware and targeted attacks. Our solutions bring advanced network security together with state-of-the-art virtualization technology to safeguard company information, customer data, intellectual property, and enterprise resources - solving critical business needs without taxing IT administration.