

Go Beyond

Standalone Antivirus Technology with FireEye Endpoint Security

KEY FEATURES:



Fully integrated malware protection engine in a single FireEye agent



Multiple detection and prevention engines to address threats AV technology misses



Complete endpoint visibility to determine the attackers' identities as well as their objective, timing, location and methodology



Single interface for comprehensive visibility into threats and suspicious activities



Extensible, so new detection and prevention engines can be added without compromising performance



Broad OS support, including Windows, MacOS and Linux

Antivirus (AV) software has long been the backbone of cyber defense. But as attacks and attackers have evolved, antivirus products have left gaps in organizational defenses. To address these gaps, FireEye Endpoint Security detects and blocks whatever AV technology can catch — and what it misses. With a single agent and an integrated detection and response workflow, FireEye Endpoint Security delivers proactive and flexible protection that far exceeds AV capabilities.

FireEye Endpoint Security surpasses even next-generation AV that uses machine learning as a core detection methodology. Endpoint Security dynamically gathers intelligence and update defenses on the fly to protect against today's constantly changing threats. It integrates malware protection, intelligence, behavior analysis and exploit prevention capabilities along with detailed endpoint visibility to stop both known and unknown threats:

- Exploit Guard delivers behavior-based monitoring, detection and prevention for applications:
 - Detect and stop exploits at any stage of a threat
 - Prevent exploit and payload codes from downloading or executing
- Terminate exploited applications
- Detect and prevent application scripts and macros from running
- FireEye MVX-based sandboxing and advanced dynamic analysis enable high-fidelity, automated prevention
- Reduced threat volumes allow analysts to focus on specific, validated threats that matter with tailored responses based on contextual information
- Intelligence-led security provides visibility into all endpoints and their processes:
 - Enable powerful search, identification and analysis of potential threats
 - Proactively hunt for questionable or suspicious endpoint activity
 - Facilitate the creation of a local threat intelligence knowledge base to protect against targeted attacks

FireEye, Inc.

1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com