FireEye Fuel Technology Alliances

FireEye and Guidance Software

Integrated Detection and Response Against Today's Advanced Threats

Key Benefits

- **Sensitive data impact assessment:** Instantly recognize if sensitive data is at risk so response activities and next steps can be prioritized accordingly
- **Automated Host-based response:** Automated queries to endpoints triggered by FireEye alerts immediately validate the alert and capture ephemeral data before the attacker covers their tracks
- **Lowers total cost of ownership:** Reduce overall security spend by lowering detection time, improving digital forensics, and decreasing malware incident response time

Integration Solution

- FireEye helps block command and control traffic and kills malicious processes, while EnCase wipes offending files from endpoints related to malicious processes.
- Guidance Software EnCase Cybersecurity automates incident response to ensure high-risk devices get the immediate attention they deserve.

The FireEye platform and Guidance Software EnCase Cybersecurity integration enables a unified incident response workflow against advanced cyber attacks. The joint solution automates attack protection, endpoint infection corroboration, and forensic evidence collection.

Defending against more targeted, sophisticated, and successful threats

Today's cyber attacks are more targeted, sophisticated, and increasingly successful. These cyber attacks are successful because they are conducted across multiple threat vectors and across multiple stages, with premeditated steps to get in, to signal back out of the compromised network, and to get valuables out. Adaptive defenses and automated response capabilities are required to address these cyber attacks in a coordinated manner to protect your data effectively.

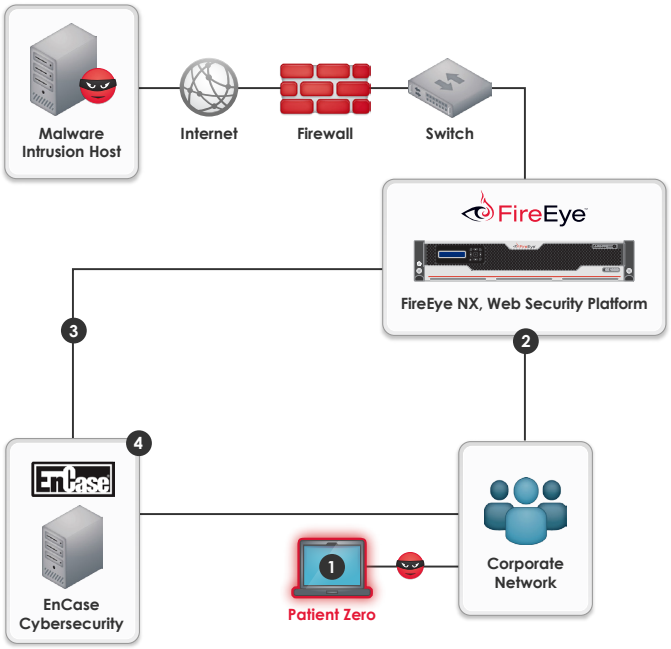
Rapidly detect and automate response to cyber attacks

FireEye and Guidance Software have integrated their security technologies to provide a comprehensive defense to rapidly detect, corroborate, and respond to cyber attacks. The joint solution addresses needs that exist both on the wire and at the endpoint. The integration is designed to automate the incident response workflow so companies can start the remediation of critical assets.

How the joint solution works

The FireEye platform continuously monitors for malware in the network and upon detection immediately shares threat intelligence about the attack with the Guidance EnCase® Cybersecurity software to trigger a variety of responses against potentially affected endpoints. The integration is based on a module enterprise service bus-based (ESB) architecture for maximum flexibility as the two products evolve for consistent and rapid implementation. The integration of the FireEye platform and the EnCase Cybersecurity software delivers a unified workflow against today's most advanced cyber attacks and provides a holistic view of the potentially affected endpoints the moment an attack is detected. In addition, the solution provides the information needed for a comprehensive scope assessment, greatly reducing the time to remediation.

FireEye Fuel Technology Alliances



1. Previously infected system plugged into corporate network and calls back to host
2. FireEye blocks callback
3. FireEye alerts EnCase Cybersecurity of the infected system and passes object information
4. EnCase Cybersecurity captures endpoint forensics (running processes, open ports, type sensitive data)

For more information, contact Alliances@FireEye.com

About FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 1,500 customers across more than 40 countries, including over 100 of the Fortune 500.

About Guidance Software

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to e-discovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing—all while maintaining the integrity of the data. There are more than 50,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by more than 60 percent of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from Law Technology News, KMWorld, Government Security News, and Law Enforcement Technology.