FireEye
SECURITY REIMAGINED

Investigation Analysis System

Accelerate incident response and investigation

DATASHEET

HIGHLIGHTS

- **Visualization:** view and share network metadata and activity through easy-to-create custom dashboards
- **Fast Answers:** centralized application-level wildcard queries and investigation across packet capture nodes
- **Powerful Search:** indexed metadata from protocols such as HTTP, SMTP, POP3, IMAP, SSL, TLS and FTP
- **Workflow Efficiency:** archive and share PCAP files with other analysts during an investigation through integrated case management
- **SIEM integration:** via RESTful API access to flow and metadata indices

Overview

As recent cyber security breach headlines reveal, the key to minimizing the impact of a security incident is early detection and swift investigation, which requires powerful forensics capabilities.

The FireEye Investigation Analysis System reveals hidden threats and accelerates incident response by adding a centralized, easy-to-use analytical interface to the FireEye Network Forensics platform, the industry's fastest, lossless network data capture and retrieval solution. When paired together, the combination of high-performance packet capture and in-depth analytics provides a powerful complement to FireEye's comprehensive threat prevention and detection capabilities.

Analysts obtain a fine-grained view of the specific network packets and session before, during, and after the attack. Being able to reconstruct and visualize the events triggering malware download or callback enables your security team to respond effectively and prevent future recurrence.

The FireEye Investigation Analysis System supports a number of configurations for single node and distributed architectures to optimize bandwidth and performance of metadata aggregation, queries, and analytics.

Capabilities

Visualization and Information Sharing

A picture is worth a thousands words -- and can save you precious time during an investigation. When visualization is paired with the FireEye Network Forensics platform, which captures packet data at speeds up to 20 Gbps, you have unprecedented ability to discover hidden threats. Create customized dashboards using drag and drop gadgets and archive and share PCAP files with other analysts using integrated case management features.

Centralized Visibility Across the Network

The FireEye Investigation Analysis System aggregates metadata across the packet captures of the Network Forensics Platform and displays insights in a centralized dashboard, eliminating blind spots and creating an end-to-end view of the kill chain. This holistic view provides context and enables you to develop a comprehensive, optimal response.

Ultrafast Queries on Massive Data Sets

When a threat is imminent, waiting hours for a query response is unacceptable. The FireEye Investigation Analysis System enables ultrafast and flexible application-level searches on large data sets and across a broad array of protocols.

Model	Total Onboard Storage	Dimensions	Power Supply / Typical Operating Load
IA 2000HN48	48 TB	2U Rack-Mount 3.5" x 17.2" x 25.5" (8.9 x 43.7 x 64.8 cm) 52 lbs (23.6 Kg)	1280W high efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto ranging

LEARN MORE

FireEye offers a comprehensive portfolio of services. For full details, contact us at services@FireEye.com or +1 855.692.2052.

WHY FIREEYE?

Expertise. Technology. Intelligence.

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you'll detect attacks as they happen. You'll understand the risk these attacks pose to your most valued assets. And you'll have the resources to quickly respond and resolve security incidents. The FireEye Global Defense Community includes more than 2,700 customers across 67 countries, including over 157 of the Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**