INVESTIGATION ANALYSIS SYSTEM (IA SERIES)

HIGHLIGHTS

- **Visualization:** View and share network metadata and activity through easy-to-create custom dashboards
- **Fast Answers:** Conduct centralized application-level wildcard queries and investigation across packet capture nodes
- **Powerful Search:** Accelerate search with indexed metadata from protocols such as HTTP, SMTP, POP3, IMAP, SSL, TLS, DNS and FTP
- **Workflow Efficiency:** Archive and share PCAP files with other analysts during an investigation through integrated case management
- **SIEM integration:** Connect to SIEM flow and metadata indices via RESTful APIs
- **IOC Aggregation and Pivoting:** Consolidate FireEye Network Security, Email Security and Endpoint Security product alerts in a single workbench and uncover potential correlations between IOCs to conduct deeper investigations.
- **Scheduled Reporting:** Automatically schedule and run reports based on time intervals or event count thresholds.
- **1-Click File Reconstruction:** Reconstruct suspect files, web pages and emails quickly and safely for further analysis and send suspect payloads to a FireEye Malware Analysis (AX series) appliance for analysis.
- **Scale for Growth:** Cluster the Investigation Analysis System appliances for greater meta data storage capacity to retain data and use a single management console to increase search capabilities across distributed Network Forensics Platform appliances and Investigation Analysis System appliances from a single management console.

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 fast, powerful forensics capabilities.

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

Analysts can review specific network packets and sessions before, during and after an attack. Being able to reconstruct and visualize the events triggering malware download or callback enables your security team to respond effectively and swiftly to prevent recurrence. They can expand visibility into attacker activity by decoding protocols typically used to laterally spread attacks in a network.

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.

FireEye

Capabilities

Single Investigative Workbench: Accelerate the investigation process by quickly identifying the alerts that require deep investigation and narrow your focus with centralized networking forensics investigation from a single workbench. The faster you answer simple questions about a threat, the more you'll protect your organization, customers and your brand: How did the attackers get in? What did they do when they got in? Where did they go? How long have they been here? What, specifically, did they take?

Reporting: Set the FireEye Investigation Analysis System to generate reports based on time or more sophisticated count-based thresholds. Use the reporting functionality to help visualize anomalous activity within the network and monitor network events.

Visualization and Information Sharing: Save precious time during an investigation and discover hidden threats. Pair visualization with the FireEye Network Forensics platform, which captures packet data at speeds up to 20 Gbps for unprecedented detection capabilities. Create customized dashboards using drag-and-drop gadgets and archive and share PCAP files with other analysts using integrated case management features.

Intelligence Integration: Automatically download IOCs from the FireEye iSIGHT Intelligence network and automate the process of analyzing historical metadata for signs of IOCs within your network. Conduct historical searches of threats prior to having any knowledge of these new threats.

Centralized Visibility Across the Network: Aggregate metadata across the packet captures from FireEye Network Forensics and display insights in a central dashboard, eliminating blind spots and creating an end-to-end view of the kill chain. Use this holistic view to provide context and develop a comprehensive, optimal response.

Ultrafast Queries on Massive Data Sets: Cut hours away from your wait times on query responses to address threats quickly. Enable 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 1000HN16	16 TB	1U Rack-Mount 1.7" x 17.2" x 25.6" (4.3 x 43.7 x 65.0 cm) 46 lbs (20.9Kg)	650W high-efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto-ranging 230-280w typical
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

For more information on FireEye, visit:
www.FireEye.com

ABOUT FIREEYE, INC.

FireEye is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

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

www.FireEye.com

FireEye