DATA SHEET

FireEye

Network Forensics

Minimize impact of network attacks with high-performance packet capture and investigation analysis

Organizations need early detection and swift investigation of incidents to determine scope and impact, effectively contain threats and re-secure their network.

The FireEye Network Forensics solution pairs the industry's fastest lossless network data capture and retrieval solution with centralized analysis and visualization. It accelerates the network forensics process with a single workbench that simplifies investigations and reduces risk.

FireEye Network Forensics allows you to identify and resolve security incidents faster by capturing and indexing full packets at extremely rapid speeds. With Network Forensics, you can detect a broad array of security incidents, improve the quality of your response and precisely quantify the impact of each incident.

As part of the FireEye Network Forensics solution, the Investigation Analysis system reveals hidden threats and accelerates incident response by adding a centralized workbench with an easy-to-use analytical interface.

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.

This unique combination of high-performance packet capture and in-depth analytics helps quickly recognize and monitor every element of an attack.

Figure 1. FireEye Network Forensics appliances for packet capture and analysis.

Packet Capture Highlights

- **High-Performance:** Continuous, lossless packet capture with time stamping at recording speeds up to 20 Gbps
- **High-Fidelity:** Real-time indexing of all captured packets using time stamp and connection attributes. Export of flow index and connection metadata in JSON format. Flow index can be converted to NetFlow v9, IPFIX and Silk Tools data formats
- **Fast Results:** Ultrafast search and retrieval of target connections and packets using patented indexing architecture
- **Rich Context:** Web-based, drill-down GUI for search and inspection of packets, connections and sessions
- **Extensive Visibility:** Session decoder support to view and search web, email, FTP, DNS, chat, SSL connection details and file attachments
- **Intelligent Capture:** Selective filtering of captured traffic to eliminate streaming video, large file transfers, encrypted payloads, etc.
- **Improved Efficiencies:** Automated processes to identify data theft, using proprietary algorithms to diagnose potentially anomalous network behavior

Table 1. Available packet capture appliances.

Model	Capture Port Configuration	Management Ports	Max Record Speed	Total Onboard Storage	Dimensions	Power Supply / Typical Operating Load
PX 1004S-6	4 x 1GbE	2 x 1GbE	500 Mbps	6 TB	1U 17.2" (437mm) x 19.7" (500mm) x 1.7" (44mm) 18 lbs (8.2 kg)	AC, Fixed AC 100 ~ 240 V @ 50 ~ 60 Hz, IEC60320-C14 inlet
PX 2060ESS-96	4 x 10GE SFP+	2 x 1GbE	2 Gbps	96 TB, expandable SAS attached storage	2U 17.24" (438mm) x 24.41" (620mm) x 3.48" (88.4mm) x 57.3 lbs (26.0 kg)	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU
PX 2060ESS-120	4 x 10GE SFP+	2 x 1GbE	7.5 Gbps	120 TB, expandable SAS attached storage	2U 17.24" (438mm) x 24.41" (620mm) x 3.48" (88.4mm) x 57.3 lbs (26.0 kg)	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU
PX 1004EXT-4G	4 x 1 Gbps, 10/100/1000 BaseT, SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	4 Gbps	No onboard storage. Fiber HBA to external SAN storage	1U Rack-Mount 1.7" (4.3cm) x 17.2" (43.7cm) x 25.6" (65.0cm) 46 lbs (20.9 kg)	650W high-efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto-ranging 230-280W typical
PX 1040EXT-20G	4 x 1 Gbps	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	20 Gbps	No onboard storage. Fiber HBA to external SAN storage	1U Rack-Mount 1.7" (4.3cm) x 17.2" (43.7cm) x 25.6" (65.0cm) 46 lbs (20.9 kg)	650W high-efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto-ranging 230-280W typical
PX 4000SX440	n/a	n/a	n/a	440TB Raw Storage shelf	17.2" (437mm) x 27.5" (698mm) x 7" (178mm) 76 lbs (34 kg)	1280W high-efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto ranging

Note: All performance values vary depending on the system configuration and traffic profile being processed.

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

Investigation Analysis Highlights

- **Visualization:** View and share network metadata and activity through easy-to-create custom dashboards
- **Fast Answers:** Conduct centralized application-level keyword, regex, and wildcard queries across all alerts, captured flow and metadata
- **Agile Interface:** Immediate pivot and download of individual or bulk PCAP data for sessions of interest
- **Powerful Search:** Accelerate search with indexed metadata from protocols such as HTTP, SMTP, POP3, IMAP, SSL, TLS, DNS and FTP
- **IOC Aggregation:** Consolidate FireEye Network Security, Email Security and Endpoint Security product alerts along with all network metadata in a single workbench with immediate "one click" pivot to session data from alerts
- **Retrospective Threat Hunting:** "Back-in-time" IOC threat analysis via integration of iSIGHT, STIX, and OpenIOC feeds with automated IA search function. Automatically be alerted to IOCs present in network days or weeks earlier
- **One-Click File Reconstruction:** Reconstruct suspect files, web pages and emails quickly and safely for further analysis

Table 2. Available Investigation Analysis appliances.

Model	Total Onboard Storage	Dimensions	Power Supply / Typical Operating Load
IA 1000 DIR	6 TB	17.2"(437mm) x 19.7"(500mm) x 1.7"(44mm)	AC, Fixed AC 100 ~ 240 V @ 50 ~ 60 Hz, IEC60320-C14 inlet
IA 2100-48	48 TB	17.2"(437mm) x 19.7"(500mm) x 1.7"(44mm)	Redundant (1+1) 800 watt, 100 - 240 VAC 10.5 – 4.0A, 50-60 Hz IEC60320-C14 inlet, FRU

To learn more about FireEye, visit: **www.FireEye.com**

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

About FireEye, Inc.
FireEye is the intelligence-led security company. 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®