FireEye
SECURITY REIMAGINED

Network Forensics Platform

Accelerate actionable intelligence and facilitate rapid incident response

DATASHEET

SECURITY REIMAGINED

HIGHLIGHTS

- Continuous, lossless packet capture with nanosecond time stamping at recording speeds up to 20 Gbps
- Real-time indexing of all captured packets using time stamp and connection attributes. Export of flow index in NetFlow v5, v9, and IPFIX formats for use with other flow analysis tools
- Ultrafast search and retrieval of target connections and packets using patent-pending indexing architecture
- Web-based, drill-down GUI for search and inspection of packets, connections, and sessions
- Session decoder support for viewing and searching Web, email, FTP, DNS, chat, SSL connection details, and file attachments
- Packet payload search using regular expressions
- Industry-standard data storage and export in PCAP format, which can be stored with flexible storage options: on the appliance, SASattached, or SAN-attached storage
- Accelerate the investigative process by using Event Based Capture to identify suspicious sessions that should be the focus for deeper investigations.

Overview

Well-maintained perimeter defenses are a key part of any security strategy. Organizations increasingly recognize that they must also complement their perimeter defenses with strong forensics capabilities to investigate and analyze attacks. When attacked, an enterprise needs to be able to rapidly investigate and determine the scope and impact of the incident so they can effectively contain the threat and secure their network.

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

The Network Forensics Platform provides a powerful complement to the FireEye comprehensive threat prevention capabilities. In addition to receiving precise alerts and correlated threat information, analysts can also get a fine-grained view of the specific packets and sessions before, during, and after the attack to confirm what may have triggered a malware download or callback, to respond rapidly and effectively, and to apply this information to enhancing future protective strategies.

Accelerate kill chain reconstruction and impact quantification

By allowing FireEye users to quickly locate and decode traffic and sessions before, during, and after a security event, the Network Forensics Platform provides greater visibility into activity around the event, further enhancing visibility that can be crucial for rapid incident response investigations.

Ultrafast access to historical network data is a necessity for security personnel in reducing mean time to resolution, as well as answering the key questions: how long has the breach been present, what data may have already left the network, and how many other hosts may already have been compromised?

Ultrafast packet capture, indexing, and search

The Network Forensics Platform ensures continuous, lossless packet capture with nanosecond time stamping at recording speeds up to 20 Gbps. Real-time indexing of all captured packets with nanosecond time stamps and connection attributes provides data for immediate forensics.

Industry-standard data storage and export

All packets are stored in standard PCAP format to enable flexibility to an analytics platform of choice.

Integrated workflow with FireEye Threat Prevention Platform

The integration with the FireEye platforms provides deeper insight into network traffic and activities through simple drill-down access to captured, indexed, and stored connection and packet information on the largest and busiest 10 Gbps networks. By allowing FireEye users to quickly locate and decode traffic and sessions before, during, and after a security event, the Network Forensics Platform provides greater visibility into activity around the event, further enhancing visibility that can be crucial for rapid incident response investigations.

Highlight suspicious sessions

Accelerate the investigative process and correlate events that have occurred over time by creating customizable rules to flag suspicious session data, enabling a starting point for deeper investigations and to ensure longstanding retention. Investigations tied to a given event can be managed as a single case.

	Capture Port Configuration	Management Ports	Max Record Speed	Total Onboard Storage	Dimensions	Power Supply / Typical Operating Load
PX 004S	4 x 1 Gbps SFP	2 x 10/100/1000 BASE-T	500Mbps	2TB	1.7" x 16.8" x 14" (4.3 x 42.67 x 35.56 cm) 11 lbs (5 kg)	200W Low Noise AC power 100-240V, 60-50 Hz auto-ranging
PX 1004ESS-16	4 x 1 Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	1.5 Gbps	16 TB, expandable SAS attached storage	1U Rack-Mount 1.7" x 17.2" x 25.6" (4.3 x 43.7 x 65.0 cm) 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 1020ESS-16	2 x 10 Gbps, SFP+	2 x 10/100/1000 BASE-T 2 x 10/100/1000/ 10G BASE-T	1.5 Gbps	16 TB, expandable SAS attached storage		
PX 2004ESS-24	4 x 1 Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000/ 10G BASE-T	4 Gbps	24 TB, expandable SAS attached storage	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
PX 2004ESS-48	4 x 1 Gbps, 10/100/1000BaseT, SFP	2 x 10/100/1000/ 10G BASE-T	4 Gbps	48 TB, expandable SAS attached storage		
PX 2020ESS-24	2 x 10 Gbps, SFP+	2 x 10/100/1000/ 10G BASE-T	5 Gbps, upgradeable to 20 Gbps	24 TB, expandable SAS attached storage		
PX 2020ESS-48	2 x 10 Gbps, SFP+	2 x 10/100/1000/ 10G BASE-T	5 Gbps, upgradeable to 20 Gbps	48 TB, expandable SAS attached storage		
PX 2040ESS-48	4 x 10 Gbps, SFP+	2 x 10/100/1000/ 10G BASE-T	5 Gbps, upgradeable to 20 Gbps	48 TB, expandable SAS attached storage		
PX 1004EXT-4G	4 x 1 Gbps, 10/100/1000BaseT, 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" x 17.2" x 25.6" (4.3 x 43.7 x 65.0 cm) 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 1020EXT-10G	2 x 10 Gbps, SFP+	2 x 10/100/1000 BASE-T 2 x 10/100/1000/ 10G BASE-T	10 Gbps			
PX 1020EXT-20G	2 x 10 Gbps, SFP+	2 x 10/100/1000 BASE-T 2 x 10/100/1000/ 10G BASE-T	20 Gbps			
PX 1040EXT-20G	4 x 10 Gbps, SFP+	2 x 10/100/1000 BASE-T 2 x 10/100/1000/ 10G BASE-T	20 Gbps			
PX 2000SX-24	n/a	n/a	n/a	24 TB storage shelf expansion for ESS models	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)	500W high-efficiency (1+1) redundant AC power 100-240 VAC, 60-50 Hz auto ranging
PX 2000SX-48	n/a	n/a	n/a	48 TB storage shelf expansion for ESS models		
PX 4000SX-264	n/a	n/a	n/a	264 TB storage shelf expansion for ESS models	4U Rack-Mount 7" x 17.2" x 27.5" (17.8 x 43.7 x 64.8 cm) 75 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.

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**

© 2015 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. — DS.NFP.EN-US.102015