Trellix

DATA SHEET

Trellix Network Forensics

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

Trellix Network Forensics 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.

Your organization needs early incident detection and swift investigation to determine scope and impact, effectively contain threats, and resecure your network.

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

Part of Network Forensics, investigation analysis appliances reveal hidden threats and accelerate 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. By reconstructing and visualizing the events triggering malware download or callback, your security team can respond effectively and swiftly to prevent recurrence. They can also 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 your organization quickly recognize and monitor every element of an attack.

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 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, and more

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 1GE	1 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) 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) 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

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

Table 2. Available next-generation packet capture appliances

Model	Capture port configuration	Management ports	Max record speed	Total onboard storage	Dimensions	Power supply/typical operating load
7600PX-HW	2p*40G FPGAQSFP Optional 8x10G fiber port	2p*10GT+2p*SFP	10-20 Gbps	192 TB raw storage, 122 TB for PCAP storage Expandable SAS attached storage	17.2" (437mm) x 25.5" (437mm) x 3.5" (89mm) 81.2 lbs (36.8 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
7620PX-HW	2p*40G FPGAQSFP Optional 8x10G fiber port	2 x 1GbE	14-20 Gbps	No onboard storage; Fibre HBA to external SAN storage	17.2" (437mm) x 25.5" (437mm) x 3.5" (89mm) 63 lbs (28.6 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
5000SX-HW	-	-	-	704 TB raw storage, 465 TB for PCAP storage	17.2" (437mm) x 25.5" (437mm) x 7" (89mm) 78 lbs (35.4 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
5600PX-HW	4p*10G FPGA-QSFP ports	2p 10/100/1000 BASE-T ports	6-10 Gbps	120TB raw storage, 80 TB for PCAP storage	17.2" (437mm) x 25.5" (647mm) x 3.5" (89mm) 42 lbs (19.05 kg)	Redundant (1+1), FRU, 920W with Input 100-240V, 11-4.4A, 50-60 Hz IEC60320-C14 inlet

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

- 7600PX and 7620PX can support continuous packet capture rates up to 20 Gbps with no metadata analysis (with at least one storage array attached).
- 7600PX and 7620PX can support continuous packet capture rates up to 16 Gbps with metadata analysis (with at least one storage array attached).
- 7600PX and 7620PX can support continuous packet capture rates up to 14 Gbps with metadata analysis and with up to 10K Suricata rules loaded (with at least one storage array attached).
- 7600PX supports continuous packet capture rates up to 10 Gbps with metadata analysis (with no storage array attached).
- 5600PX can support continuous packet capture rates up to 10 Gbps with metadata analysis (with at least one storage array attached).
- 5600PX supports continuous packet capture rates up to 6 Gbps with metadata analysis (with no storage array attached).

Table 3. Compliance for available next-generation packet capture appliances

Models	Regulatory compliance EMC	Regulatory compliance safety	Environmental compliance
7600PX-HW 7620PX-HW	FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CISPR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368 EN 62368 BS EN 62368	RoHS, REACH, Conflict Minerals
5600PX-HW	"FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CISPR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35"	"CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368"	"RoHS REACH"

Table 4. Virtual packet capture appliances (support for Azure, ESXi, KVM, and AMI)

Virtual PX appliance specifications	Minimum requirements	Trellix recommended requirements	Performance requirements
CPU cores	4 CPU Cores	8 CPU Cores	16 CPU Cores
Memory	16 GB RAM	32 GB RAM	64 GB RAM
Network interface controllers (NIC)	A dedicated NIC for management A dedicated NIC for packet capture	A dedicated NIC for management A dedicated NIC for packet capture	A dedicated NIC for management A dedicated NIC for packet capture
Hard drives	80 GB hard drive for the Linux OS 200 GB hard drive for captured data	80 GB hard drive for the Linux OS 200 GB hard drive for captured data	80 GB hard drive for the Linux OS 200 GB hard drive for captured data
Approximate capture rates	25 Mbps (with a limited number of rules)	100 Mbps (with standard device limitations)	1,000 Mbps (with standard device limitations)

Investigation analysis highlights

Trellix investigation analysis appliances support several configurations for single node and distributed architectures to optimize bandwidth and performance of metadata aggregation, queries, and analytics.

Vizualization: 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: Pivot and download individual or bulk PCAP data immediately 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 Trellix 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: Integrate Trellix Threat Intelligence, STIX, and OpenIOC feeds with an automated IA search function for back-in-time IOC threat analysis, and get alerted automatically to IOCs present in your network days or weeks earlier

One-click file reconstruction: Reconstruct suspect files, web pages, and emails quickly and safely for further analysis

Table 6. Available next-generation investigation analysis appliances

Model	Total onboard storage	Dimensions	Power supply/typical operating load
2600IA-HW*	120 TB, 82 TB for metadata storage	17.2" (437mm) x 25.5" (437mm) x 3.5" (89mm) 79.4 lbs (36 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH

Note: Ingestion rate is 50K events per second.
*Can be configured as a director node or as a data node

Table 7. Compliance for available next-generation investigation analysis appliances

Model	Regulatory compliance EMC	Regulatory compliance safety	Environmental compliance
2600IA-HW	FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CIS-PR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368 EN 62368 BS EN 62368	RoHS REACH Conflict Minerals

Table 8. Virtual investigation analysis appliances (support for Azure, ESXi, KVM, and AMI)

	Minimum requirements	Virtual IA director	Virtual IA data node
CPU cores	16	16	64
Memory (RAM)	32 GB	64 GB	256 GB
Network interface controllers (NICs)	1	1	2 (For multibox clustering)
Hard drives	2.5 TB (IO throughput > 100 MB/s)	1 TB	48 TB (IO throughput) > 1GB/sec
Performance	4–5k/sec	n/a	25–30k/sec (single box cluster)
Retention	7 days	n/a	30 days

To learn more about Trellix, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Visit Trellix.com to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.