



Network Forensics

Die effektive Erfassung und Analyse von Datenpaketen mindert die Auswirkungen von Angriffen auf Ihr Netzwerk.

Wir empfehlen Unternehmen, sich auf die frühzeitige Erkennung und rasche Untersuchung von Vorfällen zu konzentrieren. Dabei sollte es darum gehen, das Ausmaß und die Auswirkungen zu ermitteln, Bedrohungen wirksam abzuwehren und ihr Netzwerk wieder sicher zu machen.

FireEye Network Forensics kombiniert das branchenweit schnellste verlustfreie Tool für die Erfassung und Abfrage von Netzwerkdaten mit zentralisierten Analyse- und Visualisierungsfunktionen. Die einheitliche Workbench der Lösung vereinfacht forensische Untersuchungen, beschleunigt den Analyseprozess und mindert dadurch das Risiko.

Mit FireEye Network Forensics können Sie vollständige Pakete in hoher Geschwindigkeit erfassen und indexieren, um Sicherheitsvorfälle noch rascher aufzudecken und abzuwehren. Außerdem gibt Ihnen die Lösung die Möglichkeit, eine Vielzahl von Sicherheitsverletzungen zu erkennen, Ihre Abwehrmaßnahmen zu optimieren und die Auswirkungen jedes Vorfalls genau zu bestimmen.

Darüber hinaus umfasst FireEye Network Forensics das Investigation Analysis System, das verborgene Bedrohungen sichtbar macht und mit seiner anwenderfreundlichen Analyseoberfläche beschleunigte Incident-Response-Prozesse ermöglicht.

Analysten erhalten vor, bei und nach einem Angriff genaue Informationen über einzelne Netzwerkpakete und -sitzungen. Mittels einer Rekonstruktion und Visualisierung der Ereignisse, die den Malware-Download bzw. Callback ausgelöst haben, kann Ihr Sicherheitsteam schnell und effektiv reagieren und Wiederholungen verhindern. Ihre Experten können Protokolle decodieren, die üblicherweise

für die Ausbreitung im Netzwerk genutzt werden, und sich so einen besseren Einblick in die Aktivitäten der Hacker verschaffen.

Mit dieser einzigartigen Kombination aus leistungsstarken Tools für die verlustfreie Erfassung und detaillierte Analyse von Datenpaketen können Analysten alle Komponenten eines Angriffs rasch erkennen und verfolgen.



Abbildung 1: FireEye Network Forensics: Appliances für die Erfassung und Analyse von Datenpaketen

Vorteile der Paketerfassung und -analyse mit FireEye

- **Starke Leistung:** Lückenlose, verlustfreie Paketerfassung mit Zeitstempelung und Aufzeichnungsgeschwindigkeiten von bis zu 20 Gbit/s
- **Hohe Genauigkeit:** Echtzeit-Indexierung aller erfassten Pakete mit Zeitstempeln und Verbindungsattributen. Export der indexierten Datenströme und der Verbindungs-Metadaten im JSON-Format. Konvertierung der indexierten Datenströme in andere Datenformate (NetFlow v9, IPFIX und Silk Tools) möglich
- **Enorme Geschwindigkeit:** Extrem schnelles Auffinden und Abrufen von Zielverbindungen und Paketen mithilfe der patentierten Indexierungsarchitektur
- **Detaillierte Kontextinformationen:** Grafische Weboberfläche mit Drilldown-Funktion, mit denen sich Pakete, Verbindungen und Sitzungen suchen und untersuchen lassen
- **Umfassende Transparenz:** Dank der Decodierung von Sitzungen können Detailinformationen zu Web-, Mail-, FTP-, DNS-, Chat- und SSL-Verbindungen sowie Dateianhängen angezeigt und durchsucht werden.
- **Intelligente Filter:** Selektive Filterung des erfassten Datenverkehrs zum Ausschluss von Videostreams, großen Dateitransfers, verschlüsselten Paketen usw.
- **Verbesserte Effizienz:** Automatische Erkennung von Datendiebstahl mithilfe proprietärer Algorithmen zur Aufdeckung potenziell anomalen Netzwerkverhaltens

Tabelle 1: Verfügbare Appliances für die Paketerfassung

Modell	Erfassungsports	Managementports	Maximale Aufzeichnungsgeschwindigkeit	Integrierter Speicher	Maße	Stromversorgung/typische Betriebslast
PX 1004S-6	4 x 1 GbE	2 x 1 GbE	500 Mbit/s	6 TB	1 HE 437 x 500 x 44 mm 8,2 kg	100–240 V Wechselstrom; 50–60 Hz; Eingang nach IEC 60320; nicht austauschbar
PX 2060ESS-96	4 x 10 GigE SFP+	2 x 1 GbE	2 Gbit/s	96 TB, erweiterbarer SAS-Speicher	2 HE 438 x 620 x 88,4 mm; 26 kg	Redundant (1+1) 800 W bei 100–240 V; 10,5–4,0 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU
PX 2060ESS-120	4 x 10 GigE SFP+	2 x 1 GbE	7,5 Gbit/s	120 TB, erweiterbarer SAS-Speicher	2 HE 438 x 620 x 88,4 mm; 26 kg	Redundant (1+1) 800 W bei 100–240 V; 10,5–4,0 A; 50–60 Hz; Eingang nach IEC 60320-C14; FRU
PX 1004EXT-4G	4 x 1 Gbit/s, 10/100/1000 BASE-T, SFP	2 x 10/100/1000 BASE-T, 2 x 10/100/1000 /10G BASE-T	4 Gbit/s	Kein integrierter Speicher. Glasfaser-Host- Bus-Adapter zum Anschließen externer SAN- Speicher	Rackmontage (1 HE); 43 x 437 x 650 mm; 20,9 kg	Hocheffizientes 650-W-Netzteil mit 1+1-Redundanz, 100–240 V AC, 60–50 Hz, automatischer Spannungserkennung, 230–280 W im Normalbetrieb
PX 1040EXT-20G	4 x 1 Gbit/s	2 x 10/100/1000 BASE-T, 2 x 10/100/1000 /10G BASE-T	20 Gbit/s	Kein integrierter Speicher. Glasfaser-Host- Bus-Adapter zum Anschließen externer SAN- Speicher	Rackmontage (1 HE); 43 x 437 x 650 mm; 20,9 kg	Hocheffizientes 650-W-Netzteil mit 1+1-Redundanz, 100–240 V AC, 60–50 Hz, automatischer Spannungserkennung, 230–280 W im Normalbetrieb
PX 4000SX440	-	-	-	440 TB Rohspeicher	437 x 698 x 178 mm; 34 kg	Hocheffizientes 1280-W-Netzteil mit 1+1-Redundanz, 100–240 V AC, 60–50 Hz, automatischer Spannungserkennung

Hinweis: Die tatsächlichen Leistungswerte sind von der Systemkonfiguration und dem verarbeiteten Datenverkehr abhängig.

Das Investigation Analysis System von FireEye unterstützt verschiedene Konfigurationen mit einzelnen Appliances oder verteilten Architekturen, um die Bandbreite und Performance bei der Aggregation von Metadaten sowie bei Abfragen und Analysen spürbar zu verbessern.



Investigation Analysis System – die Vorteile im Überblick

- **Visualisierung:** Mithilfe einfach zu erstellender, benutzerdefinierter Dashboards können Sie Metadaten und Aktivitäten aus dem Netzwerk anzeigen und für andere Benutzer freigeben.
- **Schnelle Antworten:** Sie können von einer zentralen Konsole aus alle Warnmeldungen, erfassten Datenströme und Metadaten auf Anwendungsebene nach bestimmten Schlüsselwörtern oder regulären Ausdrücken durchsuchen und dabei auch Platzhalter verwenden.
- **Flexible Oberfläche:** Gehen Sie nahtlos von der Suche zur Analyse über und laden Sie PCAP-Daten einzeln oder gebündelt herunter.
- **Starke Suchperformance:** Die Verwendung indexierter Metadaten aus Protokollen wie HTTP, SMTP, POP3, IMAP, SSL,TLS und FTP beschleunigt die Suche beträchtlich.
- **Aggregation von Gefahrenindikatoren:** Konsolidieren Sie die Warnmeldungen von FireEye Network Security, Email Security und Endpoint Security sowie sämtliche Netzwerk-Metadaten in einer zentralen Workbench, wo Sie mit einem Klick zwischen Sitzungsdaten und Warnmeldungen hin- und herwechseln können.
- **Rückwirkende Spurensuche:** Integrierte iSIGHT-, STIX- und OpenIOC-Feeds sowie eine automatisierte IA-Suchfunktion unterstützen die rückwirkende Suche nach Gefahrenindikatoren. Auf diese Weise werden Sie automatisch über Gefahrenindikatoren informiert, die bereits seit Tagen oder Wochen nachweisbar sind.
- **Rekonstruktion von Dateien per Mausclick:** Verdächtige Dateien, Websites und E-Mails können für die gründliche Untersuchung schnell und sicher rekonstruiert werden.

Tabelle 2: Verfügbare Appliances für Investigation Analysis

Modell	Integrierter Speicher	Maße	Stromversorgung/typische Betriebslast
IA 1000 DIR	6 TB	437 x 500 x 44 mm	100-240 V Wechselstrom; 50-60 Hz; Eingang nach IEC 60320; nicht austauschbar
IA 2100-48	48 TB	437 x 500 x 44 mm	Redundant (1+1) 800 W bei 100-240 V; 10,5-4,0 A; 50-60 Hz; Eingang nach IEC 60320-C14; FRU

Mehr Informationen zu FireEye erhalten Sie unter: www.FireEye.de

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035, USA
 +1 408 321 6300/+1 877-FIREEYE (347 3393)/
 info@FireEye.com

© 2018 FireEye, Inc. Alle Rechte vorbehalten.
 FireEye ist eine eingetragene Marke von FireEye, Inc. Alle anderen Marken, Produkte oder Servicenamen sind Marken oder Dienstleistungsmarken der jeweiligen Eigentümer.
 NF-EXT-DS-DE-DE-000026-02

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye fungiert als nahtlose und skalierbare Erweiterung der Sicherheitsumgebung seiner Kunden und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz unterstützt FireEye Kundenunternehmen bei der Vorbereitung auf die Erkennung und Abwehr von Cyberangriffen.

