SCHEDA TECNICA

# Network Forensics

## Riduci al minimo l'impatto degli attacchi di rete con l'acquisizione di pacchetti ad alte prestazioni e un'analisi delle indagini

Le organizzazioni hanno bisogno di un rilevamento tempestivo e di un'analisi rapida degli incidenti per determinarne la portata e l'impatto, contenere efficacemente le minacce e tornare a proteggere la propria rete.

La soluzione FireEye Network Forensics abbina la soluzione per l'acquisizione e il recupero dei dati di rete più rapida del settore con analisi e visualizzazioni centralizzate. Accelera il processo forense della rete con un unico workbench che semplifica le indagini e riduce i rischi.

FireEye Network Forensics consente di identificare e risolvere i problemi di sicurezza più velocemente tramite l'acquisizione e l'indicizzazione dei pacchetti completi a velocità estremamente rapide. Con Network Forensics è possibile rilevare una vasta gamma di incidenti di sicurezza, migliorare la qualità della risposta e quantificare con precisione l'impatto di ogni incidente.

In quanto parte della soluzione FireEye Network Forensics, le appliance Investigation Analysis individuano le minacce nascoste e velocizzano la reazione agli incidenti aggiungendo un workbench centralizzato con un'interfaccia analitica di facile utilizzo.

Gli analisti possono rivedere sessioni e pacchetti di rete specifici prima, durante e dopo l'attacco. La possibilità di ricostruire e visualizzare gli eventi che attivano il download di malware o callback permettono al team di sicurezza di reagire in modo efficace e repentino per evitare che si ripetano. Possono quindi ampliare la visibilità sull'attività dell'aggressore decodificando i protocolli tipicamente utilizzati per diffondere lateralmente gli attacchi in una rete.

Questa combinazione unica di acquisizione di pacchetti ad alte prestazioni e analisi approfondita consente di riconoscere rapidamente e monitorare ogni elemento di un attacco.

**Figura 1.** Le appliance FireEye Network Forensics per l'acquisizione e l'analisi dei pacchetti.

## Punti salienti dei pacchetti acquisiti

- **Alte prestazioni:** acquisizione continua lossless dei pacchetti con timestamp in nanosecondi fino a una velocità di registrazione pari a 20 Gbit
- **Alta affidabilità:** indicizzazione in tempo reale di tutti i pacchetti acquisiti con timestamp e attributi di connessione. esportazione di indice di flusso e metadati di connessione in formato JSON. l'indice di flusso può essere convertito in formati per NetFlow v9, IPFIX e Silk Tools
- **Risultati veloci:** ricerca e recupero ultraveloci delle connessioni e dei pacchetti presi di mira usando un'architettura di indicizzazione in attesa di brevetto
- **Ampio contesto:** interfaccia grafica drill-down web-based per la ricerca e il controllo di pacchetti, connessioni e sessioni
- **Visibilità estesa:** supporto decoder sessione per la visualizzazione e la ricerca web, email, FTP, DNS, chat, dettagli di connessione SSL e file allegati
- **Acquisizione intelligente:** filtro selettivo del traffico catturato per eliminare lo streaming di video, i trasferimenti dei file di grandi dimensioni, i payload crittografati, ecc.
- **Maggiore efficienza:** processi automatizzati per identificare il furto di dati, utilizzando algoritmi di proprietà per diagnosticare un comportamento della rete potenzialmente anomalo

**Tabella 1.** Appliance disponibili per l'acquisizione di pacchetti.

| Modello | Configurazione della porta di acquisizione | Porte di gestione | Velocità massima di registrazione | Capacità di archiviazione totale integrata | Dimensioni | Alimentazione/Carico operativo tipico |
|---|---|---|---|---|---|---|
| **PX 1004S-6** | 1 x 2GigE | 1 x 1GbE | 500 Mbit/s | 6 TB | 1U<br>17,2" (437 mm) x<br>19,7" (500 mm) x<br>1,7" (44 mm)<br>18 lb (8,2 kg) | AC, Fisso AC 100 ~ 240 V<br>@ 50 ~ 60 Hz, ingresso<br>IEC60320-C14 |
| **PX 2060ESS-96** | 4 x 10GE SFP+ | 2 x 1GbE | 2 Gbit/s | Unità di archiviazione SAS da 96 TB espandibile | 2U<br>17,24" (438 mm) x<br>24,41" (620 mm) x<br>3,48" (88,4mm)<br>57,3 lbs (26 kg) | Ridondante (1+1) 800 watt,<br>100 - 240 VAC<br>10,5 – 4,0A, 50-60 Hz,<br>ingresso IEC60320-C14, FRU |
| **PX 2060ESS-120** | 4 x 10GE SFP+ | 2 x 1GbE | 7,5 Gbit/s | Unità di archiviazione SAS da 120 TB espandibile | 2U<br>17,24" (438 mm) x<br>24,41" (620 mm) x<br>3,48" (88,4mm)<br>57,3 lbs (26 kg) | Ridondante (1+1) 800 watt,<br>100 - 240 VAC<br>10,5 – 4,0A, 50-60 Hz,<br>ingresso IEC60320-C14, FRU |
| **PX 1004EXT-4G** | 4 x 1 Gbit/s,<br>10/100/1000<br>BaseT, SFP | 2 x 10/100/1000<br>BASE-T 2 x<br>10/100/1000/10G<br>BASE-T | 4 Gbit/s | Nessuna capacità di archiviazione locale.<br>Archiviazione Fiber HBA a SAN esterna | Montabile a rack 1U<br>1,7" (4,3 cm) x<br>17,2" (43,7 cm) x<br>25,6" (65 cm)<br>46 lbs (20,9 kg) | Alimentazione AC ridondante 650 W ad elevata efficienza (1+1)<br>100-240 VAC,<br>60-50 Hz auto-ranging<br>230-280 W tipico |
| **PX 1040EXT-20G** | 4 x 1 Gbit/s | 2 x 10/100/1000<br>BASE-T 2 x<br>10/100/1000/10G<br>BASE-T | 20 Gbit/s | Nessuna capacità di archiviazione locale.<br>Archiviazione Fiber HBA a SAN esterna | Montabile a rack 1U<br>1,7" (4,3 cm) x<br>17,2" (43,7 cm) x<br>25,6" (65 cm)<br>46 lbs (20,9 kg) | Alimentazione AC ridondante 650 W ad elevata efficienza (1+1)<br>100-240 VAC,<br>60-50 Hz auto-ranging<br>230-280 W tipico |
| **PX 4000SX440** | n/d | n/d | n/d | Ripiano archiviazione 440 TB | 17,2" (437 mm) x<br>27,5" (698 mm) x<br>7" (178 mm)<br>76 lbs (34 kg) | Alimentazione AC ridondante 1280 W ad elevata efficienza (1+1)<br>100-240 VAC,<br>60-50 Hz auto-ranging |

**Nota:** tutti i dati relativi alle prestazioni variano in base alla configurazione di sistema e al profilo di traffico elaborato.

Le appliance FireEye Investigation Analysis supportano diverse configurazioni per architetture distribuite o singoli nodi al fine di ottimizzare la larghezza di banda e le prestazioni delle attività di aggregazione, query e analisi dei metadati.

## Investigation Analysis - Caratteristiche

- **Visualizzazione:** visualizzazione e condivisione di attività e metadati relativi alla rete tramite dashboard personalizzate facili da creare
- **Risposte rapide:** parole chiave centralizzate a livello di applicazioni, espressioni regolari e query wildcard centralizzate su tutti gli avvisi, il flusso acquisito e i metadati
- **Interfaccia agile:** pivot immediato e download di dati PCAP singoli o di massa per sessioni di interesse
- **Efficaci funzioni di ricerca:** ricerca accelerata con metadati indicizzati da protocolli come HTTP, SMTP, POP3, IMAP, SSL,TLS, DNS e FTP
- **Aggregazione IOC:** consolida gli avvisi dei prodotti FireEye Network Security, Email Security ed Endpoint Security insieme a tutti i metadati di rete in un unico workbench con un pivot immediato "one-click" per i dati di sessione dagli avvisi
- **A caccia di minacce retrospettive:** analisi delle minacce IOC "back-in-time" tramite l'integrazione di feed FireEye Threat Intelligence, STIX e OpenIOC con la funzione di ricerca IA automatizzata. Avvisi automatici degli IOC presenti in rete dei giorni o delle settimane precedenti
- **Ricostruzione dei file con 1 clic:** ricostruisci e-mail, pagine web e file sospetti in modo rapido e sicuro per approfondire l'analisi

**Tabella 2.** Appliance investigation analysis disponibili.

| Modello | Capacità di archiviazione totale integrata | Dimensioni | Alimentazione/Carico operativo tipico |
|---|---|---|---|
| **IA 1000 DIR** | 6 TB | 17,2" (437 mm) x 19,7" (500 mm) x 1,7" (44 mm) | AC, Fisso AC 100 ~ 240 V @ 50 ~ 60 Hz, ingresso IEC60320-C14 |
| **IA 2100-48** | 48 TB | 17,2" (437 mm) x 19,7" (500 mm) x 1,7" (44 mm) | Ridondante (1+1) 800 watt, 100 - 240 VAC 10,5 – 4,0A, 50-60 Hz, ingresso IEC60320-C14, FRU |

Per ulteriori informazioni su FireEye, visitare il sito: **www.FireEye.com**

**FireEye Italia Srl**
Piazza IV Novembre, 7
20124 Milano
Italy
+39 0294750535
italy@FireEye.com



**A proposito di FireEye Italia Srl**
FireEye è l'azienda di sicurezza guidata dalle informazioni. Fungendo da estensione semplice e scalabile delle attività di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e servizi di consulenza Mandiant®, rinomati in tutto il mondo. Con questo approccio, FireEye elimina la complessità e il peso della sicurezza informatica per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici.