FIREEYE™

Ficha técnica

Network Forensics

Minimize o impacto de ataques a redes com análises investigativas e captura de pacotes de alto desempenho

As organizações precisam da detecção precoce e investigação rápida de incidentes para determinar o escopo e o impacto, conter efetivamente as ameaças e proteger novamente sua rede.

A solução FireEye Network Forensics combina a mais rápida solução de recuperação e captura de dados de rede sem perdas do setor com análise e visualização centralizadas. Ela acelera o processo forense de rede com um único painel que simplifica as investigações e reduz o risco.

O FireEye Network Forensics permite identificar e resolver incidentes de segurança mais rapidamente ao capturar e indexar pacotes completos em velocidades extremamente elevadas. Com o Network Forensics, é possível detectar uma ampla gama de incidentes de segurança, melhorar a qualidade de sua resposta e quantificar precisamente o impacto de cada incidente.

Como parte da solução FireEye Network Forensics, os appliances de análise investigativa revelam ameaças ocultas e aceleram a resposta a incidentes ao acrescentar um painel centralizado com uma interface analítica fácil de usar.

Os analistas podem examinar sessões e pacotes de rede específicos antes, durante e após um ataque. A possibilidade de reconstruir e visualizar os eventos que desencadeiam um download de malware ou um callback permite que sua equipe de segurança responda de maneira efetiva e imediata para prevenir novas ocorrências. Eles podem expandir a visibilidade sobre as atividades do invasor ao decodificar os protocolos normalmente utilizados para a disseminação lateral de ataques dentro da rede.

Essa combinação exclusiva de análise detalhada e captura de pacotes de alto desempenho ajuda a reconhecer e monitorar rapidamente todos os elementos de um ataque.

Figura 1. Appliances FireEye Network Forensics para análise e captura de pacotes.

Destaques da captura de pacotes

- **Alto desempenho:** captura de pacotes contínua e sem perdas, com identificação de data e hora e velocidades de gravação de até 20 Gbps
- **Alta fidelidade:** indexação em tempo real de todos os pacotes capturados utilizando-se atributos de conexão e data e hora. Exportação do índice de fluxo e metadados de conexão no formato JSON. O índice de fluxo pode ser convertido para os formatos de dado NetFlow v9, IPFIX e Silk Tools
- **Resultados rápidos:** pesquisa e recuperação ultrarrápidas de pacotes e conexões de destino utilizando uma arquitetura de indexação patenteada
- **Contexto avançado:** interface gráfica de usuário detalhada e baseada na Web para pesquisa e inspeção de pacotes, conexões e sessões
- **Visibilidade abrangente:** suporte para decodificador de sessões para visualização e pesquisa de Web, e-mail, FTP, DNS, chat, detalhes de conexões SSL e arquivos anexados
- **Captura inteligente:** filtragem seletiva do tráfego capturado para eliminar streaming de vídeo, transferências de grandes arquivos, conteúdo criptografado etc.
- **Eficiências aprimoradas:** processos automatizados para identificar roubo de dados utilizando algoritmos próprios para diagnosticar comportamentos potencialmente anômalos na rede

Tabela 1. Appliances disponíveis de captura de pacotes.

Modelo	Configuração de portas de captura	Portas de gerenciamento	Velocidade máxima de gravação	Armazenamento interno total	Dimensões	Fonte de alimentação/carga operacional habitual
PX 1004S-6	1 x 2GigE	1 x 1GbE	500 Mbps	6 TB	1U 17,2" (437 mm) x 19,7" (500 mm) x 1,7" (44 mm) 18 lbs (8,2 kg)	CA, CA fixo 100 ~ 240 V a 50 ~ 60 Hz, entrada IEC 60320-C14
PX 2060ESS-96	4 x 10GE SFP+	2 x 1GbE	2 Gbps	96 TB, armazenamento expansível por conexão SAS	2U 17,24" (438 mm) x 24,41" (620 mm) x 3,48" (88,4 mm) 57,3 lbs (26 kg)	Redundante (1+1) de 800 W, 100–240 VCA 10,5–4,0 A, 50–60 Hz, entrada IEC 60320-C14, FRU
PX 2060ESS-120	4 x 10GE SFP+	2 x 1GbE	7,5 Gbps	120 TB, armazenamento expansível por conexão SAS	2U 17,24" (438 mm) x 24,41" (620 mm) x 3,48" (88,4 mm) 57,3 lbs (26 kg)	Redundante (1+1) de 800 W, 100–240 VCA 10,5–4,0 A, 50–60 Hz, entrada IEC 60320-C14, 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	Sem armazenamento interno. Fibra HBA para armazenamento SAN externo	1U para montagem em rack 1,7" (4,3 cm) x 17,2" (43,7 cm) x 25,6" (65 cm) 46 lbs (20,9 kg)	650 W redundante de alta eficiência (1+1), alimentação CA de 100-240 VCA, 60-50 Hz com seleção automática, 230-280 W típicos
PX 1040EXT-20G	4 x 1 Gbps	2 x 10/100/1000 BASE-T 2 x 10/100/1000/10G BASE-T	20 Gbps	Sem armazenamento interno. Fibra HBA para armazenamento SAN externo	1U para montagem em rack 1,7" (4,3 cm) x 17,2" (43,7 cm) x 25,6" (65 cm) 46 lbs (20,9 kg)	650 W redundante de alta eficiência (1+1), alimentação CA de 100-240 VCA, 60-50 Hz com seleção automática, 230-280 W típicos
PX 4000SX440	n/d	n/d	n/d	Gaveta de armazenamento bruto 440 TB	17,2" (437 mm) x 27,5" (698 mm) x 7" (178 mm) 76 lbs (34 kg)	1.280 W redundante de alta eficiência (1+1), alimentação CA de 100-240 VCA, 60-50 Hz com seleção automática

Observação: todos os valores de desempenho variam dependendo da configuração do sistema e do perfil de tráfego sendo processado.

Os appliances FireEye de análise investigativa são compatíveis com diversas configurações de nó único e arquiteturas distribuídas para otimizar a largura de banda e o desempenho de análises, consultas e agregação de metadados.

Destaques sobre a análise investigativa

- **Visualização:** visualize e compartilhe metadados e atividades de rede através de dashboards personalizados e fáceis de criar
- **Respostas rápidas:** faça consultas centralizadas a nível de aplicativo com caracteres curinga, regex e palavra-chave em todos os alertas, metadados e fluxos capturados
- **Interface ágil:** mudança imediata e download de dados PCAP individuais ou em massa para sessões de interesse
- **Pesquisa avançada:** acelere a pesquisa com metadados indexados de protocolos como HTTP, SMTP, POP3, IMAP, SSL, TLS, DNS e FTP
- **Agregação IOC:** consolide alertas dos produtos FireEye Network Security, Email Security e Endpoint Security juntamente com todos os metadados de rede em um único painel centralizado com mudança imediata de "um clique" para dados de sessão com base em alertas
- **Caça retroativa a ameaças:** análise "retroativa" de ameaças IOC via integração entre os feeds do FireEye Threat Intelligence, STIX e OpenIOC com função de pesquisa automatizada por IA. Seja automaticamente alertado para IOCs presentes na rede com dias ou semanas de antecedência
- **Reconstrução de arquivos com um clique:** reconstrução rápida e segura de arquivos suspeitos, páginas da Web e e-mails para nova análise

Tabela 2. Appliances disponíveis de análise investigacional.

Modelo	Armazenamento interno total	Dimensões	Fonte de alimentação/carga operacional habitual
IA 1000 DIR	6 TB	17,2" (437 mm) x 19,7" (500 mm) x 1,7"(44 mm)	CA, CA fixo 100 ~ 240 V a 50 ~ 60 Hz, entrada IEC 60320-C14
IA 2100-48	48 TB	17,2" (437 mm) x 19,7" (500 mm) x 1,7"(44 mm)	Redundante (1+1) de 800 W, 100–240 VCA 10,5–4,0 A, 50–60 Hz, entrada IEC 60320-C14, FRU

Para saber mais sobre a FireEye, visite: **www.FireEye.com**

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

Sobre a FireEye, Inc.
A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência de ameaças em nível governamental e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos.

FIREEYE™