Ficha técnica

FireEye Central Management

Centralize gerenciamento de dispositivos e de inteligência para correlacionar dados entre vetores de ataque

DESTAQUES

- Oferece controles integrados para implantações em múltiplas plataformas
- Permite a prevenção de ameaças mistas com correlação multivetorial
- Oferece uma plataforma dedicada que pode ser implantada em menos de 60 minutos
- Exibe um dashboard de segurança de visualização rápida, informando o status da proteção contra ataques avançados e direcionados
- Acelera a geração de relatórios e auditorias por meio de um repositório consolidado de eventos de segurança
- Otimiza o gerenciamento de múltiplas soluções FireEye e reduz o tempo gasto com gerenciamento de configurações, atualizações de ameaças e atualizações de software

Figura 1. CM 4500 e CM 9500 (CM 7500 não exibido).

Visão geral

O FireEye® Central Management (série CM) consolida a administração, a geração de relatórios e o compartilhamento de dados dos produtos FireEye em uma solução baseada em rede e de fácil implantação. O Central Management viabiliza o compartilhamento em tempo real de inteligência gerada automaticamente sobre ameaças a fim de identificar e bloquear ataques avançados e direcionados contra sua empresa. Ele também permite operações centralizadas de configuração, gerenciamento e geração de relatórios de soluções FireEye.

Compartilhamento em tempo real de inteligência local sobre ameaças

As soluções FireEye geram inteligência sobre ameaças em tempo real usando o mecanismo FireEye Multi-Vector Virtual Execution™ (MVX). O Central Management distribui a inteligência de ameaças para várias implantações FireEye em seus sistemas, garantindo que cada solução tenha as mesmas proteções dinâmicas contra ataques avançados. Os assinantes do serviço de nuvem FireEye Dynamic Threat Intelligence™ (DTI) podem usar o Central Management para centralizar o envio e o recebimento de inteligência anônima sobre ameaças entre as soluções FireEye implantadas em clientes, parceiros de tecnologia e provedores de serviços em todo o mundo.

Dashboard de segurança de visualização rápida com detalhamento

O Central Management consolida as atividades e aprimora a percepção situacional com um dashboard de segurança unificado. O dashboard oferece aos administradores uma visualização em tempo real da quantidade de sistemas infectados e fornece detalhes diretos sobre a infecção para a determinação das próximas ações.

Análise unificada de ataques direcionados avançados
A análise de ameaças mistas, como a localização de um e-mail de spear-phishing usado para distribuir URLs nocivos e a correlação de um alerta de perímetro ao ponto de extremidade, passa a ser possível. Os analistas de segurança podem ligar os pontos de um ataque misto para obter a inteligência prática necessária para proteger as organizações contra ataques direcionados avançados.

Console de nível corporativo e emissão de alertas
O Central Management oferece um console com interface gráfica de usuário baseada na Web, no qual é possível visualizar, pesquisar e filtrar eventos, além de enviar notificações de alerta em tempo real via SMTP, SNMP, syslog ou HTTP POST. Os administradores podem fazer filtragem por eventos, datas ou intervalos de IP, e os resultados exibem apenas os dados com base na função operacional de TI do administrador. As notificações também podem ser enviadas para ferramentas SIEM de terceiros. Além disso, os administradores podem clicar no link de um evento e conectar-se diretamente a soluções específicas da FireEye para visualizar o segmento de rede sendo protegido.

Atualizações de plataforma e configurações centralizadas
Para implantações empresariais eficientes, o Central Management oferece configurações dinâmicas. É possível determinar configurações de modo centralizado, com a posterior distribuição adequada por toda a empresa. Os administradores podem definir e visualizar remotamente as configurações para uma ou mais soluções de segurança FireEye. Além disso, todas as atualizações podem ser implantadas simultaneamente em todas as soluções gerenciadas, garantindo que elas tenham as mais recentes capacidades de segurança.

Armazenamento consolidado e geração de relatórios detalhados
Organizações de maior porte e sujeitas a regulamentações podem usar o Central Management para operações eficientes e consolidadas de geração de relatórios sobre dados de segurança. O Central Management permite que você colete e armazene eventos de segurança relevantes para auditoria, visando a atender aos requisitos de retenção de dados de longo prazo.

O Central Management oferece maneiras convenientes de pesquisar e gerar relatórios sobre ameaças por nome ou tipo. As organizações também podem visualizar resumos, como os hosts mais infectados, além de eventos de callback e malware, incluindo detalhes de localização geográfica. As visualizações de tendências podem ajudar a mostrar o progresso na redução da quantidade de sistemas comprometidos.

Tabela 1. Especificações do appliance.

	CM 4500	CM 7500	CM 9500
Portas de interface de rede	2 x 1GigE BaseT	2 x 1GigE BaseT	2 x 1GigE BaseT
Portas de gerenciamento (painel traseiro)	2 x 1GigE BaseT	2 x 1GigE BaseT	2 x 1GigE BaseT
Porta IPMI (painel traseiro)	Incluída	Incluída	Incluída
Painel frontal LCD e teclado numérico	Incluídos	Incluídos	Incluídas
Portas PS/2 para teclado e mouse, e DB15 para monitor VGA (painel traseiro)	Incluídas	Incluídas	Incluídas
Portas USB (painel traseiro)	2 x portas USB tipo A	2 x portas USB tipo A	2 x portas USB tipo A
Porta serial (painel traseiro)	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit	115.200 bps, sem paridade, 8 bits, 1 stop bit
Capacidade de armazenamento	4 x HDD de 4 TB, compatível com RAID 10; 8 TB	4 x HDD de 4 TB, compatível com RAID 10; 8 TB	4 x HDD de 4 TB, compatível com RAID 10; 8 TB
Gabinete	1 RU, para rack de 19"	2 RU, para rack de 19"	2 RU, para rack de 19"
Dimensões do chassi (L x P x A)	17,2"x 25,6" x 1,7" (437 x 650 x 43,2 mm)	17,24" x 24,41" x 3,48" (438 x 620 x 88,4 mm)	17,24" x 24,41" x 3,48" (438 x 620 x 88,4 mm)
Fonte de alimentação CA	Fontes de alimentação redundantes (1+1), 750 W, CA	Fontes de alimentação redundantes (1+1), 800 W, CA	Fontes de alimentação redundantes (1+1), 800 W, CA
Consumo de energia máximo (W)	245 W	456 W	612 W
Dissipação térmica máxima (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h

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

Tabela 1. Especificações do appliance.

	CM 4500	CM 7500	CM 9500
MTBF (h)	35.200 h	60.700 h	60.700 h
Peso líquido/total (kg)	13,6 kg/18,6 kg	20,0 kg/29,6 kg	22,9 kg/32,5 kg
Certificações de segurança	IEC 60950, EN 60950, CSA 60950-00, marcação CE	IEC 60950, EN 60950, CSA 60950-00, marcação CE	IEC 60950, EN 60950, CSA 60950-00, marcação CE
Certificações EMC/EMI	FCC Part 15 Subparte B classe A; ICES-003 classe A; EN 61000-3-2 classe A; EN 61000-3-3; CISPR22 classe A	FCC Part 15 Subparte B classe A; ICES-003 classe A; EN 61000-3-2 classe A; EN 61000-3-3; CISPR22 classe A	FCC Part 15 Subparte B classe A; ICES-003 classe A; EN 61000-3-2 classe A; EN 61000-3-3; CISPR22 classe A
Conformidade regulatória	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Temperatura de funcionamento	0 ~ 35 °C	0 ~ 35 °C	0 ~ 35 °C
Umidade relativa de funcionamento	10 ~ 95% a 40 °C, sem condensação	10 ~ 95% a 40 °C, sem condensação	10 ~ 95% a 40 °C, sem condensação
Altitude de funcionamento	1.500 m	1.500 m	1.500 m

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

Tabela 2. Especificações do appliance virtual.

Modelo	Núcleos de CPU	RAM	NICS virtuais	Espaço em disco
CM2500V	4	32 GB	4 (total): 1 (administração) 1-3 (para uso futuro)	512 GB
CM7500V	16	128 GB	4 (total): 1 (administração) 1-3 (para uso futuro)	1200 GB

Observação: cada appliance virtual deve atender às especificações a seguir.

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™