SCHEDA TECNICA

FireEye Central Management

Centralizzare la gestione dei dispositivi e dell'intelligence per correlare i dati tra i vettori di attacco

CARATTERISTICHE PRINCIPALI

- Offre un controllo centralizzato ed integrato nel caso di installazioni di piattaforme FireEye multiple
- Facilita la prevenzione delle minacce combinate attraverso la correlazione degli eventi tra più vettori di ingresso
- Mette a disposizione una piattaforma creata appositamente che può essere resa operativa in meno di 60 minuti
- Rende disponibile una dashboard di sicurezza con visione di sintesi che fornisce lo stato di protezione contro gli attacchi mirati avanzati
- Velocizza report e verifiche attraverso un archivio consolidato sugli eventi di sicurezza
- Ottimizza la gestione di molteplici soluzioni FireEye e riduce il tempo speso nella gestione di configurazioni, aggiornamenti sulle minacce e aggiornamenti software

Figura 1. CM 4500 e CM 9500 (non incluso nella foto CM 7500).

Panoramica
FireEye® Central Management (serie CM) consolida l'amministrazione, la reportistica e la condivisione dei dati sui prodotti FireEye in un'unica soluzione di rete di semplice implementazione. La serie Central Management permette la condivisione, in modo automatico e in tempo reale, delle informazioni sulle minacce generate per identificare e bloccare attacchi avanzati contro l'azienda. Facilita inoltre la configurazione, la gestione e la reportistica centralizzate delle soluzioni FireEye.

Condivisione in tempo reale delle informazioni sulle minacce informatiche
Utilizzando il motore FireEye Multi-Vector Virtual Execution™ (MVX), le soluzioni FireEye generano informazioni sulle minacce in tempo reale. Central Management distribuisce tali informazioni sulle minacce a più implementazioni di FireEye all'interno dei sistemi, verificando che ogni soluzione disponga delle stesse protezioni dinamiche contro gli attacchi avanzati. Mediante il cloud FireEye Dynamic Threat Intelligence™ (DTI), gli utenti possono utilizzare la funzione Central Management per centralizzare l'invio e la ricezione, in forma anonima, di informazioni sulle minacce alle soluzioni FireEye distribuite presso clienti, partner tecnologici e fornitori di servizi in tutto il mondo.

Dashboard sulla sicurezza: visione di sintesi e approfondimenti
Central Management consolida le attività di gestione e migliora la percezione della situazione in essere con una dashboard di sicurezza unificata. La dashboard offre agli amministratori una visione in tempo reale sul numero di sistemi infetti per poi approfondire direttamente i dettagli relativi all'infezione e stabilire quindi i passaggi successivi.

Analisi unificata degli attacchi mirati avanzati

In tal modo si rende possibile l'analisi delle minacce combinate, come ad esempio l'individuazione di un'e-mail spear-phishing utilizzata per distribuire indirizzi URL pericolosi e la correlazione di un perimetro di avviso agli endpoint. Gli analisti della sicurezza possono collegare tutti gli elementi di un attacco combinato, per ottenere le informazioni necessarie per proteggere le aziende contro gli attacchi mirati avanzati.

Console di tipo enterprise e allarmi

Central Management mette a disposizione una console con interfaccia grafica Web da cui è possibile visualizzare, ricercare e filtrare gli eventi e da cui inviare notifiche di avviso in tempo reale tramite SMTP, SNMP, syslog o HTTP POST. Gli amministratori possono attivare dei filtri relativi a specifici eventi, date o serie di indirizzi IP; i risultati vengono visualizzati mostrando solo i dati richiesti e associati al ruolo operativo informatico dell'amministratore. Le notifiche possono essere inviate anche a strumenti SIEM di terze parti. Gli amministratori possono cliccare sul link di un evento e collegarsi a soluzioni FireEye specifiche per visualizzare il segmento di rete protetto.

Configurazione centrale e aggiornamenti della piattaforma

Al fine di ottenere implementazioni di piattaforme FireEye efficienti, la serie Central Management offre configurazioni dinamiche. Le impostazioni possono essere stabilite a livello centrale e quindi distribuite conformemente a tutte le appliance presenti all'interno di un'azienda. Gli amministratori possono configurare da remoto e visualizzare le impostazioni di una o più soluzioni di sicurezza FireEye. Inoltre, tutti gli aggiornamenti possono essere distribuiti contemporaneamente su tutte le soluzioni gestite, assicurando che tutte dispongano delle funzionalità di sicurezza più recenti.

Archivio consolidato e reportistica dettagliata

Aziende di grandi dimensioni e complesse possono usare Central Management per ottenere in modo efficiente una reportistica consolidata riguardante la sicurezza dei dati. Central Management consente di acquisire e archiviare eventi di sicurezza rilevanti per i processi di verifica per soddisfare i requisiti di conservazione dei dati sul lungo periodo.

Central Management offre un modo pratico per ricercare e fornire report sulle minacce, in base al nome o al tipo. Le aziende possono anche visualizzare dei documenti di sintesi relativi, per esempio, ai principali host infetti, malware ed eventi di callback, inclusivi di dettagli di geo-localizzazione. Le visualizzazioni sui trend aiutano a mostrare i progressi nella riduzione del numero di sistemi compromessi.

Tabella 1. Specifiche delle appliance.

	CM 4500	CM 7500	CM 9500
Porte interfacce di rete	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Porte di gestione (pannello posteriore)	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Porta IPMI (pannello posteriore)	Incluso	Incluso	Incluso
LCD frontale e tastierino numerico	Incluso	Incluso	Incluso
Tastiera e mouse PS/2, porte VGA DB15 (pannello posteriore)	Incluso	Incluso	Incluso
Porte USB (pannello posteriore)	2 porte USB Tipo A	2 porte USB Tipo A	2 porte USB Tipo A
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità di archiviazione	4 HDD da 4 TB, RAID 10; 8 TB	4 HDD da 4 TB, RAID 10; 8 TB	4 HDD da 4 TB, RAID 10; 8 TB
Involucro	1RU, Rack 19 pollici	2RU, Rack 19 pollici	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	437 x 650 x 43,2 mm	438 x 620 x 88,4 mm	438 x 620 x 88,4 mm
Alimentatore CA	Ridondante (1+1) 750W AC PSUs	Ridondante (1+1) 800W AC PSUs	Ridondante (1+1) 800W AC PSUs
Consumo massimo (watt)	245 watt	456 watt	612 watt
Dissipazione termica massima (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h
MTBF (h)	35.200 ore	60.700 ore	60.700 ore
Peso sola appliance/con confezione, kg (lb)	30,0 lb (13,6 kg) / 41,0 (18,6 kg)	20,0 kg (44,1 lb)/29,6 kg (65,3 lb)	50,4 lb (22,9 kg) / 71,6 lb (32,5 kg)

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

Tabella 1. Specifiche delle appliance.

	CM 4500	CM 7500	CM 9500
Certificazioni di sicurezza	IEC 60950, EN 60950, CSA 60950-00, Marchio CE	IEC 60950, EN 60950, CSA 60950-00, Marchio CE	IEC 60950, EN 60950, CSA 60950-00, Marchio CE
Certificazioni EMC/EMI	FCC Parte 15 Sottoparte B Classe A; ICES-003 Classe A; EN 61000-3-2 Classe A; EN 61000-3-3; CISPR22 Classe A	FCC Parte 15 Sottoparte B Classe A; ICES-003 Classe A; EN 61000-3-2 Classe A; EN 61000-3-3; CISPR22 Classe A	FCC Parte 15 Sottoparte B Classe A; ICES-003 Classe A; EN 61000-3-2 Classe A; EN 61000-3-3; CISPR22 Classe A
Conformità normativa	RoHS, REACH, RAEE	RoHS, REACH, RAEE	RoHS, REACH, RAEE
Temperatura operativa	0 - 35 °C	0 - 35 °C	0 - 35 °C
Umidità operativa relativa	10 - 95% @ 40 °C, senza condensa	10 - 95% @ 40 °C, senza condensa	10 - 95% @ 40 °C, senza condensa
Altitudine operativa	1.500 metri	1.500 metri	1.500 metri

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

Tabella 2. Specifiche delle appliance virtuali.

Modello	CPU Cores	RAM	NIC virtuali	Spazio hard disk
CM2500V	4	32 GB	4 (totale): 1 (gestione) 1-3 (per uso futuro)	512 GB
CM7500V	16	128 GB	4 (totale): 1 (gestione) 1-3 (per uso futuro)	1200 GB

Nota: ciascuna appliance virtuale deve rispettare le seguenti specifiche.

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.