SCHEDA TECNICA

FireEye Network Security

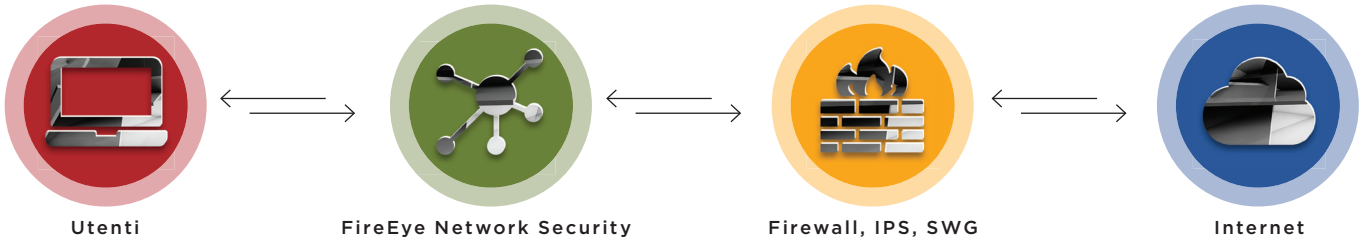
Protezione efficace contro le intrusioni informatiche per imprese di medie e grandi dimensioni

Panoramica
FireEye Network Security è un'efficace soluzione di protezione dalle minacce informatiche che aiuta le imprese a ridurre al minimo il rischio di costose violazioni, rilevando con precisione e bloccando immediatamente attacchi avanzati, mirati e altri tipi di attacchi evasivi nascosti nel traffico Internet. Consente di risolvere i ciberincidenti rilevati in modo efficiente, in pochi minuti, con prove concrete, informazioni fruibili e integrazione delle attività di risposta. Con FireEye Network Security, le imprese sono protette in modo efficace contro le attuali minacce, da quelle che sfruttano i sistemi operativi Microsoft Windows e Apple OS X o le vulnerabilità delle applicazioni a quelle dirette alle sedi centrali o filiali, passando per quelle nascoste in un grande volume di traffico Internet in ingresso che deve essere ispezionato in tempo reale.

Alla base di FireEye Network Security vi sono le tecnologie Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX è un motore di analisi dinamico senza firma che controlla il traffico di rete sospetto per identificare attacchi che eludono i sistemi di difesa tradizionali basati su criteri e firme. IDA è una raccolta di motori contestuali con regole dinamiche, che rilevano e bloccano le attività dannose in tempo reale e retroattivamente grazie alle ultime informazioni basate su macchina, hacker e vittima. Inoltre, FireEye Network Security include la tecnologia IPS (sistema di prevenzione delle intrusioni) per rilevare gli attacchi comuni con la convenzionale corrispondenza delle firme.

FireEye Network Security è disponibile in diverse opzioni suddivise per fattore di forma, implementazione e prestazioni. Normalmente si inserisce nel percorso del traffico Internet dietro alle apparecchiature di sicurezza di rete tradizionali come firewall di nuova generazione, IPS e gateway web sicuri (SWG). FireEye Network Security integra queste soluzioni mediante una rapida rilevazione di attacchi noti e sconosciuti con elevata precisione e un basso indice di falsi positivi, facilitando al contempo una risposta efficiente a ogni avviso.

Figura 1. Configurazione tipica - Soluzioni di sicurezza di rete.



Funzionalità	Vantaggi
Rilevamento	
Rilevamento accurato di attacchi informatici avanzati, mirati e altri tipi di attacchi evasivi	Riduce al minimo il rischio di costosi ciberincidenti
Architettura di protezione modulare ed estensibile	Fornisce una protezione degli investimenti
Livello coerente di protezione per ambienti multi-OS e tutti i punti di accesso a Internet	Crea una difesa solida in tutta l'azienda per tutti i tipi di dispositivi
Opzioni di distribuzione integrata, distribuita, fisica, virtuale, in loco e su cloud	Offre la flessibilità necessaria per allinearsi alle preferenze e alle risorse aziendali
Correlazione multi-vettoriale con Email e Content Security	Fornisce visibilità su una più ampia superficie di attacco
Prevenzione	
Blocco immediato degli attacchi a velocità di linea da 10 Mbit/s a 8 Gbit/s	Fornisce protezione in tempo reale contro gli attacchi evasivi
Risposta	
Basso tasso di falsi allarmi, categorizzazione riskware e convalida avvisi IPS automatizzata	Riduce i costi operativi per filtrare gli avvisi inaffidabili
Agevola convalida di avvisi e indagini, contenimento degli endpoint e risposta agli incidenti	**Automatizza e semplifica i flussi di lavoro di sicurezza**
Prove di esecuzione e informazioni fruibili sulle minacce con una visione contestuale	**Accelera la definizione delle priorità e la risoluzione dei ciberincidenti rilevati**
Scalabilità da un sito a migliaia di siti	**Sostiene la crescita aziendale**

Vantaggi tecnici

Rilevamento accurato delle minacce

FireEye Network Security utilizza più tecniche di analisi per rilevare attacchi con elevata precisione e un basso tasso di falsi allarmi:

- Il motore **Multi-Vector Virtual Execution™ (MVX)** rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica, senza firma in un ambiente sicuro e virtuale. Ferma le fasi di infezione e compromissione della catena di attacchi informatici identificando exploit e malware mai visti prima.
- I motori **Intelligence-Driven Analysis (IDA)** rilevano e bloccano attacchi camuffati, mirati e altri attacchi personalizzati attraverso l'analisi contestuale basata su regole grazie a informazioni di prima mano raccolte in tempo reale da milioni di verdetti MVX, migliaia di ore di attività di risposta agli incidenti svolta da Mandiant, un'azienda FireEye, e centinaia di esperti di cibersicurezza iSight. Interrompe le fasi di infezione, compromissione e intrusione della catena di ciberattacchi identificando exploit dannosi, malware e callback di comando e controllo (CnC). Inoltre, estrae e sottopone il traffico di rete sospetto al motore MVX per un'analisi di verdetto definitiva.
- **Structured Threat Intelligence eXpression (STIX)** permette di inglobare le informazioni sulle minacce di terze parti utilizzando un formato standard di settore per aggiungere indicatori di minaccia personalizzati nei motori IDA.

Protezione immediata e resiliente

FireEye Network Security offre modalità di configurazione flessibili, tra cui:

- Monitoraggio fuori banda tramite un TAP/SPAN, monitoraggio in linea o blocco attivo in linea. La modalità di blocco in linea blocca automaticamente gli exploit web in ingresso e i callback multiprotocollo in uscita. In modalità monitoraggio in linea genera gli avvisi e permette alle aziende di decidere come reagire. In modalità di prevenzione fuori banda, FireEye Network Security rilascia reset TCP per il blocco fuori banda di connessioni TCP, UDP o HTTP.
- Integrazione con lo switch Active Fail Open (AFO) di FireEye per garantire l'assenza di interruzioni di rete.
- Alcuni modelli offrono un'opzione di elevata disponibilità attiva (HA) per fornire capacità di recupero in caso di guasti di rete o del dispositivo.

Ampia copertura della superficie di attacco

FireEye Network Security offre un livello coerente di protezione per gli eterogenei ambienti di rete di oggi:

- Supporto per i sistemi operativi più diffusi di Microsoft Windows e Apple Mac OS X
- Analisi di oltre 140 tipi di file diversi, tra cui eseguibili portatili (PEs), contenuti web, archivi, immagini, Java, applicazioni e file multimediali Microsoft e Adobe
- Esecuzione del traffico di rete sospetto su migliaia di combinazioni di sistemi operativi, service pack, tipi di applicazione e versioni dell'applicazione

Avvisi convalidati e prioritari

Oltre a rilevare gli attacchi veri e propri, la tecnologia FireEye MVX è utilizzata anche per determinare l'affidabilità degli avvisi rilevati con metodi convenzionali di corrispondenza della firma, e per individuare le minacce critiche e stabilirne l'ordine di priorità:

- Il sistema di prevenzione delle intrusioni (IPS) con convalida del motore MVX riduce il tempo necessario per valutare il rilevamento basato su firme che è tradizionalmente soggetto a falsi allarmi
- La categorizzazione del riskware separa reali tentativi di violazione da attività indesiderabili, ma meno dannose (come adware e spyware) per stabilire l'ordine di priorità per le risposte agli avvisi

Informazioni fruibili sulle minacce

Gli avvisi generati da FireEye Network Security si basano su prove concrete e informazioni contestuali che permettono di rispondere rapidamente, ordinare per priorità e contenere una minaccia:

- **Dynamic Threat Intelligence (DTI):** dati concreti, in tempo reale e globalmente condivisi per fermare rapidamente e in modo proattivo gli attacchi mirati e di recente scoperta
- **Advanced Threat Intelligence (ATI):** informazioni contestuali sull'attacco per accelerare la risposta e indicazioni prescrittive per contenere la minaccia

Integrazione delle attività di risposta

FireEye Network Security può essere potenziato in vari modi per automatizzare le attività di risposta agli avvisi:

- FireEye Central Management correla gli avvisi inviati da Email Security e da FireEye Network Security per una visibilità più ampia dell'attacco e per impostare regole di blocco che ne impediscano un'ulteriore diffusione
- FireEye Network Forensics si integra con FireEye Network Security per fornire una dettagliata acquisizione di pacchetti associata a un avviso e consentire indagini approfondite
- FireEye Endpoint Security identifica, convalida e contiene compromissioni rilevate da FireEye Security Network per semplificare il contenimento e la correzione degli endpoint colpiti

Opzioni di distribuzione flessibili

FireEye Network Security offre varie opzioni di distribuzione per soddisfare le esigenze e il budget di un'azienda:

- **Integrated Network Security:** appliance hardware autonoma all-in-one con servizio MVX integrato per proteggere i punti di accesso a Internet in un unico ambiente. FireEye Network Security è una piattaforma senza client, di facile gestione, che può essere distribuita in meno di 60 minuti. Non necessita di regole, criteri o messa a punto.
- **Distributed Network Security:** appliance estensibili con servizio MVX condiviso centralmente per garantire punti di accesso a Internet all'interno delle aziende.
  - **Network Smart Node:** appliance fisiche o virtuali che analizzano il traffico Internet per rilevare e bloccare il traffico dannoso e segnalare le attività sospette tramite una connessione crittografata al servizio MVX per l'analisi definitiva del verdetto.
  - **MVX Smart Grid:** servizio MVX elastico, locale, gestito centralmente, che offre scalabilità trasparente, tolleranza ai guasti integrata N+1 e bilanciamento automatizzato del carico.
  - **FireEye Cloud MVX:** servizio in abbonamento MVX ospitato da FireEye che garantisce la privacy, analizzando il traffico sul Network Smart Node. Solo gli oggetti sospetti sono inviati tramite una connessione crittografata al servizio MVX, dove gli oggetti che si rivelano non dannosi vengono scartati.

Figura 2. Esempi di integrazione di Network Security comprendono NX 2550, NX 3500, NX 5500, NX 6500.

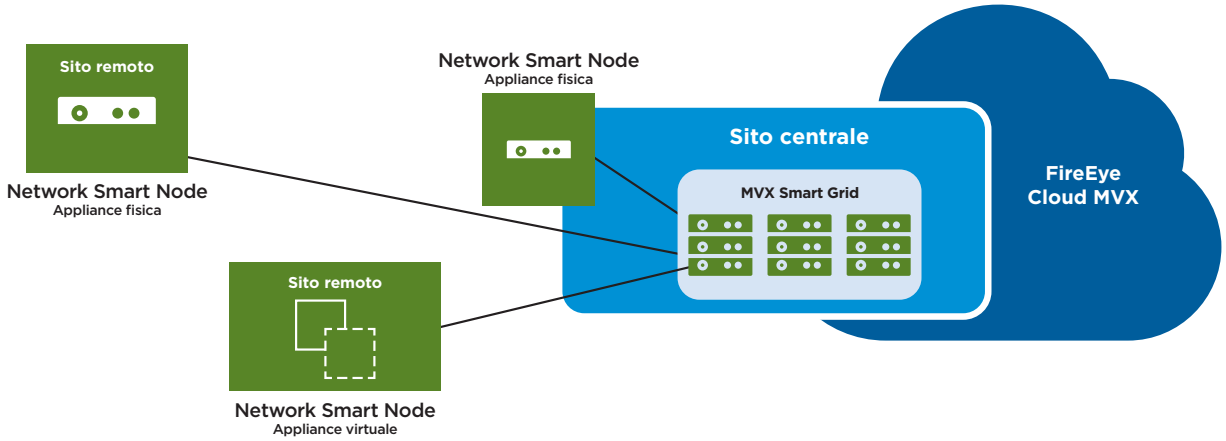


Figura 3. Modelli di implementazione distribuita per la sicurezza di rete.

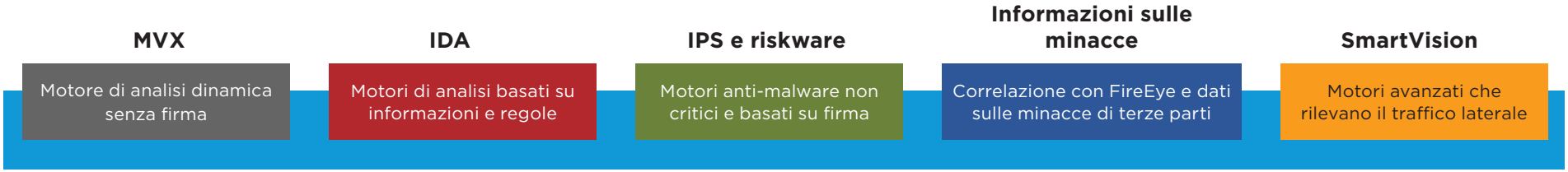


Figura 4. Componenti modulari di FireEye Network Security.

Architettura estensibile

I FireEye Network Smart Nodes dispongono di un'architettura software modulare ed estensibile e un sistema progettato per fornire più strumenti di protezione dalle minacce come i moduli software.

Elevate prestazioni e scalabilità

FireEye Network Security protegge i punti di accesso a Internet a velocità di linea con un'ampia gamma di scelte prestazionali per filiali e uffici centrali di svariate dimensioni:

L'architettura scalabile di MVX Smart Grid e FireEye Cloud MVX consente al servizio MVX di supportare fino a mille Network Smart Node e scalare senza problemi in base alle esigenze.

Formato	Prestazioni
Integrated Network Security	Da 50 Mbit/s a 5 Gbit/s
Network Smart Node fisico	Da 50 Mbit/s a 10 Gbit/s
Network Smart Node virtuale	Da 50 Mbit/s a 1 Gbit/s

Vantaggi per le aziende

Progettato per soddisfare le esigenze di aziende con un'unica sede o varie sedi distribuite, FireEye Network Security offre diversi vantaggi:

Riduce al minimo il rischio di ciberincidenti

FireEye Network Security è una soluzione altamente efficace per la protezione dai ciberattacchi:

- Impedisce agli intrusi di entrare in un'azienda per rubare beni di valore o interrompere l'attività fermando attacchi avanzati, mirati e altri tipi di attacchi evasivi
- Blocca gli attacchi e contiene le intrusioni più velocemente con prove concrete, informazioni fruibili, blocco in linea e automazione delle attività di risposta
- Tappa le falle dei sistemi di difesa informatici di un'azienda con una protezione coerente per i vari sistemi operativi, tipi di applicazione, filiali e sedi centrali

Breve periodo di recupero dell'investimento

Secondo un recente studio di Forrester Consulting[1], i clienti con FireEye Network Security possono aspettarsi un ROI del 152% in tre anni e ammortizzare l'investimento iniziale in soli 9,7 mesi. FireEye Network Security:

- Concentra le risorse del team di sicurezza sugli attacchi reali per ridurre le spese operative
- Ottimizza la spesa di capitale con un servizio MVX condiviso e una grande varietà di punti di performance per strutturare la distribuzione in base ai requisiti
- Investimenti adeguati alle future esigenze di sicurezza con possibilità di scalare senza problemi quando il numero di filiali o la quantità di traffico Internet aumenta
- Protegge gli investimenti esistenti, consentendo la migrazione a costo zero da un sistema integrato a un'implementazione distribuita
- Riduce le spese in conto capitale grazie a un'architettura modulare ed estensibile

Premi e certificazioni

Il portafoglio di prodotti FireEye Network Security ha ricevuto numerosi premi e certificazioni da organismi statali e associazioni di settore:

- Nel 2016, Frost & Sullivan ha riconosciuto FireEye come il leader indiscusso del mercato con una quota di mercato del 56%, più dei dieci principali concorrenti messi insieme[2]
- FireEye Network Security ha ricevuto numerosi premi da SANS Institute, SC Magazine, CRN e altri
- FireEye Network Security è stata la prima soluzione di sicurezza sul mercato a ricevere la certificazione del SAFETY Act del Dipartimento della sicurezza interna degli Stati Uniti

1 Forrester (maggio 2016). The Total Economic Impact Of FireEye.
2 Frost & Sullivan (ottobre 2016). Network Security Sandbox Market Analysis.