PANORAMICA SULLA

FIREEYE™

Affronta la sfida dell'evoluzione delle minacce di rete

Tieniti pronto agli attacchi che passano inosservati agli altri

Le sfide della sicurezza di oggi
Attacchi avanzati, mirati ed evasivi di altra natura rendono estremamente difficile per le aziende prevenire efficacemente le violazioni informatiche:

- I criminali informatici utilizzano attacchi avanzati per aggirare soluzioni antivirus, IPS e firewall di nuova generazione e si nascondono nelle aziende per mesi (320 giorni in media nel 2015, quando notificato esternamente)[1]
- Oltre il 68% del malware è specifico per un'azienda e l'80% di quel malware è usato solo una volta,[2] pertanto le difese basate su firme sono inefficaci contro gli attacchi mirati
- Oltre l'80% degli avvisi generati dai sistemi di sicurezza basati su criteri e firme sono inaffidabili[3] e sottraggono risorse all'analisi delle segnalazioni critiche

L'odierna trasformazione imprenditoriale dell'IT, che espande la superficie di attacco dell'azienda, rende ancora più complessa questa sfida:

- Entro il 2020, le applicazioni cloud pubbliche rappresenteranno oltre i due terzi della spesa aziendale.[4] Le operazioni basate su cloud aumentano del 40% il traffico Internet aziendale (e le potenziali minacce) in entrata e in uscita.[5] Tutto questo traffico deve essere controllato
- Al giorno d'oggi, i dispositivi non Windows supportati dal 96% delle aziende[6] solitamente non sono stati ben protetti
- L'adozione dei collegamenti diretti a Internet da parte del 40% delle filiali[5] aumenta la loro esposizione agli attacchi al di fuori dell'elevata protezione della sede centrale

Quattro requisiti per difendersi dalle violazioni informatiche
Per ridurre al minimo il rischio di costose violazioni informatiche, le aziende di tutte le dimensioni hanno bisogno di una soluzione che protegga efficacemente dagli attacchi. Deve:

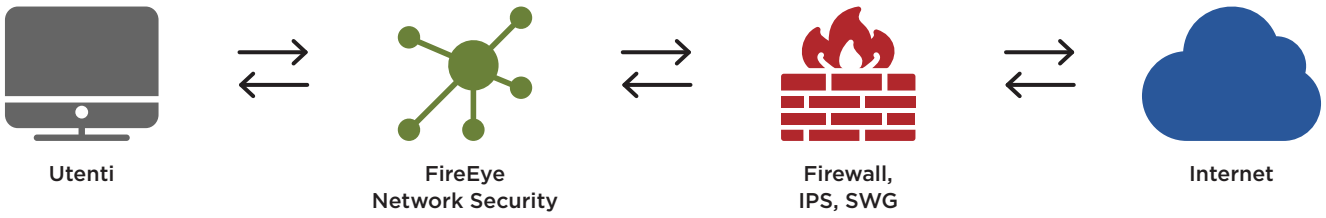
1. Rilevare e bloccare le minacce che i prodotti di sicurezza tradizionali non rilevano
2. Rispondere rapidamente e contenere l'impatto degli incidenti
3. Adattarsi costantemente all'evoluzione delle minacce
4. Scalare e rimanere flessibile quando l'azienda cresce o la modalità di erogazione dei servizi IT cambia

FireEye Network Security
FireEye Network Security aiuta le aziende di tutte le dimensioni 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. Il fulcro di FireEye Network Security sono le tecnologie Multi-Vector Virtual Execution™ (MVX) e Intelligence-Driven Analysis (IDA). MVX è un motore di analisi dinamica senza firme che ispeziona gli oggetti sospetti per identificare minacce mirate, evasive e sconosciute. I motori IDA rilevano e bloccano gli oggetti dannosi basati su informazioni della vittima, dell'aggressore o del computer.

FireEye Network Security è disponibile in diverse opzioni suddivise per fattore di forma e implementazione. 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).

1 FireEye (febbraio 2016). M-Trends 2016.
2 Joshua Goldfarb (19 settembre 2016). "Detection Innovations."
3 Ponemon Institute LLC (gennaio 2015). "The Cost of Malware Containment."
4 Forrester (settembre 2016). "The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020."
5 IDC (febbraio 2016). "Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services."
6 JAMF Software (2015). Sondaggio 2015: Managing Apple Devices in the Enterprise

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



Per proteggere efficacemente le aziende di tutte le dimensioni dalle violazioni informatiche, FireEye Network Security fornisce:

- **Rilevamento accurato:** le tecnologie MVX e IDA rilevano gli attacchi con un'elevata precisione e una bassa percentuale di falsi avvisi. Queste tecnologie correlano inoltre gli eventi su vari flussi e vettori di minaccia per proteggere da attacchi multifase che altre soluzioni non sono in grado di rilevare o bloccare.
- **Protezione immediata e resiliente:** il blocco in linea degli exploit in ingresso e i callback multiprotocollo in uscita fermano immediatamente gli attacchi. Un'opzione a disponibilità elevata fornisce resilienza e protezione aggiuntive quando un dispositivo o link di rete ha un malfunzionamento.
- **Informazioni immediatamente disponibili:** gli avvisi includono prove concrete e informazioni contestuali ottenute in prima linea che permettono di rispondere rapidamente, ordinare per priorità e contenere una minaccia.
- **Inserimento degli indicatori:** il formato Structured Threat Intelligence eXpression (STIX) permette di inserire le informazioni personalizzate nei motori IDA.
- NOVITÀ **Architettura estensibile:** la progettazione del sistema e del software consente l'erogazione di varie tecnologie di protezione dalle minacce come moduli software.

- **Protezione completa:** supporta diversi ambienti, tra cui le versioni più diffuse dei sistemi operativi Microsoft Windows e Apple OS X, oltre 140 tipi di file diversi e migliaia di combinazioni di sistemi operativi/service pack/applicazioni per coprire un'ampia superficie d'attacco
- **Integrazione delle attività di risposta:** convalida avviso, categorizzazione del rischio e pivot al cattura dei pacchetti per un'indagine approfondita automatizzano e accelerano i flussi di lavoro di risposta agli avvisi

Perfetto per la tua azienda

FireEye Network Security offre opzioni di distribuzione flessibili e scalabili fino a 8 Gbit/s per le esigenze e i budget delle aziende di medie e grandi dimensioni.

- **Network Security integrata:** un'appliance hardware indipendente tutto in uno che utilizza il servizio MVX per garantire un unico punto di accesso a Internet
- NOVITÀ **Sicurezza di rete distribuita:** i Network Smart Node e il servizio MVX condiviso estendono la protezione a tutta l'azienda
  - **Network Smart Node:** appliance fisiche o virtuali distribuite nei punti di accesso a Internet per identificare e proteggere dalle attività sospette
  - **MVX Smart Grid o FireEye Cloud MVX:** servizio MVX in loco o su cloud che conduce ulteriori analisi per rilevare attacchi avanzati e migliorare l'efficienza dei team di sicurezza

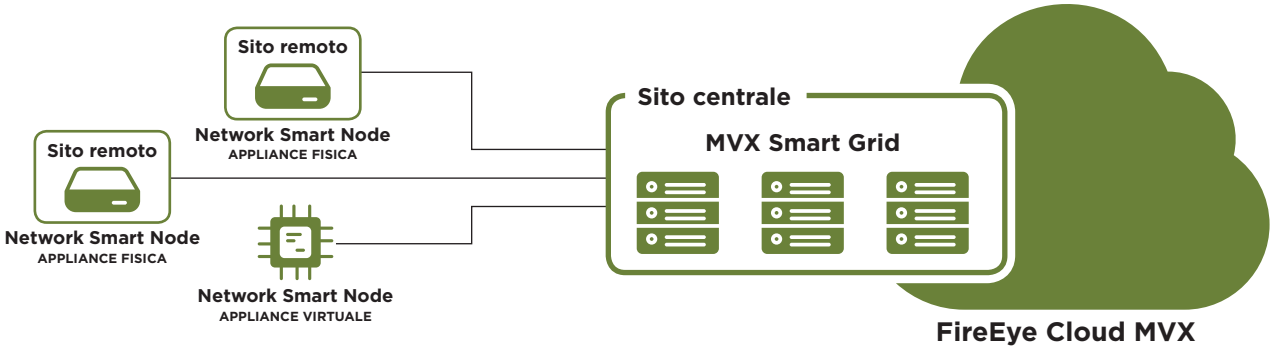


Figura 2. Sicurezza di rete distribuita.

FireEye Network Security Essentials offre opzioni di implementazione convenienti, integrate e distribuite da 10 Mbit/s a 2 Gbit/s per piccole e medie imprese.

Tabella 1. Opzioni di distribuzione FireEye Network Security.

	Appliance integrata	Network smart node	MVX Smart Grid Richiede network smart nodes	FireEye Cloud MVX Richiede network smart nodes
FireEye Network Security per aziende di medie e grandi dimensioni	In loco	Fisico o virtuale	In loco e distribuito	Basato su cloud e distribuito
FireEye Network Security Essentials per piccole e medie imprese	In loco	Fisico o virtuale	Non disponibile	Basato su cloud e distribuito

Rapido periodo di recupero dell'investimento

Progettato per soddisfare le esigenze di aziende con un'unica sede o varie sedi distribuite, FireEye Network Security minimizza il rischio di violazioni informatiche e riduce il tempo di recupero dell'investimento.

Secondo un recente studio di Forrester Consulting[7], i clienti FireEye Network Security possono aspettarsi un ritorno dell'investimento del 152% in tre anni grazie al risparmio e ammortizzare l'investimento iniziale in soli 9,7 mesi. Si possono ottenere risparmi presenti e futuri:

- Concentrando le risorse del team di sicurezza sugli attacchi reali per ridurre le spese operative
- Ottimizzando la spesa di capitale con opzioni di condivisione del servizio MVX e una grande varietà di punti di performance per dimensionare al meglio la distribuzione
- Rendendo gli investimenti a prova di futuro tramite un'espansione incrementale della capacità quando il numero di filiali o la quantità di traffico Internet aumenta
- Proteggendo gli investimenti esistenti, consentendo la migrazione a costo zero da un sistema integrato per un'implementazione distribuita
- Riducendo il futuro esborso di capitale grazie a un'architettura modulare ed estensibile

Perché scegliere FireEye Network Security?

Il motore FireEye MVX è la soluzione di protezione avanzata dalle minacce originale e più efficace[8] presente sul mercato:

- Dal 2013, FireEye ha scoperto più attacchi zero-day attivamente sfruttati di tutte le altre soluzioni messe insieme.
- Nel 2016, Frost & Sullivan ha riconosciuto FireEye come il leader indiscusso del settore con una quota di mercato del 56%, più dei dieci principali competitori messi insieme[9].
- 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.

7 Forrester (maggio 2016). "The Total Economic Impact Of FireEye."
8 IDC (2015). Worldwide Specialized Threat Analysis and Protection Market Shares.
9 Frost & Sullivan (settembre 2016). "Network Security Sandbox Market Analysis."

Tabella 2. Vantaggi di FireEye Network Security.

FUNZIONALITÀ	VANTAGGIO
Rilevare e bloccare le minacce che i prodotti di sicurezza tradizionali non rilevano	
Rilevamento delle minacce senza firma (MVX)	Rileva attacchi multiflusso, multifase, zero-day, polimorfici, ransomware ed evasivi di altra natura
Rilevamento in tempo reale e retroattivo	Rileva in tempo reale minacce note e sconosciute e consente anche il rilevamento di minacce passate
Correlazione multivettore	Automatizza la convalida e il blocco degli attacchi su vettori file, endpoint ed e-mail
Supporto multi-applicazione, multi-file e multi-OS	Supporta ambienti endpoint eterogenei per un'ampia gamma di applicazioni
Hardened hypervisor	Fornisce evasion proofing
Rispondere rapidamente e contenere l'impatto degli incidenti	
Blocco in linea in tempo reale	Blocca immediatamente gli attacchi
Flussi di lavoro di sicurezza integrati	Passa dal rilevamento all'indagine e risposta
Disponibilità elevata (HA)	Difesa resiliente
Rilevamento IPS basato su firme con riduzione del rumore	Automatizza e accelera la valutazione degli avvisi tradizionalmente rumorosi per eliminare i costi manuali
Rilevamento e categorizzazione del riskware	Categorizza il malware critico e non critico per definire la priorità delle risorse di risposta
Informazioni contestuali fruibili	Accelera il contenimento delle minacce avanzate con informazioni approfondite sull'attacco e l'aggressore
Adattarsi costantemente all'evoluzione delle minacce	
Condivisione in tempo reale delle informazioni sulle minacce	Prova reale condivisa globalmente per bloccare immediatamente attacchi precedentemente ignoti e accelerare la risposta
NOVITÀ **Informazioni sulle minacce personalizzate e di terze parti (STIX)**	Inserire gli indicatori FireEye e di terze parti nei motori IDA abilitati STIX
Informazioni strategiche sulle minacce	Consente una valutazione proattiva delle modifiche al panorama delle minacce e un atteggiamento attivo nei confronti della sicurezza
Scalare e rimanere flessibile quando l'azienda cresce o la modalità di erogazione dei servizi IT cambia	
Larghezze di banda supportate	10 Mbit/s – 8 Gbit/s
Scala supportata	Da sito singolo a migliaia di siti per implementazioni distribuite
Fattori di forma supportati	Fisico, virtuale, cloud
Modelli di distribuzione	Sicurezza di rete integrata e sicurezza di rete distribuita con Network Smart Node e architettura di servizio MVX

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

Informazioni su FireEye Italia Srl

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Fungendo da estensione semplice e scalabile delle operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i 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. FireEye conta oltre 6.600 clienti in 67 Paesi, tra cui più del 45% dei Forbes Global 2000.

FIREEYE™