SCHEDA TECNICA

FireEye Email Security Server Edition

Difesa scalabile, intelligente e adattiva contro le minacce via e-mail

CARATTERISTICHE PRINCIPALI

- Offre sicurezza e-mail completa da allegati nocivi, URL di phishing delle credenziali, spoofing, attacchi zero-day e multifase
- Supporta l'analisi delle immagini dei sistemi operativi Microsoft Windows e Apple macOS X
- Esamina dettagliatamente le e-mail in cerca di minacce nascoste in file protetti da password, allegati crittografati e URL
- Acquisisce in tempo reale l'intelligence sulle minacce da FireEye DTI Cloud
- Assegna priorità e contiene le minacce fornendo informazioni utili contestuali per gli avvisi
- Implementazione in loco con il servizio MVX integrato o distribuito

Figura 1. Le appliance Email Security integrate includono EX 3500, EX 5500 ed EX 8500.

Panoramica

Le e-mail rappresentano il vettore più vulnerabile per gli attacchi informatici, in quanto sono il punto di ingresso con il maggior volume di dati. Le aziende devono affrontare un numero crescente di sfide per la sicurezza, quali le minacce avanzate via e-mail. Molte delle minacce moderne sfruttano l'e-mail per consegnare URL che reindirizzano a siti di phishing delle credenziali e file allegati usati come arma. Poiché si tratta di una risorsa che può essere presa di mira facilmente e altamente personalizzabile, l'e-mail è il principale mezzo per i crimini informatici.

FireEye Email Security aiuta le aziende a minimizzare il rischio di costose violazioni causate da attacchi e-mail avanzati. Implementato in loco, FireEye Email Security - Server Edition è leader di settore nell'identificare, isolare e interrompere immediatamente gli attacchi basati su URL e allegati, prima che entrino nell'ambiente aziendale. Email Security combina plug-in di contestualizzazione e individuazione regolati da intelligence per scoprire gli URL di phishing dannosi e benigni sfruttano una piattaforma scalabile big data. Il motore Multi-Vector Virtual Execution™ (MVX) senza firme analizza gli allegati e-mail e gli indirizzi URL di collegamento a contenuti scaricabili confrontandoli con un'ampia struttura a matrice multipla di sistemi operativi, applicazioni e browser. Le minacce sono identificate in modo semplice e i falsi positivi sono praticamente inesistenti.

FireEye raccoglie informazioni dettagliate relative alle minacce attraverso indagini svolte direttamente sulle violazioni e attraverso l'utilizzo di milioni di sensori. Email Security sfrutta prove reali e intelligence di contesto su attacchi e aggressori, per stabilire l'ordine di priorità degli avvisi e bloccare le minacce in tempo reale.

Integrando FireEye Network Security con Endpoint Security, le aziende otterranno una maggiore visibilità, al fine di coordinare la protezione in tempo reale contro gli attacchi lanciati da vettori misti.

Difesa contro le minacce dalle e-mail
Poiché tutte le informazioni personali sono disponibili online, un criminale informatico è in grado di convincere, utilizzando tecniche di social engineering, qualunque utente a cliccare su un URL o ad aprire un allegato.

Email Security offre funzioni di rilevamento e prevenzione in tempo reale da attacchi di raccolta delle credenziali, impersonificazione e spear-phishing, che tipicamente eludono con facilità i sistemi di difesa e-mail tradizionali. Le e-mail vengono analizzate e messe in quarantena (bloccate), qualora vengano trovate minacce sconosciute e avanzate nascoste in:

- Tutti i tipi di allegato, tra cui: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 e archivi ZIP/RAR/TNEF
- Allegati protetti da password e crittografati
- Allegati protetti da password con password inviata tramite immagine
- URL incorporati in e-mail, documenti MS Office, PDF e file di archivio (ZIP, ALZIP, JAR) e altri tipi di file (con codifica Uuencode, HTML)
- File scaricati tramite URL e perfino link FTP
- URL camuffati, falsificati, abbreviati e reindirizzati in modo dinamico
- Indirizzi URL per furto delle credenziali e typosquatting
- Immagini di sistemi operativi Microsoft Windows e Apple macOS X, vulnerabilità di browser e applicazioni sconosciute
- Codici dannosi incorporati in e-mail di spear-phishing

Sebbene gli attacchi con ransomware inizino con un'e-mail, per crittografare i dati è necessario eseguire una callback a un server di comando e controllo. Email Security identifica e blocca le campagne malware multifase difficili da rilevare.

Rilevamento ottimizzato delle minacce

Email Security permette di minimizzare il rischio di costose violazioni, identificando e isolando attacchi avanzati, mirati e altri attacchi evasivi camuffati come normale traffico. Una volta rilevati, questi attacchi vengono immediatamente fermati, analizzati e schedati, per semplificare l'identificazione delle minacce in futuro.

Alla base di Email Security si trovano Advanced URL Defense, il motore MVX e MalwareGuard. Queste tecnologie sfruttano machine learning e analytics per identificare gli attacchi che eludono le tradizionali difese basate su firma e criteri.

Parte integrante di Advanced URL Defense, PhishVision è un motore di classificazione delle immagini che sfrutta algoritmi di deep learning per compilare e confrontare acquisizioni di schermate di marchi attendibili e comunemente utilizzati, a fronte delle pagine Web indicate negli URL dell'e-mail. In tandem con PhishVision, Kraken è un plug-in di rilevamento phishing che applica analytics di dominio e contenuti della pagina per potenziare il machine learning. Skyfeed, un ulteriore avanzamento tecnologico in quanto a rilevamento degli URL, è un sistema di acquisizione intelligence sui malware completamente automatizzato creato appositamente. Vengono analizzati account di social media, blog, forum e feed in quanto a minacce, per scoprire i falsi negativi. La sfaccettata natura di Advanced URL Defense offre alle organizzazioni protette da Email Security una difesa impareggiabile dagli attacchi di raccolta delle credenziali e spear-phishing.

MalwareGuard è un'utility di machine learning che prende in input i file binari e produce in output un punteggio di sospettosità. Ogni file PE (Portable Executable) rilevato viene analizzato da MalwareGuard. In base al punteggio viene presa una decisione e ai rilevamenti attivati da MalwareGuard viene assegnato un nome.

Il motore MVX rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica, senza firma in un ambiente sicuro e virtuale. Identifica exploit mai visti prima e malware, per fermare l'infezione ed evitare compromissioni.

Minimizzazione dell'evasione

Email Security supporta una funzionalità in tempo reale controllata per difendere da attacchi che evadono le richieste per oggetti remoti. Il motore MVX rileva i malware che richiedono diversi download e restituisce gli oggetti remoti richiesti dai file binari di esempio. La modalità in tempo reale controllata riduce i falsi negativi per i download multifase, gli attacchi avanzati di spear-phishing e le intrusioni avanzate ransomware.

Gli aggressori inoltre tentano di eludere la tecnologia utilizzata per rilevare gli URL sospetti. Nell'ambito di Advanced URL Defense, le contromisure alle elusioni per i siti di phishing sono in costante evoluzione. La minimizzazione delle elusioni è costantemente ottimizzata come parte di Advanced URL Defense. Altra tecnologia per ridurre le elusioni, Guest Images può essere personalizzato per interpretare un end-point "usato" quando viene eseguito un oggetto potenzialmente dannoso. Molte tecniche evasive vengono bloccate garantendo che Guest Image riproduca un dominio end-point, un utente di dominio, dati di Outlook e la cronologia del browser.

Integrazione per migliorare l'efficienza di gestione degli avvisi

Email Security analizza ogni allegato e-mail e URL per individuare con precisione gli attacchi avanzati attualmente in circolazione. Gli aggiornamenti in tempo reale dell'intero ecosistema di sicurezza FireEye, unitamente all'attribuzione degli avvisi ad autori di minacce noti, forniscono il contesto necessario per dare priorità e rispondere agli avvisi critici, oltre a bloccare gli attacchi via e-mail avanzati. Le minacce note, sconosciute e non imputabili a malware sono individuate in modo semplice e con pochissimi falsi positivi, in modo tale da indirizzare le risorse verso gli attacchi reali al fine di ridurre le spese operative. La categorizzazione del riskware separa reali tentativi di violazione da attività indesiderabili ma meno dannose (come adware e spyware) stabilire l'ordine di priorità per le risposte agli avvisi.

Rapido adattamento all'evoluzione delle minacce

Email Security permette alle organizzazione di adattare costantemente la propria difesa proattiva da minacce via e-mail, sfruttando intelligence sulle minacce in tempo reale dal cloud FireEye Dynamic Threat Intelligence (DTI). L'intelligence accurata su minacce e aggressori combina informazioni di intelligence su attacchi, macchine e vittime per:

- Visibilità immediata e più ampia
- Identificazione di capacità e caratteristiche specifiche del malware rilevato e degli allegati dannosi
- Accesso a informazioni contestuali per stabilire le priorità e accelerare la risposta
- Determinazione della probabile identità e delle motivazioni di un hacker e monitoraggio delle sue attività all'interno dell'azienda
- Riscrittura di tutti gli URL incorporati in un'e-mail per proteggere gli utenti da collegamenti nocivi
- Individuazione retroattiva degli attacchi di spear-phishing e prevenzione dell'accesso a siti di phishing grazie alla segnalazione di indirizzi URL dannosi

Integrazione delle attività di risposta

Email Security funziona senza problemi con FireEye Helix e FireEye Central Management.

- Come componente della piattaforma operativa di sicurezza — FireEye Helix — offre visibilità nell'intera infrastruttura. FireEye Helix correda le e-mail e gli avvisi di terze parti con informazioni, correlazione a endpoint, automazione e suggerimenti investigativi. Grazie a queste capacità, FireEye Helix rileva minacce invisibili e consente agli esperti di prendere decisioni.
- 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.
- Central Management supporta il tagging basato su ruoli per sapere chi viene preso di mira.
- Central Management supporta la risposta agli avvisi e la correzione secondo criteri basati su ruoli.

Capacità supplementari

Personalizzazione tramite regole YARA

Email Security consente agli analisti di specificare e testare le regole personalizzate di analisi degli allegati in cerca di minacce specifiche per l'azienda.

Protezione da impersonificazione di dirigenti

Email Security - Server Edition offre la possibilità di bloccare le compromissioni di e-mail aziendali (Business Email Compromises, BEC) per proteggere dalla falsificazione dei dipendenti più importanti dell'azienda. Viene creato un criterio che confronta i nomi visualizzati dell'e-mail in arrivo con un elenco approvato corrispondente ai mittenti approvati.

Gestione di code di messaggi, avvisi e quarantena

Email Security - Server Edition offre un elevato livello di controllo sui messaggi e-mail che analizza. Per distribuzioni attive in modalità protetta, i messaggi possono essere tracciati e gestiti durante lo spostamento lungo la coda MTA. Gli attributi delle e-mail possono essere utilizzati per cercare messaggi e verificare che siano stati ricevuti, analizzati e consegnati all'hop successivo. Inoltre, è possibile monitorare nel tempo i trend utilizzando una dashboard intuitiva. Elenchi espliciti di autorizzazione e blocco forniscono un controllo personalizzato sull'elaborazione di e-mail. che consente di ricercare e selezionare attributi di avvisi comuni. Inoltre, è possibile eseguire operazioni in massa su avvisi e messaggi posti in quarantena.

Modalità di protezione attiva o solo di monitoraggio

Email Security può analizzare le e-mail e mettere in quarantena le minacce per garantire una protezione attiva. Per implementazioni di solo monitoraggio, le aziende devono impostare solamente una regola CCN trasparente per inviare copie delle email a Email Security per l'analisi.

Opzioni di distribuzione flessibili
Email Security - Server Edition offre varie opzioni di implementazione, per soddisfare le esigenze e il budget di ogni 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 Email Security è una piattaforma di facile gestione che può essere implementata 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 di e-mail 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.

  Il bursting da un'appliance hardware integrata su MVX Smart Grid offre una capacità aggiuntiva di rilevamento e analisi delle minacce tramite e-mail durante i periodi di picco del throughput dei messaggi.
- **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.

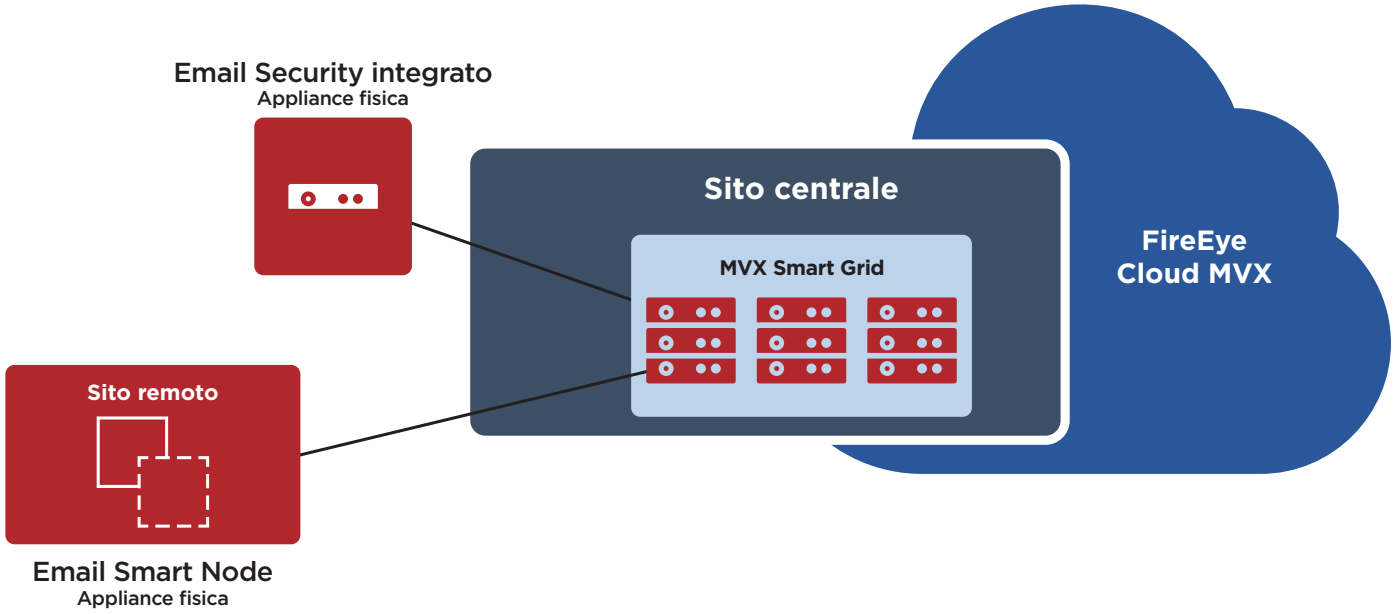

Figura 2. Modelli di bursting e implementazione distribuiti per Email Security.

Tabella 1. Caratteristiche tecniche.

	EX 3500	EX 5500	EX 8500
Prestazioni*	Fino a 700 allegati unici all'ora	Fino a 1800 allegati unici all'ora	Fino a 2650 allegati unici all'ora
Porte interfacce di rete	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporto di 10GigE in fibra, 10GigE in rame, 1GigE in rame), 2x 1GigE BaseT
Porte di gestione	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Monitoraggio IPMI	Incluso	Incluso	Incluso
Porta VGA (pannello posteriore)	Incluso	Incluso	Incluso
Porte USB (pannello posteriore)	4x USB Tipo A posteriore	2x USB Tipo A anteriore, 2x USB Tipo A posteriore	2x USB Tipo A anteriore, 2x USB Tipo A posteriore
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	4x 2TB, RAID 10, HDD 3,5 pollici, FRU	4x 2TB, RAID 10, HDD 3,5 pollici, FRU	4x 2TB, RAID 10, HDD 3,5 pollici, FRU
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) 750 watt, 100 - 240 VCA, 9 – 4,5 A, 50-60 Hz, ingresso IEC60320-C14, FRU	Ridondante (1+1) 800 watt, 100 - 240 VCA, 9 – 4,5 A, 50-60 Hz, ingresso IEC60320-C14, FRU	Ridondante (1+1) 800 watt, 100 - 240 VCA, 9 – 4,5 A, 50-60 Hz, ingresso IEC60320-C14, FRU
Alimentatore CC	Non disponibile	Non disponibile	Non disponibile
Potenza termica massima	245 watt (836 BTU all'ora)	456 watt (1556 BTU all'ora)	530 watt (1808 BTU all'ora)
MTBF (h)	54.200 ore	57.401 ore	53.742 ore
Peso sola appliance/con confezione, kg (lb)	13,6 kg (30 lb)/18,6 kg (41 lb)	20,0 kg (44,1 lb)/29,6 kg (65,3 lb)	20,2 kg (44,4 lb)/29,8 kg (65,6 lb)
Sicurezza e conformità	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Conformità EMC	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015	FCC Parte 15 ICES-003 Classe A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 e V-3/2015
Certificazioni di sicurezza	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Conformità ambientale	Direttiva RoHS 2011/65/UE; REACH; Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE; REACH; Direttiva RAEE 2012/19/UE	Direttiva RoHS 2011/65/UE; REACH; Direttiva RAEE 2012/19/UE
Temperatura operativa	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)
Umidità operativa relativa	10 ~ 95% @ 40 °C, senza condensa	10 ~ 95% @ 40 °C, senza condensa	10 ~ 95% @ 40 °C, senza condensa
Altitudine operativa	3.000 m	3.000 m	3.000 m

* Tutti i dati relativi alle prestazioni variano in base alla configurazione di sistema e al profilo del traffico di e-mail elaborato. Dimensioni dell'appliance basate su allegati unici per ora.

Tabella 2. Specifiche FireEye MVX Smart Grid.

	VX 5500	VX 12500
Sistema operativo supportato	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Prestazioni*	Fino a 480 allegati unici all'ora	Fino a 3.780 allegati unici all'ora
Disponibilità elevata**	N+1	N+1
Porte di gestione (pannello posteriore)	1 porta 10/100/1000 Mbit/s BASE-T	1 porta 10/100/1000 Mbit/s BASE-T
Porte cluster (pannello posteriore)	3 porte 10/100/1000 Mbit/s BASE-T	1 porta 10/100/1000 Mbit/s BASE-T, 2 porte 10 Gb/s BASE-T
Porta IPMI (pannello posteriore)	Incluso	Incluso
LCD frontale e tastierino numerico	Non disponibile	Incluso
Porte VGA	Incluso	Incluso
Porte USB (pannello posteriore)	4 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
Capacità unità	2 unità HDD 2TB 3,5 pollici SAS, RAID 1, collegabile a caldo, FRU	4 unità HDD SAS3 da 3,5" da 4 TB, RAID 1, FRU
Involucro	1RU, Rack 19 pollici	2RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	17. 437 x 650 x 43,2 mm (2 x 25,6 x 1,7 pollici)	437 x 851 x 89 mm (17,2 x 33,5 x 3,5 pollici)
Alimentatore CC	Non disponibile	Non disponibile
Alimentatore CA	Ridondante (1+1) 750 watt, 100-240 VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, ingresso, collegabile a caldo, FRU	Ridondante (1+1) 800 W: 100-127 V, 9,8 A - 7 A 1000 W: 220-240 V, 7-5 A, 50-60 Hz, FRU ingresso IEC60320-C14, FRU
Consumo energetico massimo	285 watt	760 watt
Dissipazione termica massima	972 BTU all'ora	2594 BTU all'ora
MTBF	54.200 ore	38.836 ore
Peso sola appliance / con la confezione	15 kg (33 lb)/21,8 kg (48 lb)	21 kg /40,2 kg
Certificazione di sicurezza	FIPS 140-2 Livello 1, CC NDPP v1.1	FIPS 140-2 Livello 1, CC NDPP v1.1
Conformità alle normative sulla sicurezza	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* Tutti i dati relativi alle prestazioni variano in base alla configurazione di sistema e al profilo di traffico elaborato.

** Con apposite configurazioni di hardware ridondante.

Tabella 3. FireEye Email Security smart node, specifiche virtuali dei sensori.

	EX 5500V
Sistema operativo supportato	Microsoft Windows, Apple macOS X
Prestazioni*	Fino a 1250 allegati unici all'ora
Porte per il monitoraggio della rete	2
Porte per la gestione della rete	2
CPU Cores	8
Memoria	16 GB
Capacità unità	384 GB
Adattatori di rete	VMXNet 3, vNIC
Supporto Hypervisor	VMWare ESXi 6.0 o successivo

* Tutti i dati relativi alle prestazioni variano in base alla configurazione di sistema e al profilo di traffico elaborato.

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, Inc.
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 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.