



FireEye Email Security Cloud Edition

**Protezione su cloud che identifica, analizza e blocca
gli attacchi via e-mail**



CARATTERISTICHE PRINCIPALI

- Garantisce una protezione completa delle e-mail contro attacchi di spear phishing e altri sofisticati attacchi multifase e zero-day, così da spam e virus
- Analizza le e-mail per verificare la presenza di minacce nascoste nei file, compresi gli allegati protetti da password e crittografati e indirizzi URL pericolosi
- Rileva automaticamente e riduce o previene del tutto il furto delle credenziali
- Fornisce informazioni contestuali per stabilire l'ordine di priorità degli avvisi e contenere le minacce
- Si integra con Office 365, Google Mail e una serie di tecnologie FireEye
- Utilizzato in modalità di protezione attiva o di solo monitoraggio
- Soddisfa i requisiti di sicurezza FedRAMP ed è conforme alla certificazione SOC 2 di Tipo II



“Perché crediamo veramente che FireEye Email Security garantisca la protezione che cerchiamo. Non perdiamo tempo a combattere contro eventuali attacchi”.

Shaun Guthrie
Direttore dell'IT
Go Auto

Panoramica

Le e-mail rappresentano il vettore per attacchi informatici più vulnerabile, in quanto sono il punto di ingresso con il maggior volume di dati. Le aziende devono affrontare un numero crescente di minacce come lo spam via e-mail, i virus e le minacce avanzate. La maggior parte delle minacce arriva per e-mail, sotto forma di allegati di file nocivi, link pericolosi, frodi per il trasferimento di denaro e phishing delle credenziali. Sebbene i software anti-spam e antivirus siano in grado di individuare i tradizionali attacchi di phishing di e-mail di massa con allegati noti, link e contenuti pericolosi, essi non riescono a rilevare attacchi di spear-phishing specifici e sofisticati, ideati per aggirare queste soluzioni legacy. Le e-mail rimangono il metodo principale per avviare un attacco avanzato o distribuire ransomware, in quanto possono essere altamente specializzate e adattate per migliorare le possibilità di sfruttamento.

FireEye Email Security aiuta le aziende a minimizzare il rischio di costose violazioni. Implementato sul cloud, rileva accuratamente attacchi avanzati mirati, compresi spear phishing e ransomware, ed è in grado di interromperli all'istante prima che possano accedere al vostro ambiente. Email Security utilizza il motore Multi-Vector Virtual Execution™ (MVX) senza firme per analizzare gli allegati e gli indirizzi URL di e-mail rispetto a una vasta gamma di sistemi operativi, applicazioni e web 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 in prima persona sulle violazioni e l'utilizzo di milioni di sensori. Email Security utilizza queste prove reali e queste informazioni contestuali per stabilire l'ordine di priorità degli avvisi e bloccare le minacce in tempo reale.

Email Security si integra con FireEye Network Security per offrire una maggiore visibilità al fine di coordinare la protezione in tempo reale contro gli attacchi lanciati da vettori misti.

Efficace rilevamento delle minacce

Email Security è un'efficace soluzione di protezione dalle minacce informatiche che aiuta le aziende 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 e-mail.

Alla base di Email Security vi è il motore MVX, che controlla il traffico di e-mail sospette per identificare attacchi che eludono i sistemi di difesa tradizionali basati su criteri e firme. Il motore MVX rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica, senza firma in un ambiente sicuro e virtuale. Interrompe le fasi di infezione e compromissione della catena di attacchi informatici identificando exploit e malware mai visti prima.

Email Security - Cloud Edition è disponibile con protezione anti-spam e antivirus per rilevare attacchi comuni che utilizzano metodi convenzionali di corrispondenza della firma.

Difesa contro le minacce dalle e-mail

Poiché tutte le informazioni personali sono disponibili online, un criminale informatico è in grado di utilizzare tecniche di ingegneria sociale per convincere l'utente a cliccare su un indirizzo URL o ad aprire un allegato.

Email Security offre funzioni di rilevamento e prevenzione in tempo reale da attacchi di spear-phishing, ransomware, sostituzione dell'utente e furto delle credenziali che eludono con facilità i sistemi di difesa tradizionali. Riduce il furto delle credenziali con il rilevamento dei domini "simili ma diversi" (typosquatting).

Se un attacco viene confermato, Email Security mette in quarantena le e-mail dannose per analizzarle più approfonditamente o per eliminarle. Esegue un'analisi per malware nascosti in:

- Tutti i tipi di allegato, tra cui EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3 e MP4 e archivi ZIP/RAR/TNEF
- Allegati protetti da password e crittografati
- Indirizzi URL integrati in e-mail
- Indirizzi URL per furto delle credenziali e typosquatting
- SO sconosciuti e vulnerabilità di browser e applicazioni
- 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.

Risposta efficiente agli avvisi

Email Security analizza ogni allegato e indirizzo 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, e bloccare le e-mail di spear phishing. 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.

Rapido adattamento all'evoluzione delle minacce

Email Security aiuta la vostra azienda ad adattare costantemente il vostro sistema di difesa proattiva contro attacchi via e-mail in base alle informazioni dettagliate raccolte su minacce e hacker. Oltre alle informazioni su attacchi, macchine e vittime si ottengono i benefici seguenti:

- 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
- Individuazione retroattiva degli attacchi di spear-phishing e prevenzione dell'accesso a siti di phishing grazie alla segnalazione di indirizzi URL dannosi

Le aziende hanno accesso al portale di Email Security per visualizzare avvisi in tempo reale e generare report.

Semplice distribuzione e protezione per l'intera azienda

Email Security - Cloud Edition è basato sul cloud e non necessita dell'installazione di alcun hardware o software. È ideale per le imprese che intendono trasferire la propria infrastruttura di posta elettronica sul cloud. In questo modo si elimina la complessità legata all'acquisizione, installazione e gestione di un'infrastruttura fisica.

Email Security - Cloud Edition si integra perfettamente con sistemi di posta elettronica basati sul cloud quali Microsoft Office 365 con Exchange Online Protection e Google Mail.

Per garantire protezione dalle e-mail dannose, le aziende devono semplicemente indirizzare i messaggi a Email Security, che analizzerà prima le e-mail per verificare la presenza di spam e virus noti. Dopodiché utilizza la "camera di combustione" senza firme, il motore MVX, per analizzare ogni allegato e indirizzo URL, rilevare eventuali minacce e bloccare gli attacchi avanzati in tempo reale.

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. Le aziende semplicemente aggiornano i propri record MX per indirizzare i messaggi a FireEye. Per il solo monitoraggio, è sufficiente configurare una regola BCC trasparente per inviare copie delle e-mail a FireEye per l'analisi da parte di MVX.

Integrazione delle attività di risposta

Email Security funziona con altre varie soluzioni FireEye 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.
- La piattaforma FireEye Helix funziona perfettamente con Email Security ed è stata progettata per semplificare, integrare e automatizzare le operazioni di sicurezza.

Certificazioni di conformità

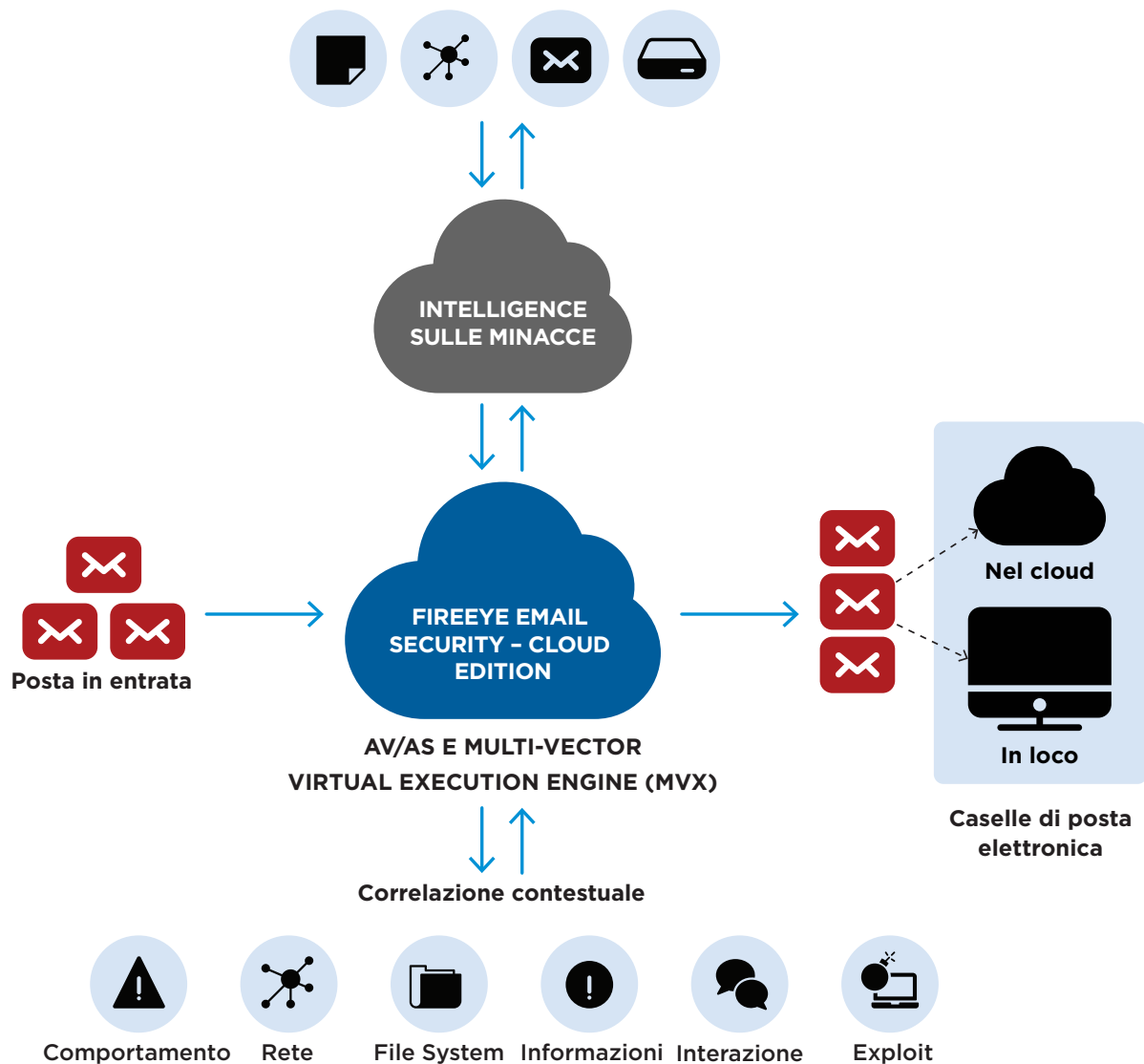
FedRAMP

Email Security - Cloud Edition soddisfa i requisiti di sicurezza FedRAMP per i servizi cloud gestiti da enti governativi e istituti di istruzione pubblica.

SOC 2 Tipo II

Email Security - Cloud Edition rispetta la certificazione di sicurezza e riservatezza di Tipo II di Service Organization Controls (SOC 2) dell'American Institute of Certified Public Accountants (AICPA).

FireEye Email Security - Cloud Edition



Per ulteriori informazioni su FireEye, visitare il sito: www.FireEye.com

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

© 2018 FireEye, Inc. Tutti i diritti riservati.
FireEye è un marchio registrato di FireEye, Inc.
Altri marchi, nomi di prodotto e servizi sono o possono essere rivendicati come proprietà di terzi. DS.ETP.IT-IT-022018

Informazioni su FireEye, Inc.

FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Funendo 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 i costi indiretti della cibersicurezza 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% del Forbes Global 2000.

