SCHEDA TECNICA

FireEye Email Security Cloud Edition

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

CARATTERISTICHE PRINCIPALI

- Garantisce una sicurezza completa delle e-mail in entrata e in uscita
- Consolida lo stack di sicurezza della posta elettronica con una soluzione unica e completa per il fornitore
- Supporta le regole YARA personalizzate per migliorare l'efficacia del rilevamento delle minacce
- Attiva la correzione automatica di Office 365 per rimuovere le e-mail che diventano dannose dopo la consegna
- Si integra con qualsiasi provider di posta elettronica di terze parti
- Fornisce una conoscenza approfondita degli attacchi e degli aggressori da indagini di prima linea e dalle osservazioni degli avversari
- Soddisfa i requisiti di sicurezza FedRAMP

"Le e-mail sono fondamentali per tutti gli ambienti collaborativi, per cui la distribuzione di FireEye Email Security ci offre la possibilità di mitigare i rischi di compromissione da questo canale altamente sfruttato utilizzando un'unica soluzione."

Nils Göldner
Managing Partner e Consulente Cloud
Blackboat GmbH

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 malware e le minacce avanzate. La maggior parte delle minacce arriva per e-mail, sotto forma di URL di collegamento a siti di phishing delle credenziali, richieste fraudolente di trasferimento di denaro e allegati di file nocivi. La natura altamente vulnerabile e personalizzabile delle e-mail permette ai criminali informatici di attaccare frequentemente tramite questo vettore, rendendolo il bersaglio principale per i crimini cibernetici.

FireEye Email Security può ridurre i costi e aumentare la produttività dei dipendenti attraverso un'unica soluzione di sicurezza e-mail che minimizza il rischio di costose violazioni causate da attacchi e-mail avanzati. Implementato nel cloud, FireEye Email Security è un gateway di posta elettronica sicuro con funzionalità complete leader di settore nell'identificare, isolare e interrompere immediatamente gli attacchi basati su URL, impersonificazione e allegati, prima che entrino nell'ambiente aziendale. Grazie alla funzione di correzione automatica di Office 365 (O365), è possibile estrarre le e-mail che diventano dannose dopo la consegna nella casella di posta di un utente. FireEye Email Security analizza anche il traffico e-mail in uscita per evitare minacce avanzate, spam e virus.

Sfrutta una reale piattaforma scalabile big data per scoprire URL dannosi grazie a una confluenza di plug-in contestuali e di rilevamento basati sull'intelligence. Nomi dei mittenti e indirizzi e-mail sono controllati in quanto ad autenticità e i contenuti vengono vagliati per evitare le tattiche di impersonificazione e fermare CEO fraud e altri attacchi malware. Il motore Multi-Vector Virtual Execution™ (MVX) senza firme analizza gli allegati di e-mail e gli indirizzi URL rispetto a un'ampia struttura a matrice multipla di sistemi operativi, applicazioni e browser web. 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 utilizza queste prove reali e queste informazioni contestuali sugli attacchi e i malintenzionati per stabilire l'ordine di priorità degli avvisi e bloccare le minacce in tempo reale.

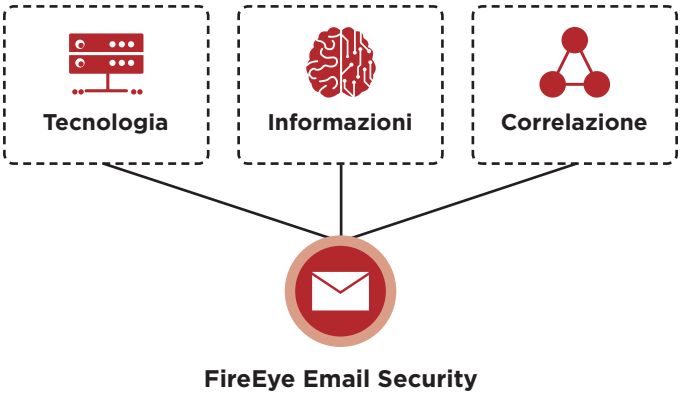

Figura 1. Un gateway di posta elettronica sicuro.

Integrando FireEye Network 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 le informazioni personali sono prontamente 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 protezione in tempo reale da attacchi di raccolta delle credenziali, impersonificazione e spear-phishing, che tipicamente eludono con facilità i servizi 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 e MP4 e archivi ZIP/RAR/TNEF
- Allegati protetti da password e crittografati
- URL incorporati in email, PDF e documenti di Microsoft Office
- 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.

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 e il motore MVX. Queste tecnologie sfruttano machine learning e analytics all'avanguardia 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 e di accesso 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. Ulteriore avanzamento tecnologico in quanto a rilevamento degli URL, Skyfeed è un sistema di acquisizione intelligence sui malware completamente automatizzato e creato appositamente. Vengono analizzati account di social media, blog, forum e feed sulle minacce, per individuare 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.

Un'e-mail potrebbe inizialmente essere benigna per superare le difese informatiche. Solo dopo essere stata consegnata nella casella di posta di un utente diventa effettivamente dannosa. Email Security—Cloud Edition esegue l'analisi in maniera retroattiva e segnala quando un'e-mail diventa dannosa dopo essere stata consegnata. Tramite l'API O365, le e-mail che diventano retroattivamente dannose possono essere estratte automaticamente dalla casella di posta creando un criterio di correzione automatica di O365.

Il motore MVX rileva attacchi zero-day, multi-flusso e altri attacchi evasivi con analisi dinamica e 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.

Protezione AVAS ottimizzata

Email Security—Cloud Edition è disponibile con protezione anti-spam e antivirus (AVAS) per rilevare attacchi comuni che utilizzano metodi convenzionali di corrispondenza della firma, oltre alle tecniche di impersonificazione.

Gli attacchi di impersonificazione, noti anche come CEO fraud (spesso detti anche compromissione dell'e-mail aziendale o Business Email Compromises, BEC) continuano a influire significativamente sulle aziende a livello finanziario. Questo è dovuto in parte alle carenze dei tradizionali indicatori di minacce per elementi quali allegati nocivi o collegamenti, dato che gli attacchi sono privi di malware e si basano su tecniche di ingegneria sociale. Per combattere tali minacce e proteggere i clienti, FireEye ha sviluppato innovativi algoritmi, sistemi e strumenti specializzati nel rilevamento e nella difesa da impersonificazione.

Un indicatore comune di un attacco e-mail è l'età del dominio del mittente. Quando creano campagne di impersonificazione, i criminali informatici inviano le e-mail di attacco da un dominio simile a quello della persona o dell'azienda che stanno impersonando, solitamente dopo poche ore dalla creazione di quel dominio.

Email Security è in grado di determinare con precisione l'età e la maturità di un dominio sfruttando strumenti sviluppati internamente, Newly Existing Domains (NED) e Newly Observed Domains (NOD). I domini identificati come appena creati vengono trattati come sospettosi e controllati approfonditamente per altri indicatori di attacco, come typosquatting e spoofing del nome visualizzato o del nome utente del mittente.

Invece di dover acquistare e registrare un dominio, i criminali informatici possono cambiare semplicemente il nome visualizzato o il nome utente del mittente, rendendo l'aspetto dell'e-mail simile a una fonte attendibile. Email Security difende dallo spoofing del mittente, determinando l'autenticità del nome visualizzato e del nome utente tramite l'identificazione del nome descrittivo.

Scansione in uscita

Email Security rileva minacce avanzate sconosciute, inclusi allegati dannosi e URL di phishing recapitati tramite messaggi di posta elettronica in uscita. Il traffico di posta elettronica in uscita viene anche scansionato per ricercare malware e spam al fine di proteggere i domini di un'organizzazione e non essere messi in lista nera.

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.

Rapido adattamento all'evoluzione delle minacce

Email Security aiuta le aziende ad adattare costantemente il sistema di difesa proattiva contro attacchi via e-mail. Email Security crea la propria intelligence sulle minacce invece di affidarsi a feed terze parti, spesso in ritardo. L'intelligence sulle minacce specifica per le e-mail in loco (o Smart DNS), le capacità di raccolta dei dati, gli esperti della sicurezza e-mail e gli analisti delle minacce costituiscono l'infrastruttura base per tecnologie anti-spam ottimizzate e il rilevamento dell'impersonificazione. 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
- Offerta di informazioni contestuali per dare 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 riscrittura di indirizzi URL dannosi

Le aziende hanno accesso al portale di Email Security per visualizzare avvisi in tempo reale, creare regole personalizzate intelligenti e generare report. Le regole personalizzate intelligenti permettono alle aziende di creare criteri e regole in base a svariate condizioni granulari.

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.

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 G Suite.

Per garantire protezione dalle e-mail dannose e fraudolente, le aziende devono semplicemente indirizzare i messaggi a Email Security, che analizzerà prima le e-mail per verificare la presenza di spam, malware noti e tattiche di impersonificazione. Dopodiché utilizza la tecnologia di difesa da URL e 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.

Capacità supplementari

Personalizzazione tramite regole YARA

Email Security consente agli analisti di utilizzare le regole YARA personalizzate per gestire e migliorare i rilevamenti, bloccare le minacce più recenti e identificare le campagne in corso.

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.

Certificati di autorizzazione e conformità

ISO 27001
Email Security—Cloud Edition soddisfa lo standard per la sicurezza delle informazioni ISO 27001 che garantisce la gestione in sicurezza dei data center.

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

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

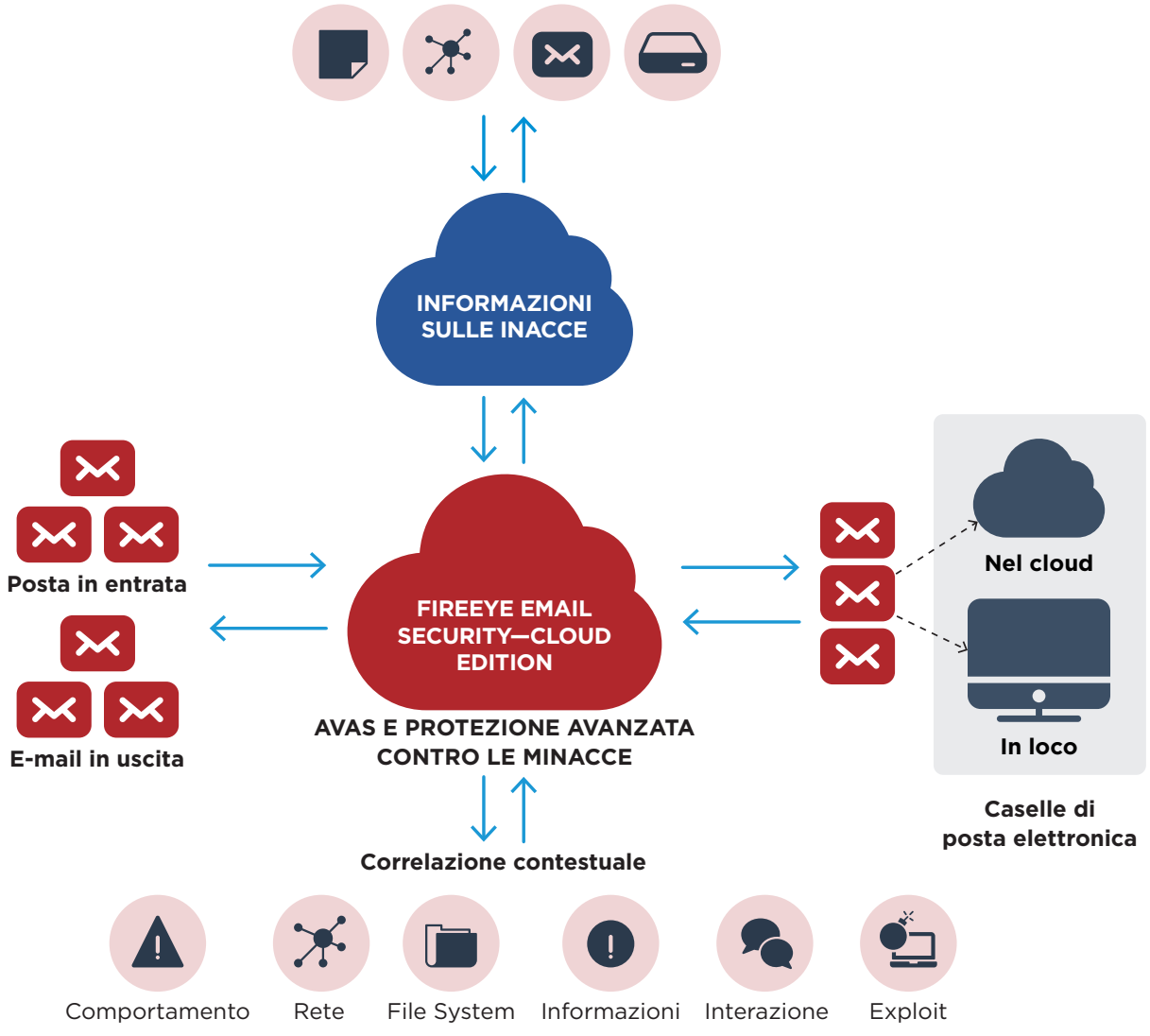

Figura 2. FireEye Email Security – Cloud Edition.

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl.
Piazza IV Novembre, 7
20124 Milano, Italia
+39 0294750535
italy@FireEye.com

A proposito di FireEye Italia Srl.
FireEye è l'azienda di sicurezza guidata dalle informazioni. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.