McAfee Email Gateway

Protezione per le email dell'azienda

Principali vantaggi

Protezione completa in entrata e in uscita

- Totale sicurezza in ingresso contro tutte le minacce veicolate dai messaggi email
- Crittografia delle email incorporata
- Modelli incorporati per la conformità e prevenzione delle fughe di dati per contrastare la fuoriuscita di informazioni sensibili

Sicurezza, gestione e scalabilità avanzate

- Disponibile come appliance virtuale, appliance hardware, server blade o soluzione ibrida integrata con McAfee SaaS Email Protection
- Gestione centralizzata, ricerca dei messaggi, reportistica e quarantena
- Il clustering e il bilanciamento integrato del carico hanno caratteristiche di scalabilità in grado di soddisfare le esigenze più impegnative per i sistemi in sede

Sfruttate tutti i vantaggi di Security Connected attraverso il software McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee Global Threat Intelligence (McAfee GTI), McAfee Advanced Threat Defense e l'approccio ibrido alla sicurezza del traffico email.

Dell'email non si può fare a meno, ed è uno dei servizi più essenziali in qualsiasi ambiente aziendale. Per la sua capacità di distribuire un'ampia gamma di carichi di informazioni superando confini organizzativi, geografici e politici, rappresenta uno strumento fondamentale ma anche una sfida formidabile per la sicurezza. McAfee® Email Gateway aiuta a migliorare la sicurezza del sistema di posta elettronica e a consolidare le difese con protezione contro le minacce in ingresso, prevenzione della fuga di dati verso l'esterno, crittografia, conformità avanzata e amministrazione centralizzata in un'unica appliance semplice da distribuire.

Problemi di sicurezza dell'email

Prendiamo in esame le principali problematiche per la sicurezza dei messaggi email che le aziende si trovano ad affrontare oggi:

- Gli attacchi tramite email in ingresso sono sempre più opera di criminali organizzati alla ricerca di informazioni da sfruttare a scopo di lucro. Gli attacchi utilizzano tecniche sofisticate di social engineering e si trasformano rapidamente per eludere le difese convenzionali basate sulle firme.
- L'email è uno dei principali vettori per il furto o la fuga di dati riservati e sensibili, sia a opera di dipendenti con buone intenzioni ma distratti, sia a opera di utenti interni malintenzionati.
- Data la sua importanza sul piano operativo e la sua vulnerabilità diffusa, l'email è diventata oggetto di osservazione da parte degli organi di controllo al di là dei confini politici e del settore. Le disposizioni interessano il mondo delle carte di pagamento (PCI DSS), dei servizi finanziari (GLBA), della sanità (HIPAA) e tutte le aziende statunitensi quotate in borsa (SOX).
- Circa il 75% del volume globale dei messaggi email è rappresentato da spam, con differenze nette tra i vari Paesi. Lo spear phishing sta diventando più mirato, a scopo di lucro e più efficace che mai.
- McAfee Labs ha identificato circa 2.250 URL di phishing al giorno nel 4° trimestre 2013, valore rimasto costante per tutto l'anno.

Perché accontentarsi di difese frammentate e inadeguate?

I moderni sistemi di difesa del traffico email aziendale si sono evoluti e, in particolare, la maggior parte delle soluzioni di sicurezza esistenti si concentra esclusivamente sui messaggi in entrata, senza offrire alcuna protezione contro la fuga di dati in uscita. Ciò significa che esistono difese costituite da varie tipologie di soluzioni singole non integrate — antimalware, antispam, antiphishing, antivirus, crittografia, prevenzione delle fughe di dati — acquisite da fornitori diversi, distribuite separatamente e ridimensionate a più riprese. Molte non soddisfano gli attuali standard consigliati in termini di prestazioni.

intel Security

Premi 2013

- Leader, Quadrante Magico Gartner per gateway e-mail protetti.
- Leader, Forrester Wave per la sicurezza dei contenuti email.
- Cinque stelle, Migliore acquisto per *SC Magazine*, migliore protezione dei contenuti email.
- Innovatori del settore: Protezione dei dati, *SC Magazine*.

Mentre le principali soluzioni antispam raggiungono una precisione di almeno il 99% nel rilevamento dello spam, molte soluzioni di protezione per l'email arrivano al massimo al 95%. Se una differenza del 4% può sembrare trascurabile, essa si traduce nella realtà in una differenza del 400% nella penetrazione dello spam e nelle potenziali infezioni dei sistemi. Quando lo spam viene misurato nell'ordine dei miliardi di email, un aumento del 4% può incidere in modo significativo sull'azienda, sovraccaricando l'infrastruttura di posta e assottigliando la larghezza di banda. Quando anche una piccola parte delle email indesiderate penetra nelle difese, controllare e cancellare lo spam può diventare una distrazione per gli utenti. Le opportunità per le infezioni malware aumentano, portando a un incremento dei costi, a una perdita di produttività e alla potenziale fuga di dati.

Il risultato inevitabile è che la maggior parte dei reparti IT impiega troppo tempo e denaro per mantenere difese non integrate, evitare la fuoriuscita di informazioni sensibili, dimostrare la conformità alle normative e rimediare alle conseguenze di una protezione inadeguata del traffico email. A livello aziendale, questi sono tutti argomenti molto convincenti a favore di una soluzione di sicurezza email completa che integri difese in ingresso e in uscita, semplifichi l'amministrazione e ottimizzi la conformità: il suo nome è McAfee Email Gateway.

Protezione completa per le email

Sicurezza leader del mercato

McAfee Email Gateway integra protezione avanzata contro le minacce in ingresso con funzioni di prevenzione delle fughe di dati in uscita, conformità e crittografia email avanzate, prestazioni elevate, reportistica e amministrazione unificata, il tutto su un'unica piattaforma inattaccabile a un prezzo tutto compreso.

- Combinando informazioni di rete locali e dati di intelligence globale sulla reputazione forniti da McAfee GTI, McAfee Email Gateway offre la protezione più completa attualmente disponibile contro minacce, spam e malware in ingresso.
- La scansione dei link al momento del clic dell'utente con funzioni di emulazione del comportamento da parte di McAfee Gateway Anti-Malware Engine blocca gli attacchi che utilizzano URL malevoli come catalizzatori.
- L'integrazione con McAfee Advanced Threat Defense consente di rilevare il malware più sofisticato e sfuggente grazie a un'innovativa combinazione di analisi del codice statica e dinamica (in una sandbox).
- Le raffinate tecnologie di scansione dei contenuti, le tecniche di crittografia multiple e la gestione capillare dei messaggi basata su policy evitano la fuga dei dati in uscita e semplificano la conformità.
- La piena integrazione con il software McAfee ePO garantisce la gestione completa della soluzione, all'interno dei singoli cluster o fra più cluster, con funzionalità di registrazione e reportistica di livello aziendale che semplificano i carichi amministrativi e di conformità per ridurre in modo significativo i costi.

Protezione completa contro le minacce in ingresso

McAfee Email Gateway identifica e blocca lo spam in ingresso con una precisione di oltre il 99%, garantendo contemporaneamente protezione integrata contro virus, malware, phishing, directory harvesting, attacchi denial of service (DoS) e bounceback. Previene le minacce zero-hour, gli attacchi mirati e misti e riduce drasticamente l'impatto delle ondate di spam mediante una efficace combinazione di funzioni di classificazione dinamica dello spam e di risposta alle minacce. McAfee Email Gateway fornisce gli aggiornamenti utilizzando informazioni sulla reputazione di mittente, messaggistica e URL provenienti da McAfee GTI.

È incluso anche un motore antivirus secondario per aiutare i clienti a garantirsi una protezione multilivello contro il malware e a soddisfare i requisiti di conformità.

La scansione dei link al momento del clic dell'utente blocca gli attacchi in evoluzione.
McAfee ClickProtect, una funzione di McAfee Email Gateway, elimina le minacce che si celano negli URL incorporati nei messaggi email. Rileva gli eventuali cambiamenti nelle intenzioni dell'URL fra il momento in cui il messaggio viene esaminato (momento della scansione), indipendentemente dalla sua apparente innocuità, e il momento in cui l'URL viene selezionato (momento del clic). Questa doppia ispezione prevede sia il controllo della reputazione dell'URL, sia l'emulazione proattiva, che sfrutta la stessa tecnologia antimalware per gateway di McAfee Web Protection, leader nel settore. Gli amministratori possono configurare policy sia per il momento della scansione, sia per il momento del clic dell'utente e abilitare l'emulazione degli URL per proteggere gli utenti dal clic. Safe Preview offre una rapida anteprima delle pagine successive, sfruttando le informazioni utente degli utenti come livello supplementare di sicurezza. Per impedire del tutto l'accesso al Web attivato da messaggi email, gli URL si possono rilevare ed eliminare completamente, oppure sostituire con un testo esplicativo.

McAfee Advanced Threat Defense rileva il malware sofisticato e sfuggente.
McAfee Advanced Threat Defense individua i moderni tipi di malware zero-day furtivi con un approccio innovativo su più livelli. Il prodotto abbina analisi statica approfondita e analisi dinamica (sandboxing) del codice per esaminare il comportamento effettivo del malware.
La stretta integrazione fra McAfee Email Gateway e McAfee Advanced Threat Defense permette di condurre l'analisi sui file sospetti allegati alle email, bloccando quelli malevoli prima ancora che giungano in una casella di posta.

Mentre metodi con un'intensità analitica inferiore come le firme e l'emulazione in tempo reale sono vantaggiosi sul piano delle prestazioni, l'aggiunta dell'analisi statica completa del codice al sandboxing offre informazioni dettagliate per la classificazione del malware, amplia la protezione contro le minacce elusive particolarmente ben mimetizzate e permette l'identificazione del malware associato che sfrutta il riutilizzo del codice. Percorsi di esecuzione ritardati o imprevisti, spesso non eseguiti in un ambiente dinamico, possono essere rilevati attraverso la decompressione e l'analisi statica completa del codice.

Insieme, l'analisi statica e dinamica del codice forniscono una valutazione completa e informazioni dettagliate come una sintesi del comportamento, la gravità del malware, le associazioni ad altre famiglie di malware, i percorsi di esecuzione e la percentuale di codice eseguita durante l'analisi dinamica.

Il filtraggio della graymail riduce ulteriormente la quantità di posta indesiderata.
La posta indesiderata potrebbe essere formata da grandi volumi di messaggi legittimi, richiesti inizialmente dagli utenti ma ormai non più desiderati (ad esempio newsletter di settore e notifiche). Anche se in genere non è considerata spam, la graymail può risultare molto fastidiosa per i destinatari. L'applicazione di filtri per abilitare azioni come il blocco e la quarantena aiuta a mantenere le caselle di posta pulite.

Protezione completa della posta in uscita per garantire la sicurezza dei contenuti
Con funzione di crittografia delle email.
La crittografia delle email basata su policy è prevista come funzione standard integrata e abbina tecnologie business-to-business (TLS, S/MIME e OpenPGP) e business-to-consumer (push o pull), garantendo anche ai destinatari sprovvisti di funzioni di crittografia la possibilità di ricevere messaggi email sicuri e di rispondervi. La tecnologia push/pull include un client Webmail personalizzabile con il marchio aziendale e permette di recuperare e visualizzare i messaggi crittografati su dispositivi mobili. L'implementazione della crittografia in corrispondenza del gateway anziché del desktop solleva gli utenti dalla necessità di stabilire i requisiti per crittografare i messaggi ed evita il problema diffuso della mancata crittografia dei dati sensibili.

Conformità e prevenzione delle fughe di dati
Un'altra funzione standard integrata è una nutrita raccolta di modelli di conformità incorporati, gli stessi che sono presenti in McAfee Data Loss Prevention. Fingerprinting, analisi lessicale e tecniche di clustering integrano funzioni di corrispondenza di parole chiave e schemi per garantire un rilevamento completo sia dei dati strutturati, sia di quelli non strutturati. Il gateway identifica con precisione i contenuti soggetti a regolamentazione (HIPAA, SOX, GLBA), le informazioni che consentono l'identificazione personale come carte di credito, codice fiscale, dati identificativi specifici di alcuni Paesi e altri dati di clienti e dipendenti. È possibile rilevare e trattare anche dati non strutturati e proprietà intellettuale come codice sorgente, brevetti, informazioni finanziarie e business plan.
Una volta effettuato il rilevamento, il sistema è predisposto per un'ampia gamma di azioni basate su policy tra cui crittografia forzata (di tipo push, pull e TLS), avvisi, reindirizzamento, quarantena, blocco e altre azioni personalizzate.

Poteri amministrativi completi
McAfee Email Gateway aiuta gli amministratori a garantire la massima protezione per l'email e a documentarla grazie a funzioni di reportistica di livello aziendale, registri esportabili completi, dashboard e avvisi configurabili in tempo reale e reportistica approfondita. Combina prestazioni, scalabilità e stabilità con un modello di distribuzione flessibile per garantire il massimo ritorno sull'investimento con costi amministrativi minimi. La soluzione può essere gestita interamente dalla console amministrativa di McAfee Email Gateway o dal software McAfee ePO e inoltre offre:

Controlli sofisticati dell'utilizzo e delle policy che semplificano l'amministrazione.
- Interfaccia agile e intuitiva con installazione e configurazione guidate.
- Integrazione directory/LDAP (Lightweight Directory Access Protocol).
- Gestione centralizzata della sicurezza email, completa di imposizione sistematica delle policy, ricerca di messaggi e registri dettagliati delle conversazioni.
- Reportistica in tempo reale, con dashboard interattive e funzionalità di reportistica approfondite.

Architettura avanzata che garantisce prestazioni elevate.
- Scansione asincrona basata sulla memoria.
- Clustering e bilanciamento del carico integrati per un'elevata disponibilità.
- La funzione on-box o McAfee Quarantine Manager, estremamente scalabile, fornisce servizi di quarantena consolidati per varie appliance McAfee Email Gateway e code di quarantena personalizzate; inoltre, riduce i carichi di lavoro per archiviazione ed elaborazione con una capacità di 1,5 milioni di messaggi, con supporto fino a 200.000 utenti.

Certificazioni e supporto
- Certificazione Common Criteria livello EAL2+, compresa la conformità NDPP.
- Convalida e certificazione software FIPS 140-2 L1.
- Supporto per Common Access Card (x.509).
- Supporto IPv6.

Semplicemente a prova di futuro: protezione email completa per qualsiasi azienda

Flessibilità d'implementazione

McAfee Email Gateway può essere implementato come appliance hardware (in quattro diverse dimensioni), come computer virtuale o in un'architettura di server blade. Questa flessibilità garantisce protezione a un prezzo conveniente e scalabilità per gli ambienti di messaggistica aziendale più esigenti. Inoltre, McAfee Email Gateway fa parte di McAfee Email Protection, che consente di distribuire la soluzione di sicurezza email come gateway email in loco (hardware o virtuale), come Security-as-a-Service (SaaS) su cloud o come combinazione ibrida integrata con un unico prezzo di abbonamento.

Le aziende che desiderano sfruttare i vantaggi del cloud ma preferiscono mantenere il controllo in locale possono utilizzare la soluzione ibrida integrata, che utilizza McAfee Email Gateway come centro di controllo per la gestione delle policy cloud e in locale, la reportistica consolidata, la ricerca dei messaggi e la quarantena. Uno scenario tipico per un'implementazione ibrida è un'azienda che desidera bloccare i contenuti pericolosi o indesiderati ai limiti della rete, ridurre l'utilizzo della larghezza di banda e gestire le informazioni sensibili e la crittografia da un'appliance in sede.

Security Connected

L'infrastruttura Security Connected aiuta i clienti a migliorare i piani per la sicurezza, ottimizzarli per una maggior efficacia dei costi e allineare la sicurezza in modo strategico con le iniziative aziendali. L'integrazione con il software McAfee ePO riunisce le funzioni di gestione e reportistica all'interno delle soluzioni di sicurezza e fra le varie soluzioni. McAfee Global Threat Intelligence (McAfee GTI), che sfrutta l'intera gamma di soluzioni McAfee, acquisisce informazioni collettive da ogni possibile vettore di minacce protetto da McAfee. Le informazioni e i dati di intelligence correlati vengono condivisi con i prodotti e le soluzioni McAfee. In questo modo la protezione del traffico email offerta da McAfee, divisione di Intel Security, dispone sempre delle informazioni più recenti, aggiornate all'ultimo minuto. McAfee Advanced Threat Defense rileva le moderne forme di malware zero-day occulto e si integra perfettamente con vari prodotti, compreso McAfee Email Gateway. Operando come risorsa condivisa fra più soluzioni, McAfee Advanced Threat Defense è scalabile su tutta la rete a costi contenuti e riduce al minimo le spese operative.

Con questa soluzione vi garantite funzioni di livello aziendale per gestire i carichi di lavoro più pesanti e intensivi, il tutto con esigenze di supervisione amministrativa e spese minime. La sua combinazione esclusiva di funzionalità, prestazioni, affidabilità e prezzo adeguato fa di McAfee Email Gateway la soluzione di sicurezza per l'email preferita da oltre la metà dei reparti IT delle aziende Fortune 500. Ulteriori informazioni sulle soluzioni McAfee Email Gateway sono disponibili all'indirizzo **www.mcafee.com/fr/products/email-and-web-security/email-security.aspx**.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com