



# McAfee SaaS Email Protection and Continuity

**Protezione delle email, controllo degli accessi e della conformità per una maggiore produttività**

**Protezione delle email e dell'accesso alle email in tutta semplicità**

Le funzionalità principali di McAfee SaaS Email Protection and Continuity comprendono:

- Filtraggio IP perimetrale per bloccare le minacce prima che raggiungano la tua rete
- Protezione avanzata contro spam, graymail e frodi
- Scansione a più livelli contro virus e worm per bloccare il 100 per cento di tutti i virus conosciuti
- Protezione dagli attacchi via email
- Filtraggio e applicazione delle policy sui messaggi e sugli allegati in uscita
- Massima continuità del sistema di messaggistica
- Gestione delle policy di gruppo
- Audit messaggi, monitoraggio messaggi e strumento smaltimento messaggi
- Opzione: McAfee SaaS Email Encryption

Affronta la sicurezza della posta elettronica con McAfee® SaaS Email Protection and Continuity. Oltre a bloccare spam, phishing, malware, graymail (ovvero notifiche che intasano la casella di posta) e contenuti inappropriati delle email prima che raggiungano la rete, questo servizio basato su cloud applica le policy di posta in uscita per proteggerti dalle fughe di dati. Affidati alla continuità della posta elettronica e la tua azienda potrà accedere alle email 24 ore su 24. Senza hardware da acquistare, nessun software da installare e con aggiornamenti automatici per la protezione dalle minacce più recenti, potrai concentrarti su come rendere più sicuro il tuo business, anziché sull'esecuzione delle applicazioni.

Le email sono il motore della produttività di oggi; i messaggi di posta elettronica che attraversano ogni giorno i server di qualsiasi azienda si contano a migliaia. Gestire le email per garantire la sicurezza e la connettività è divenuto un compito gravoso che distoglie continuamente le risorse IT da attività più strategiche per il raggiungimento degli scopi aziendali.

**Protezione delle email a basso costo e di facile gestione**

La soluzione McAfee SaaS Email Protection and Continuity è facile da implementare e impedisce alle minacce via email in entrata e in uscita di incidere negativamente sulla tua rete e sugli utenti, mantenendo un accesso continuo alla posta elettronica in ogni circostanza. Questa soluzione di sicurezza di tipo Software-as-a-Service (SaaS) è sempre attiva e aggiornata e non richiede alcun investimento aggiuntivo a livello di tempo e risorse per la configurazione e la gestione. Poiché il servizio blocca lo spam e le minacce via email prima che queste si infiltrino nella rete,

il carico di lavoro che grava sui tuoi server di posta è sensibilmente ridotto. Di conseguenza, puoi risparmiare molta larghezza di banda e spazio di memorizzazione sul server. Inoltre, l'avanzata assistenza clienti di McAfee 24/7 garantisce un supporto costante a portata di telefono.

**Semplifica amministrazione e reportistica basate su web.**

Nella singola console di gestione basata su web centralizzata e intuitiva, le best practice sono già integrate e gli aggiornamenti delle policy per le email sono semplici da gestire nelle tue sedi e nei tuoi domini, permettendoti di liberare risorse IT e di abbassare il costo totale di proprietà. Gli amministratori possono configurare e applicare le policy, che comprendono regole di filtraggio dei contenuti e regole sui contenuti degli allegati. È possibile applicare le policy a livello globale per gruppi di utenti o singoli individui per la massima flessibilità. Le informazioni complete contenute nei rapporti, nei registri e nella quarantena forniscono una visibilità ottimale.



### **Sicurezza e continuità delle email conveniente e gestibile**

- Nessun componente hardware o software da acquistare, gestire o aggiornare
- Nessun esborso di capitale iniziale
- Nessun costo di configurazione o aggiornamento
- Attivazione e sincronizzazione automatiche per la più completa continuità
- Semplice gestione via web
- Assistenza clienti 24/7 senza costi aggiuntivi
- Certificazione ISO 27001

### **Continuità delle email semplificata per proteggere la reputazione, le attività e la produttività della tua azienda**

- Attivazione automatica del servizio quando viene riscontrata un'interruzione dell'attività
- Accesso alle email ricevute durante un periodo di interruzione dell'attività attraverso un'interfaccia web sicura
- Completa funzionalità della posta elettronica, incluse le operazioni di lettura, scrittura, risposta, inoltre ed eliminazione
- Sincronizzazione intelligente dell'attività della posta elettronica dopo un periodo di interruzione
- Notifiche di interruzione dell'attività e aggiornamenti del sistema
- Filtraggio dei messaggi in entrata e in uscita

### **Infrastruttura solida e affidabile**

La nostra strategia SaaS prevede la gestione di più centri dati in quattro continenti. Ogni centro dati è dotato di certificato ISO 27001 e fornisce la ridondanza completa grazie ad hardware ridondante active-active su tutti i livelli della rete: firewall, router e switch per il bilanciamento del carico. All'interno di ogni data center forniamo inoltre servizi di monitoraggio automatizzati di reti e applicazioni, offrendo al personale addetto alle operazioni da remoto la visibilità necessaria su avvisi di situazioni sospette e guasti, con esperti di sicurezza impegnati 24/7 nella supervisione dei sistemi.

### **Sicurezza email inattaccabile**

#### **Godi di una protezione antispam di classe superiore.**

Il nostro sistema di rilevamento dello spam Stacked Classification Framework, basato su una tecnologia brevettata, si applica a più livelli di analisi per determinare la probabilità che un'email sia spam, a prescindere dalla lingua del messaggio. Poiché ciascuna tecnologia di filtraggio ha dei punti di forza unici per identificare delle minacce specifiche, compreso lo spam basato su immagini, la combinazione consente di ottenere uno dei processi di filtraggio più precisi e completi del settore

La funzione di reputazione dei messaggi di McAfee Global Threat Intelligence (McAfee GTI) ispeziona ogni messaggio per rilevare le minacce conosciute ed emergenti basate su messaggi, quali lo spam, anche se provengono da una fonte affidabile come ad esempio un sistema infetto all'interno di un'azienda inserita nella whitelist. La classificazione si basa non solo sulle informazioni di intelligence raccolte da tutti i sensori che presentano le richieste nel cloud McAfee e sull'analisi eseguita dai ricercatori e dagli strumenti automatici di McAfee Labs, ma anche sulla correlazione delle informazioni di intelligence tra vettori da file, web e dati sulle minacce alla rete. Ciò permette di bloccare o mettere in quarantena le email in modo più efficiente e preciso e massimizzare così le prestazioni.

### **Il filtraggio per i messaggi graymail mantiene libera le caselle della posta elettronica in arrivo.**

La posta indesiderata potrebbe essere una mail massiva legittima richiesta a suo tempo dall'utente ma ora non più desiderata (per esempio, newsletter di settore e notifiche). Utilizzando i filtri graymail gli amministratori possono impostare delle policy graymail per individui o per gruppi e addirittura possono permettere agli utenti finali di abilitare questa funzione per mantenere le caselle di posta libere da posta indesiderata.

### **Scansione multilivello per bloccare efficacemente i virus e i worm.**

McAfee SaaS Email Protection and Continuity include la nostra tecnologia brevettata di rilevamento dei worm WormTraq. Esegue la scansione in cerca di malware sia nel corpo dei messaggi che in tutti gli allegati, utilizzando il nostro avanzato motore antivirus basato su firme che sfrutta l'approccio McAfee GTI. Oltre a bloccare gli attacchi della posta in entrata, è altrettanto importante filtrare le email in uscita per proteggere i client contro il malware.

### **La scalabilità completa protegge la tua azienda dagli attacchi email su vasta scala.**

La nostra soluzione completa difende la tua rete e i gateway di messaggistica strategici dagli attacchi via email, bloccando istantaneamente gli attacchi di tipo denial of service e altri attacchi basati su SMTP, inclusi gli attacchi directory harvesting, email bombing e channel flooding.

### **La crittografia TLS (Transport Layer Security) integrata protegge le comunicazioni intra-aziendali.**

Per le aziende che richiedono un livello di sicurezza maggiore per le email in entrata e in uscita, il nostro protocollo TLS accetta e filtra i messaggi cifrati in entrata e in uscita, include la convalida dell'autorità di certificazione TLS e distribuisce le email attraverso un tunnel sicuro.

### **Compatibile con Microsoft Office 365 e Google Apps for Business**

#### **Ulteriori informazioni**

Per ulteriori informazioni sui vantaggi a livello di risparmio di tempo, produttività e sicurezza offerti da tutte le nostre soluzioni SaaS, tra cui McAfee SaaS Email Protection and Continuity, visita il nostro sito web all'indirizzo <http://www.mcafee.com/it/products/security-as-a-service/index.aspx>.

### **La soluzione di email continuity è sempre attiva, in ogni circostanza.**

L'attività non si ferma quando le reti di posta elettronica non funzionano. Se la rete non è accessibile a causa di un disastro naturale, di un blackout o di operazioni di manutenzione ordinaria, McAfee SaaS Email Protection and Continuity mantiene attiva la connessione di dipendenti, clienti, partner e fornitori con una copertura 24/7. La nostra interfaccia web sicura e facile da usare consente agli utenti di inviare e ricevere i messaggi con protezione costante, cercare e recuperare i messaggi archiviati e gestire le cartelle di quarantena e gli archivi dei messaggi.

### **Regole preimpostate, scansione avanzata del contenuto e fingerprinting dei documenti incluse.**

Hai a disposizione funzionalità avanzate di prevenzione della fuga di dati (DLP) e di conformità che sfruttano le tecnologie leader del settore fornite da McAfee. Oltre a McAfee SaaS Email Protection and Continuity, con McAfee SaaS Email Encryption puoi accedere a regole integrate basate sul contenuto per PCI DSS, settore sanitario, informazioni finanziarie, normative locali sulla privacy ecc. con cui creare rapidamente policy di conformità. Scansione e protezione di oltre 300 tipi di documenti per tutelare l'azienda da fughe di dati in uscita.

La tecnologia avanzata di fingerprinting dei documenti permette di creare e memorizzare fingerprint digitali di documenti selezionati per addestrare la funzione di sicurezza email a riconoscere il tipo di contenuto soggetto a policy.

Le policy possono essere applicate in modo granulare per la corrispondenza totale o parziale del contenuto delle email e degli allegati. È possibile utilizzare anche la tecnologia basata su espressioni regolari per parole chiave e frasi.

### **La crittografia push/pull è facile da utilizzare.**

McAfee SaaS Email Encryption ti consente di cifrare le informazioni sensibili, anche se il destinatario non dispone di una soluzione di crittografia. Una tecnologia di tipo push/pull di facile utilizzo progettata per gli utenti business e disponibile anche su dispositivi mobili protegge i dati da occhi indiscreti.

### **Protezione, gestione e conformità ottimizzate grazie a Security Connected**

L'unificazione delle diverse componenti semplifica la gestione e assicura che le soluzioni di sicurezza siano strettamente collegate tra loro, in modo da ridurre al minimo le curve di apprendimento e fornire visibilità in tempo reale da un unico punto di osservazione. L'intera suite di soluzioni McAfee SaaS può essere gestita tramite una console unica.

### **È tempo di cambiare**

Scopri come puoi ridurre al minimo la manutenzione e liberare le risorse del tuo personale IT, permettendogli di concentrarsi su progetti più strategici. Per saperne di più e registrarti per una prova gratuita, visita [www.mcafeesaas.com](http://www.mcafeesaas.com).



**McAfee. Part of Intel Security.**

Via Fantoli, 7  
20138 Milano  
Italia  
(+39) 02 554171  
[www.intelsecurity.com](http://www.intelsecurity.com)

Intel e il logo Intel sono marchi registrati di Intel Corporation negli Stati Uniti e/o in altri Paesi. McAfee e il logo McAfee sono marchi registrati o marchi di McAfee, Inc. o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. I piani, le specifiche e le descrizioni dei prodotti contenuti nel presente documento hanno unicamente scopo informativo, sono soggetti a variazioni senza preavviso e sono forniti senza alcun tipo di garanzia, esplicita o implicita. Copyright © 2014 McAfee, Inc. 60166ds\_saas-protect-continuity\_0313B\_fnL\_ETMG