

Protezione dei messaggi di Google



INFORMAZIONI SULLA SICUREZZA E SULL'ARCHIVIAZIONE DI GOOGLE

I servizi di sicurezza e archiviazione di Google, powered by Postini, garantiscono la protezione e la conformità del sistema email esistente. Basati su una piattaforma di servizio ospitata, questi prodotti bloccano spam, phishing, malware e altre intrusioni prima che colpiscano la rete e consentono la gestione e l'archiviazione dei contenuti in base ai requisiti legali. Il modello ospitato di Google offre diversi vantaggi precisi. Sfruttando l'“effetto rete” di decine di migliaia di reti email, la tecnologia Google rileva le nuove minacce in tempo reale e le blocca sull'intera rete di sicurezza Google, senza bisogno di aggiornamenti in sede. Allo stesso modo le economie di scala dell'archiviazione, la distribuzione semplice e l'assenza di manutenzione per il servizio garantiscono un costo totale di proprietà basso.

Per ulteriori informazioni, consultare il sito www.google.com/postini

Protezione dei messaggi di Google, powered by Postini, garantisce una protezione efficacissima delle email in entrata e in uscita per le organizzazioni di tutte le dimensioni. Semplifica la gestione della sicurezza e della conformità dei messaggi e libera risorse IT preziose. Poiché questo servizio è sempre attivo e aggiornato, le aziende sono sicure di disporre sempre di una protezione efficace e affidabile della posta.

Basato su un'architettura on demand brevettata, Protezione dei messaggi di Google blocca spam, phishing, virus e altre minacce email prima che colpiscano l'organizzazione, riducendo il carico sui server email, conservando la larghezza di banda e migliorando le prestazioni dell'infrastruttura di messaggistica esistente. Questo servizio viene fornito in un modello Software as a Service (SaaS) che consente di risparmiare denaro e risorse IT perché non vi sono hardware o software da installare e mantenere.

Protezione dei messaggi di Google conserva le risorse IT eliminando la patch e gli aggiornamenti costanti richiesti da altri dispositivi o altre soluzioni software. Riduce inoltre il carico dell'help desk IT consentendo agli utenti finali di gestire la quarantena e le impostazioni delle email con un'interfaccia intuitiva, basata sul Web. Piuttosto che chiamare il servizio di assistenza, gli utenti finali possono esaminare i messaggi in quarantena e distribuire quelli desiderati. Gli utenti ricevono periodicamente un'email riepilogativa della quarantena con i relativi dettagli. Sono inoltre in grado di ottimizzare le impostazioni antispam in base a livelli personalizzati. Tutti questi controlli degli utenti finali sono completamente configurabili a livello di norme e offrono il controllo completo su ciò che gli utenti sono autorizzati a fare.

Protezione dei messaggi di Google può applicare automaticamente le norme di sicurezza dell'email. In questo modo garantisce la conformità legale e normativa per i messaggi in entrata e in uscita nell'intera organizzazione. Il supporto TLS (Transport Layer Security) incluso consente di crittografare le comunicazioni email sensibili e può essere automaticamente applicato a tutte le comunicazioni tra i domini email designati.



Figura 1: Protezione dei messaggi di Google garantisce una protezione efficacissima delle email in entrata e in uscita per le organizzazioni di tutte le dimensioni

Ne risulta che le comunicazioni sensibili e regolate vengono sempre distribuite con il livello di protezione appropriato.

Protezione dei messaggi di Google fornisce inoltre una console Web pratica per l'amministrazione. Questa console consente di eseguire in tempo reale la configurazione, la modifica delle norme, il monitoraggio e l'allerta, nonché generare rapporti esaurienti per gli amministratori. Gli utenti possono essere definiti nella console oppure Protezione dei messaggi di Google può essere integrato nella struttura organizzativa di directory per la sincronizzazione degli utenti.

Protezione dei messaggi di Google combina più componenti per garantire una protezione efficace dalle minacce email. Di seguito sono descritte alcune funzionalità specifiche.

- L'identificazione in tempo reale delle minacce, basata sull'elaborazione di oltre due miliardi di messaggi email al giorno, fornisce una visibilità globale delle minacce emergenti. Questo "effetto rete" identifica e rileva automaticamente gli indirizzi IP da cui hanno origine attacchi quali spam, virus, DoS (Denial of Service), ecc. Non appena viene individuata una minaccia, questa viene bloccata per tutti i clienti di Protezione dei messaggi di Google. L'identificazione delle minacce comporta anche la correzione automatica. Man mano che gli indirizzi IP identificati interrompono l'attacco sono di nuovo autorizzati a stabilire connessioni SMTP (Simple Mail Transfer Protocol) per inviare messaggi email legittimi.
- La tecnologia antispam in tempo reale brevettata esamina migliaia di elementi di un messaggio email per determinare se si tratta di spam. Fornisce un filtro antispam estremamente efficace e una percentuale di falsi positivi eccezionalmente bassa.
- La protezione antivirus si basa sulla rilevazione antispam e include metodi di rilevazione euristica e basata sulla firma "zero-hour", nonché diversi motori antivirus commerciali.
- La gestione dei contenuti consente di definire le norme per i messaggi in entrata e in uscita e fornisce un ulteriore livello di protezione dalle minacce esterne. Garantisce inoltre la protezione da fughe accidentali o intenzionali di dati riservati nelle email in uscita e nei relativi allegati.
- La tecnologia di gestione degli allegati permette di definire norme specifiche relative agli allegati di file e consente il blocco o la messa in quarantena dei messaggi a seconda dei tipi o delle dimensioni dei file allegati. La gestione degli allegati consente inoltre di esaminare i file di archivio, ad esempio .zip e .rar, per valutare il contenuto dei file e definire norme specifiche per l'amministrazione dei file di archivio crittografati.

PROTEZIONE DEI MESSAGGI DI GOOGLE

Funzionalità	Vantaggi
Architettura pass-through brevettata	Filtro antispam estremamente efficace e percentuale di falsi positivi bassa
Blocco dei virus multilivello, rilevazione euristica e basata sulle firme	Protezione "zero-hour" dai virus in rapido mutamento SLA antivirus totale
Piattaforma SaaS estremamente scalabile e disponibile, SLA tempo di attività del filtro pari al 99,999%	Protezione sempre attiva e sempre aggiornata con un costo totale di proprietà ridotto
Console di amministrazione basata sul Web	Possibilità di aggiornamenti in tempo reale di utenti e norme, modifiche alla configurazione e generazione di rapporti
Blocco di attacchi directory harvest/Denial of Service	Prevenzione degli attacchi con un'analisi brevettata del comportamento
Crittografia TLS basata sulle norme	Protezione della trasmissione di email
Filtraggio degli allegati	Applicazione delle norme degli allegati email
Gestione delle norme per i contenuti	Applicazione di norme di utilizzo accettabili e conformità dei contenuti
Spooling email	Possibilità di continuare a ricevere messaggi email anche in caso di blocco del server email

