Forcepoint

Sintesi della soluzione

Forcepoint Data Loss Prevention for Cloud Email

Protezione e controllo per le e-mail, con la tecnologia DLP più affidabile del settore

Sfida

- Dati sensibili trapelano dalle organizzazioni in quantità crescenti, attraverso molteplici canali.
- L'e-mail è indicata come il vettore di minaccia usato più diffusamente per gli attacchi.
- Proteggere i dati senza ostacolare la produttività aziendale è oggi più importante e complesso che mai.

Soluzione

- Forcepoint estende la soluzione Data Loss Prevention (DLP) più affidabile del settore anche al canale e-mail.
- Monitora accuratamente e previeni le perdite di dati sensibili tramite e-mail.
- Sfrutta una soluzione cloud completamente gestita per adattare la protezione della posta in uscita alle esigenze della tua azienda.

Risultato

- Migliora l'efficienza, riducendo nettamente il numero di falsi positivi riscontrati nelle e-mail
- Migliora la conformità normativa grazie a un numero di policy predefinite triplo rispetto a tutti gli altri fornitori di DLP.
- Migra la tua soluzione DLP su Forcepoint in sole 6 settimane, grazie alla competenza di Forcepoint, alle policy già pronte e al trasferimento di conoscenze all'avanguardia nel settore.

L'importanza della protezione dei dati continua a crescere nelle priorità delle organizzazioni di tutto il mondo. Che i dipendenti lavorino nello spazio confinato di un classico ufficio oppure, com'è oramai la nuova normalità, da remoto o in modalità ibrida, garantire la sicurezza dei dati sui vari canali è diventata una questione sempre più complessa. L'e-mail è un canale critico, sul quale le organizzazioni devono ottenere visibilità e controllo per bloccare esfiltrazioni indesiderate di dati, proprietà intellettuale e file preziosi. Esempi tipici di perdite di dati tramite e-mail includono:

→ **Dati o file aziendali inviati** ad account di posta privati utilizzando l'e-mail di lavoro.

→ **Dati sensibili** che vengono diffusi all'esterno dell'azienda a causa di negligenza o tramite account compromessi.

→ **File e dati sensibili che malintenzionati interni all'azienda** inviano alla concorrenza, a giornalisti e a siti web. Spesso l'intento è quello di commettere una frode, sabotare l'azienda o sottrarre dati proprietari.

→ **Utenti interni in buona fede che, in seguito ad attacchi di phishing e malware oppure di adware e spam,** aiutano inconsapevolmente dei criminali a mettere le mani su dati critici e proprietà intellettuale.

"L'e-mail è il vettore di minacce più utilizzato dai criminali per diffondere il malware tra le organizzazioni. È anche una linea diretta tra utenti e criminali informatici, con e-mail aziendali compromesse e frodi che creano danni nell'ordine di miliardi di dollari ogni anno."

IDC, WORLDWIDE MESSAGING SECURITY MARKET SHARES, 2021: HYBRID WORK DRIVES NEED FOR THREAT INVESTIGATION INTEGRATION, DOC. N. US49144522, GIUGNO 2022

Per le organizzazioni è imperativo avere un'ottima visibilità e uno stretto controllo sulle mail in uscita, in modo da poter proteggere la proprietà intellettuale da attacchi mirati ed esposizioni accidentali. La tecnologia che offre questi risultati è la DLP. Secondo IDC, "Negli ultimi 24 mesi il mercato delle tecnologie di prevenzione delle perdite di dati ha attraversato una fase di rinascita. Tecniche di classificazione oscure e manuali stanno lasciando il posto all'automazione e all'apprendimento automatico. La contestualizzazione ha permesso tutto questo, rendendo le soluzioni molto più efficaci ed efficienti." [1] La sicurezza e-mail, unita ai progressi della DLP, che rileva, protegge e controlla le informazioni sensibili, è essenziale per monitorare le e-mail in quanto vettore importante. In assenza di salde funzionalità DLP, le violazioni della sicurezza e-mail possono nuocere gravemente alla reputazione e all'operatività delle organizzazioni.

I vantaggi di Forcepoint DLP for Cloud Email

Leader tra le soluzioni per la protezione dei dati, Forcepoint DLP for Cloud Email offre una visibilità e un controllo senza precedenti sulle e-mail in uscita. In combinazione con DLP for Endpoints, Cloud, Web e Network, DLP for Cloud Email è una soluzione potente e articolata per proteggere i dati delle organizzazioni. La DLP di Forcepoint è studiata per prevenire la perdita di dati ovunque lavorino i dipendenti e ovunque risiedano i dati.

Identificazione dei dati ad altissima precisione

La DLP di Forcepoint include oltre 1.600 classificatori e modelli predefiniti implementabili velocemente per identificare i dati sensibili. Sfrutta inoltre tecnologie avanzate che fanno uso dell'analisi del linguaggio naturale, dell'apprendimento automatico e di una delle tecnologie di fingerprinting più efficaci del settore per identificare con precisione i dati a riposo, in movimento e in uso. Per la sicurezza dei dati, la visibilità è essenziale e DLP Discover di Forcepoint, oltre a renderli visibili, identifica formalmente i dati consentendo così di controllarli come necessario. Questo aspetto è importante per molteplici motivi:

- → **Conformità.** Forcepoint DLP assicura il rispetto di normative importanti come il GDPR, l'HIPA e molte altre in vigore in oltre 83 paesi, per assicurare alle organizzazioni una conformità costante.
- → **Semplicità.** La creazione e l'implementazione di classificatori conformi alle necessità delle organizzazioni e ai requisiti del business sono molto dispendiose in termini di tempo e risorse per distribuire una soluzione DLP. Con i classificatori e i modelli predefiniti di Forcepoint, le organizzazioni possono distribuire velocemente classificatori specifici per una serie di settori e tipologie di dati, semplificando enormemente la DLP.
- → **Efficienza.** Grazie alla tecnologia completa di identificazione dei dati di Forcepoint, Forcepoint DLP riduce nettamente il numero di falsi positivi, classificando gli incidenti critici da approfondire e definendone la priorità.

Controllo unificato delle policy

Una solida strategia DLP deve proteggere tutti i canali essenziali, come endpoint, cloud, web ed e-mail. Spesso le organizzazioni gestiscono questi canali separatamente, con prodotti DLP diversi e mirati su un singolo canale, ad esempio il cloud o l'e-mail. Con Forcepoint, tutti questi canali vengono protetti con un'unica soluzione e gestiti con le stesse policy. La possibilità di configurare una volta sola per poi distribuire la configurazione più volte ti offre un controllo impareggiabile sui dati aziendali, anche grazie a un'interfaccia unificata da cui monitorare tutti i canali critici esposti al rischio di perdita di dati. L'uso delle policy tramite DLP for Cloud Email ti offre visibilità anche su altri dispositivi, come tablet e telefoni, che le tipiche soluzioni per gli endpoint raramente controllano.

Scalabilità senza precedenti

Forcepoint DLP for Cloud Email ha il vantaggio di essere un servizio completamente gestito nel cloud, con la flessibilità delle risorse tipica delle distribuzioni cloud. Se, ad esempio, in un dato momento si verifica un picco di messaggi in uscita, DLP for Cloud Email ti permette di espandere velocemente le risorse, per poi ridurle in base alla reale necessità del servizio. In più, offre un servizio DLP continuo che risponde alle esigenze in crescita della tua organizzazione senza bisogno di distribuire e configurare hardware aggiuntivo.

Protezione adattiva al rischio

Forcepoint è il primo provider del settore a offrire una soluzione DLP adattiva al rischio. Grazie al monitoraggio costante delle attività degli utenti, la soluzione offre ai dipendenti la massima libertà d'azione per non intralciare la produttività, intervenendo solo quando identifica attività ad alto rischio o schemi ripetuti di comportamenti rischiosi. Grazie all'automazione, tutto avviene quasi in tempo reale: in altre parole, è in grado di anticipare e bloccare una violazione prima che avvenga.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: DLP IS Dead, Long Live DLP, n. doc. US48261521, ottobre 2021

Soluzioni Forcepoint DLP for Cloud Email

DLP for Cloud Email: protezione per i dati in uscita

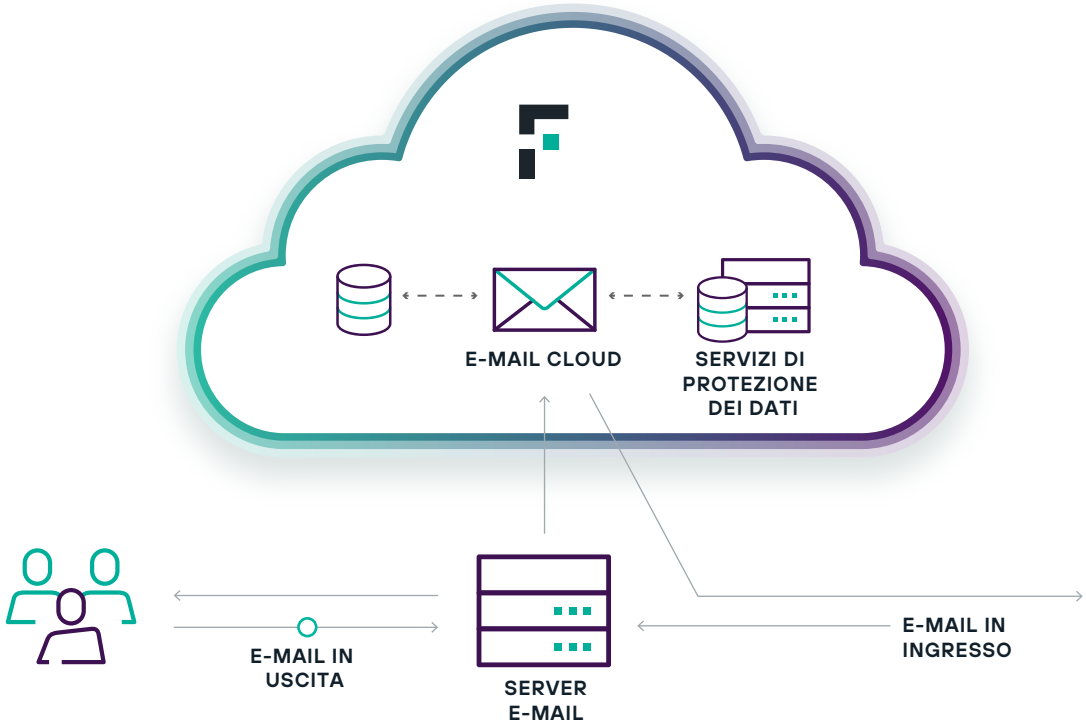
Forcepoint semplifica la distribuzione di DLP for Cloud Email affiancando il fornitore della tua soluzione di sicurezza e-mail corrente per analizzare i messaggi in uscita. Grazie ai connettori universali di DLP for Cloud Email, Forcepoint integra i prodotti dei brand più diffusi, come Google e Microsoft, per l'inoltro di tutte le e-mail in uscita o solo di specifici messaggi a Forcepoint Cloud. Lì, i messaggi vengono esaminati da Forcepoint DLP in base alle azioni e policy DLP (che variano in base al tuo piano DLP predefinito e personalizzato). Prima dell'invio, i messaggi e-mail possono essere autorizzati, messi in quarantena o crittografati (con il modulo di crittografia separato). Quelli messi in quarantena sono segnalati mediante notifica e possono essere conservati fino a un massimo di 30 giorni (in base alla tua configurazione), a meno che non siano rilasciati da un amministratore autorizzato. Per tutelare la reputazione delle organizzazioni, tutti i messaggi in uscita vengono analizzati anche per rilevare eventuali spam, virus e malware.

Funzionalità standard:

- → **Interfaccia semplice per le policy,** che offre protezione da virus, malware e spam
- → **Dashboard, registri e report di presentazione**
- → **Abbonamento e-mail personale**

Componenti aggiuntivi:

- → **Cronologia dei report estesa di Forcepoint Cloud Email** (opzioni per 6, 12 e 18 mesi)
- → **Modulo di crittografia di Forcepoint Email Security**
- → **Modulo di analisi immagini di Forcepoint Email Security**



forcepoint.com/contact