Proofpoint Email DLP e Proofpoint Email Encryption

Protezione degli utenti dagli attacchi che li inducono a inviare informazioni sensibili via email

Vantaggi principali

- Gestione e implementazione centralizzata della prevenzione della perdita di dati e della crittografia delle email sul nostro avanzato gateway email
- Integrazione con la piattaforma Proofpoint Information and Cloud Security e supporto completo di tutti gli scenari di perdita di dati incentrati sulle persone
- Analisi e classificazione delle informazioni riservate all'interno di dati strutturati e non strutturati
- Esperienza utente e mobile trasparente

Conformità

- Oltre 240 classificatori integrati
- Normative PCI, SOX, GLBA, termini per l'insider trading definite dalla SEC e altri modelli internazionali specifici per ogni paese
- GDPR, legge britannica sulla protezione dei dati, direttiva europea sulla protezione dei dati, legge canadese per la protezione delle informazioni personali e dei documenti elettronici, numero di previdenza sociale britannico, numeri delle carte di credito giapponesi
- Codice sulle informazioni personali, legge HIPAA, ICD-9, ICD-10, codice nazionale dei farmaci americano e altri codici sanitari

Proofpoint Email Data Loss Prevention (DLP) e Proofpoint Email Encryption forniscono una visibilità e funzionalità di implementazione uniche senza i costi e la complessità associati a soluzioni disparate. Presentano una classificazione automatica dei dati e una crittografia trasparente che viene gestita centralmente a livello di gateway. Migliorano l'esperienza di amministrazione nella definizione e nell'applicazione delle policy nel tuo ambiente email.

Proofpoint Email DLP e Proofpoint Email Encryption ti offrono un maggior controllo sui dati sensibili, consentendoti di soddisfare meglio i requisiti di conformità. Ti aiutano a proteggere i tuoi utenti dagli attacchi che li inducono a inviare informazioni sensibili via email. L'email è il principale vettore di minaccia per le minacce in entrata, ma è anche un vettore critico per la perdita di dati in uscita.

Proofpoint Email DLP - Prevenzione di potenziali violazioni dei dati

Proofpoint Email DLP classifica accuratamente i dati sensibili e rileva le esfiltrazioni dei dati tramite email. Impedisce la fuoriuscita di dati sensibili dalla tua azienda.

Corrispondenza esatta dei dati

Proofpoint Email DLP include una funzione di corrispondenza esatta dei dati. Questa funzione rileva i dati sensibili che devono essere protetti. Ti permette di caricare facilmente o creare dizionari e identificatori personalizzati, unici per la tua azienda. In questo modo, per esempio, puoi utilizzare i numeri di conto dei servizi finanziari, forme locali di identificazione e numeri delle cartelle cliniche per analizzare i dati più importanti delle email. Puoi anche ampliare i dizionari esistenti con termini e codici personalizzati. Inoltre, puoi utilizzare definizioni basate sull'instradamento per creare delle policy per i flussi di messaggi in entrata e in uscita.

Protezione contro le frodi via email

Proofpoint Email DLP include oltre 240 classificatori ottimizzati. Questi classificatori possono identificare, classificare e bloccare i messaggi che vengono tipicamente utilizzati come parte degli attacchi di violazione dell'email aziendale (BEC, Business Email Compromise). Riducono notevolmente il rischio di inviare a degli impostori documenti personali, informazioni fiscali o bonifici bancari.

Analisi approfondita e analisi delle impronte digitali

Proofpoint Email DLP permette di rilevare con precisione i dati sensibili all'interno di contenuti non strutturati. Con la nostra soluzione è possibile:

- Analizzare oltre 300 tipi di file in modo immediato.
- Garantire il corretto trattamento dei dati sensibili contenuti in allegati in formati diversi da Microsoft Office o PDF.
- Utilizzare il programma per la profilazione del tipo di file per estendere il supporto a tipi di file nuovi, personalizzati o proprietari, inclusi brevetti e promemoria.
- Analizzare l'impronta digitale dei documenti sensibili grazie a funzionalità di corrispondenza completa o parziale, anche se i dati risiedono in file di formati diversi.

Automazione della conformità normativa

Proofpoint Email DLP va ben oltre delle semplici corrispondenze di espressioni regolari. Può utilizzare dizionari pre-costruiti per scoprire rapidamente i dati sensibili esposti. Proofpoint Email DLP offre i seguenti vantaggi:

- Rilevamento estremamente affidabile delle comunicazioni non conformi
- Controlli algoritmici dettagliati integrati negli identificatori intelligenti
- Riduzione dei falsi positivi per i numeri delle carte di credito, i numeri di identificazione e un'ampia gamma di informazioni sensibili
- Analisi avanzata di prossimità e correlazione per il rilevamento ottimizzato di più elementi.

I termini del dizionario possono essere ponderati per aumentare o diminuire il valore di corrispondenza di qualsiasi termine o per consentire delle eccezioni.

Miglioramento dell'efficacia operativa

Integrazione con la piattaforma Proofpoint Information and Cloud Security
Proofpoint Email DLP è integrato con la piattaforma Proofpoint Information and Cloud Security. Questa integrazione permette di unificare le nostre avanzate soluzioni DLP per l'email, il cloud, il web, gli endpoint e i repository di file on premise. La nostra piattaforma combina i dati di analisi dei contenuti, dei comportamenti e delle minacce provenienti da questi canali per consentirti di gestire tutti gli scenari di perdita di dati incentrati sulle persone tramite un'interfaccia unificata di gestione degli allarmi. I classificatori di dati comuni ti consentono di implementare policy DLP coerenti sui diversi canali. In questo modo risparmi tempo prezioso e riduci il carico amministrativo.

Smart Send
La funzione Smart Send permette ai mittenti di correggere le proprie violazioni delle policy per le email in uscita. Questo potente strumento potente facile da amministrare consente di educare gli utenti, liberando al contempo le risorse IT per attività più strategiche. Puoi definire il routing in base alle policy. Puoi anche reindirizzare le risorse sensibili verso l'utente, il team delle risorse umane, il team IT o chiunque altro.

Reportistica in tempo reale
Proofpoint Email DLP fornisce la visibilità e il flusso di lavoro necessari per aiutarti a prendere decisioni rapide e a metterle in pratica. Permette di consultare le statistiche e le tendenze in tempo reale, di gestire gli incidenti in corso e di intraprendere le azioni appropriate in caso di messaggi non conformi. Tutto ciò da una dashboard centralizzata. Questo permette di esaminare in dettaglio tutti gli incidenti visualizzando una vista affiancata di regioni specifiche di un'email di un allegato e identificare gli elementi del contenuto che si discostano dal documento di formazione o dalle policy originarie. Puoi inoltre commentare, tracciare e indagare sulle violazioni nel gestore di incidenti ed esportare i messaggi corrispondenti.

I report grafici mostrano le violazioni nel tempo. Puoi visualizzarle in base a diversi filtri: policy, utente, principali trasgressori per policy, ecc. Puoi visualizzare le tendenze per identificare le aree di successo e le opportunità di miglioramento. I report possono essere inviati tramite email su base programmata. Possono anche essere pubblicati su un sito intranet per risparmiare tempo.

Proofpoint Email Encryption - Crittografia, visibilità e controlli garantiti

Proofpoint Email Encryption è attivata dal motore DLP basato su policy. I suo solidi controlli offrono i seguenti vantaggi:

- Possibilità di definire policy di crittografia
- Applicazione dinamica delle policy a livello globale, di gruppo e di utente attraverso l'integrazione con LDAP o AD
- Possibilità di definire la crittografia in base alla destinazione (puoi, per esempio, includere un partner commerciale, un fornitore, gli attributi del mittente e del messaggio, come i tipi di allegati)

Proofpoint Email Encryption può anche essere utilizzato come TLS di backup. Ciò assicura un meccanismo di crittografia affidabile.

Con Proofpoint Email Encryption puoi:

- Garantire la sicurezza delle tue comunicazioni aziendali.
- Proteggere le comunicazioni tra gruppi o utenti. La soluzione offre funzionalità di crittografia delle comunicazioni interne eliminando la necessità di instradare i messaggi esternamente o di implementare un'altra soluzione che potrebbe essere difficile da adottare.
- Ottenere la revoca granulare delle email crittografate. Ciò permette agli utenti di revocare, far scadere o ripristinare l'accesso a un'email crittografata senza influire sugli altri utenti o altri messaggi indirizzati allo stesso destinatario.

Gestione delle chiavi senza intervento

Puoi eliminare l'onere amministrativo legato alla gestione delle chiavi e concentrarti sulle tue esigenze in termini di crittografia. Le chiavi vengono memorizzate e gestite in modo sicuro man mano che vengono generate. La loro gestione tramite la nostra infrastruttura cloud garantisce inoltre un'elevata disponibilità. Le chiavi vengono memorizzate separatamente dal contenuto delle email al fine di garantire riservatezza e sicurezza.

Esperienza ottimizzata per il destinatario

Fornendo un'esperienza utente trasparente, Proofpoint Email Encryption scoraggia i dipendenti dall'aggirare le policy. Offriamo un'ampia gamma di opzioni per consentire agli utenti di accedere ai messaggi crittografati. Il metodo predefinito utilizza l'interfaccia Secure Reader. Ciò consente all'utente di fare clic su un allegato HTML crittografato dal messaggio. Gli utenti vengono quindi indirizzati al portale web dove possono accedere facilmente al messaggio crittografato. L'altro metodo è conosciuto come Decrypt Assist, progettato per l'accesso mobile. L'accesso è fornito sotto forma di link in un messaggio. Quando gli utenti fanno clic sul link, vengono indirizzati sul portale web ottimizzato per i dispositivi mobili in modo da poter consultare il messaggio cifrato.

Gli utenti possono accedere e gestire i messaggi dalla casella di posta di Secure Reader. In questo modo godono di un'esperienza trasparente quando ricevono un messaggio cifrato. Ciò permette inoltre all'azienda di gestire facilmente i messaggi ricevuti. Il componente aggiuntivo unificato Outlook permette agli utenti di inviare e leggere messaggi crittografati con un solo clic. Inoltre, puoi abilitare la crittografia dei messaggi interni per le comunicazioni sensibili tra i dipendenti.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita la pagina **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it.**