

PANORAMICA SULLA SOLUZIONE

Modernizzare la sicurezza dei dati dell'email con un approccio adattivo

Per godere di una protezione multilivello contro la perdita dei dati via email, adotta Proofpoint Adaptive Email DLP

Vantaggi principali

- Prevenzione della perdita di dati accidentale e intenzionale attraverso l'email
- Riduzione dei rischi di danni alla reputazione e abbandono della clientela
- Riduzione delle sanzioni a seguito di violazioni del Regolamento Generale sulla Protezione dei Dati (GDPR) e della legge CCPA (California Consumer Privacy Act)
- Miglioramento della sensibilizzazione alla sicurezza informatica in tutta la tua azienda

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a mitigare le quattro principali categorie di rischi legati agli utenti.

La perdita di dati sensibili può essere particolarmente dannosa per la tua azienda. Secondo il report *Data Loss Landscape 2024* di Proofpoint, l'85% delle aziende coinvolte ha affermato di aver subito un incidente di perdite di dati nell'anno passato. Per il 50% di tali aziende, gli incidenti hanno causato un'interruzione delle attività. Gli utenti negligenti sono stati menzionati come la causa più comune di perdita di dati.

La prevenzione della perdita dei dati (DLP) via email è un componente essenziale della strategia globale di sicurezza dei dati della tua azienda. Protegge i dati sensibili contro tutte le esposizioni indesiderate tramite email. Un programma efficiente di DLP via email combina analisi dei contenuti, avvisi in tempo reale, applicazione delle policy e formazione degli utenti. Previene la perdita di dati e assicura la tua conformità con i requisiti legali e normativi.

I prodotti tradizionali di DLP via email possono creare basi solide applicando regole e policy definite per i rischi noti. Tuttavia, è possibile migliorare in modo significativo la tua strategia di protezione dei dati dell'email utilizzando un prodotto tradizionale di DLP via email e Proofpoint Adaptive Email DLP. Questa soluzione combinata offre un approccio più dinamico e incentrato sulle persone alla prevenzione della perdita di dati tramite email.

Ecco i vantaggi che l'aggiunta di Proofpoint Adaptive Email DLP alla tua soluzione può offrirti:

Protezione più completa

- **I prodotti tradizionali di DLP via email** mettono l'accento sui contenuti. Forniscono protezione basata su regole contro i rischi noti come l'invio via email di dati sensibili. Sono efficaci nella protezione di dati strutturati noti e ben definiti, tra cui dati a carattere personali, numeri della carta di credito, ecc.
- **Proofpoint Adaptive Email DLP** si concentra sui contenuti. Estende la copertura offerta dalle soluzioni tradizionali di DLP via email per proteggerti anche contro le minacce sconosciute e in costante evoluzione. Proofpoint Adaptive Email DLP si basa sull'IA comportamentale per rilevare i comportamenti insoliti degli utenti. Può rilevare quando un utente invia dati sensibili al destinatario errato, condivide file in un modello insolito o invia email a un account non autorizzato.

Rilevamento adattivo

Proofpoint Adaptive Email DLP utilizza l'IA comportamentale per rilevare l'attività email che differisce dai comportamenti normali degli utenti. La nostra IA non si limita a ricercare dei modelli di dati specifici.

1/3 degli utenti

ha inviato una o due email al destinatario sbagliato.

Fonte: report Data Loss Landscape 2024 di Proofpoint

84%

Email inviate a un indirizzo errato l'anno scorso che contenevano allegati.

Fonte: report Data Loss Landscape 2024 di Proofpoint

50%

Violazioni dovute a un errore che sono state causate dall'invio di email destinatario errato nel 2024.

Fonte: Verizon, 2024 Data Breach Investigations Report (Report sulla violazione dei dati)

>160.000

Email inviate al destinatario errato bloccate da Proofpoint Adaptive Email DLP nel 2024.

Fonte: Proofpoint

Analizza un contesto più ampio, che include:

- Le persone a cui gli utenti inviano abitualmente email
- I tipi di allegati che gli utenti condividono generalmente
- Il modo in cui gli utenti solitamente gestiscono i dati sensibili

Proofpoint Adaptive Email DLP si adatta ai comportamenti dei tuoi collaboratori e alle tendenze dell'email. Rileva potenziali incidenti di perdita di dati anche quando i dati non sono ben definiti. Per esempio, immaginiamo che un collaboratore che normalmente non invia dati finanziari cerchi improvvisamente di inviare un allegato contenente tali informazioni a un contatto esterno non autorizzato. Proofpoint Adaptive Email DLP rileverà l'account email non autorizzato e l'allegato sensibile e farà una segnalazione.

Blocco delle email inviate al destinatario errato

Può accadere che un utente invii per errore un'email alla persona sbagliata. Queste email inviate al destinatario errato sono una fonte comune di violazioni dei dati. Secondo i dati Proofpoint, il 33% dei collaboratori invia una o due email alla persona sbagliata ogni anno. Si tratta inoltre dell'incidente di perdita di dati più segnalato all'ICO (Information Commissioner's Office) del Regno Unito¹. Inoltre, Verizon ha scoperto che il 50% delle violazioni dovute a un errore nel 2023 è stato causato dall'invio di email al destinatario errato².

L'invio di email al destinatario errato è un problema difficile da risolvere con prodotti tradizionali di DLP via email. Per contro, Proofpoint Adaptive Email DLP utilizza l'ispezione approfondita dei contenuti e l'analisi comportamentale di Proofpoint Nexus® Relationship Graph (RG) per identificare le email indirizzate al destinatario errato prima del loro invio. Quando un utente cerca di inviare un'email al destinatario errato, Proofpoint Adaptive Email DLP rileva l'errore e genera un avviso. Secondo i dati di Proofpoint, Proofpoint Adaptive Email DLP ha impedito l'invio di oltre 160.000 email indirizzate al destinatario errato nel 2024.

Prevenzione dell'invio di allegati sbagliati

L'invio di un allegato sbagliato avviene quando un utente invia un'email al destinatario giusto ma allega un file sbagliato. Quando la nostra IA comportamentale rileva un allegato che sembra insolito per un determinato destinatario, avverte l'utente in tempo reale. L'utente può allora correggere il problema prima che si verifichi una grave perdita di dati.

1. Information Commissioner's Office, "Common data protection mistakes (and how to fix them) (Errori comuni in termini di protezione dei dati e come correggerli)", febbraio 2025.
2. Verizon, 2024 Data Breach Investigations Report 2023 (Report 2023 sulle violazioni dei dati), 2024.

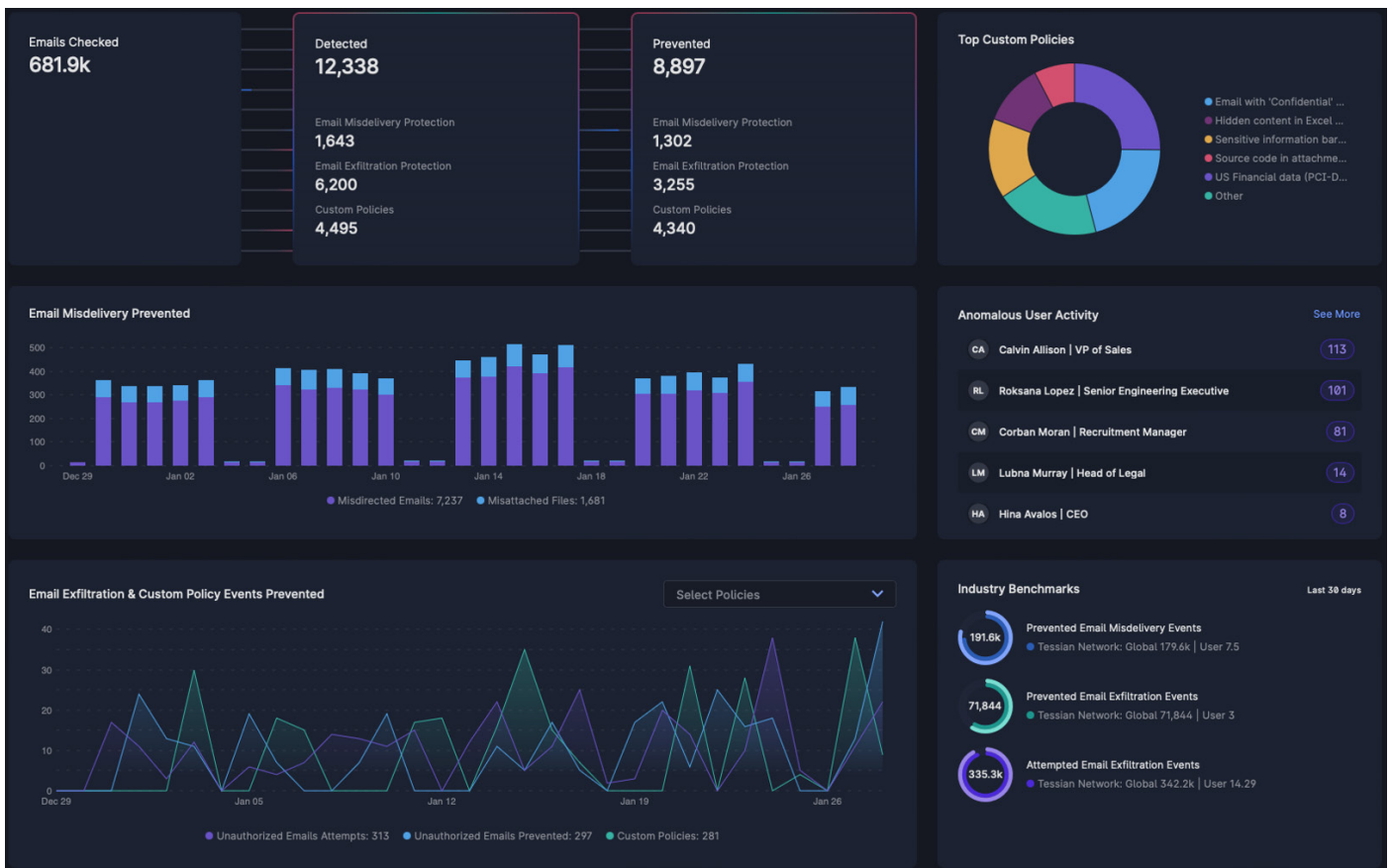


Figura 1. La dashboard Proofpoint Adaptive Email DLP offre ai team della sicurezza delle informazioni una visibilità completa e una fiducia maggiore nella prevenzione della perdita di dati.

>1.100.000

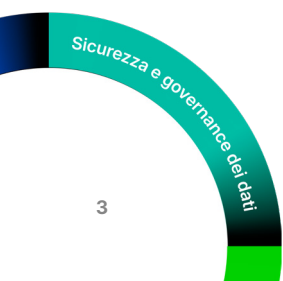
Email che esfiltrano dati rilevate da Proofpoint Adaptive Email DLP nel 2024.

Fonte: Proofpoint

Blocco di esfiltrazioni di dati tramite email

La sottrazione di dati sensibili via email è costosa da correggere per le aziende. Secondo il Ponemon Institute, un team della sicurezza ha bisogno da 48 a 72 ore per identificare e correggere un incidente di esfiltrazione dei dati³. Proofpoint Adaptive Email DLP alleggerisce questo crescente onere per il tuo team. Analizza e classifica automaticamente i tuoi dati sensibili e identifica gli account email personali o non autorizzati dei tuoi utenti. Se un utente cerca di inviare dati sensibili o trasferirli a altre persone, Proofpoint Adaptive Email DLP blocca o sorveglia le sue attività, in base alla sua configurazione. Secondo i dati di Proofpoint, Proofpoint Adaptive Email DLP ha rilevato oltre 1.100.000 email di sottrazione di dati nel 2024.

3. Ponemon Institute, "Email Data Loss Prevention: The Rising Need for Behavioral Intelligence." (Prevenzione della perdita di dati tramite email: la crescente necessità di una threat intelligence comportamentale), maggio 2022.



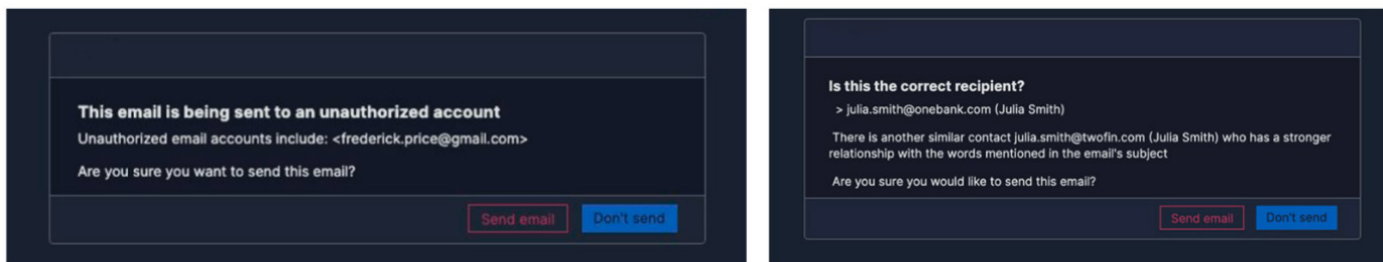


Figura 2. Proofpoint Adaptive Email DLP avvisa gli utenti in tempo reale in caso di invio di email al destinatario errato o a account non autorizzati.

Formazione degli utenti in tempo reale

La formazione degli utenti in tempo reale permette di prevenire gli errori e le violazioni delle regole. Complementare alla formazione di sensibilizzazione alla sicurezza informatica, Proofpoint Adaptive Email DLP spiega agli utenti i rischi legati alle email in tempo reale. Gli utenti possono correggere i loro errori senza l'aiuto di un amministratore.

L'unione fa la forza

Le conseguenze derivanti dalla perdita di dati sensibili possono essere gravi.

Questi incidenti possono comportare sanzioni normative, danni alla reputazione e perdita di fatturato. Possono anche aumentare il costo del lavoro a causa delle indagini e dei report normativi e di conformità.

Integrando sia un prodotto tradizionale di DLP via email e Proofpoint Adaptive Email DLP, la tua azienda può implementare un approccio moderno e multilivello alla sicurezza dei dati dell'email. Questa soluzione riunisce una protezione solida contro i rischi noti con un rilevamento intelligente e dinamico delle minacce di perdita di dati sconosciute incentrate sulle persone. Disponi anche di una protezione rafforzata dei dati, di una miglior conformità degli utenti, di una riduzione dei costi operativi e di un livello rafforzato di sicurezza dei dati dell'email globale.

proofpoint®

Proofpoint, Inc. 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 l'85% delle Fortune 100, 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.

Seguici: [LinkedIn](#)

Proofpoint è un marchio registrato di Proofpoint, Inc. negli Stati Uniti e/o negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari. ©Proofpoint, Inc. 2025

SCOPRI LA PIATTAFORMA PROOFPOINT →