

## PANORAMICA SULLA SOLUZIONE

# Soluzione Proofpoint di sicurezza dei dati

Protezione unificata contro la sottrazione di dati, la divulgazione dei dati e le minacce interne

### Vantaggi principali

- Protezione completa grazie alla prima soluzione unificata di sicurezza dei dati del settore
- Riduzione dei rischi per la sicurezza dei dati grazie alla prevenzione della perdita dei dati, alla gestione delle minacce interne e alla gestione del livello di sicurezza dei dati su tutti i canali
- Razionalizzazione delle operazioni di sicurezza, accelerazione dei tempi di valorizzazione e riduzione del costo di possesso totale
- Agilità aziendale grazie a un utilizzo sicuro dell'IA e alla produttività degli utenti finali

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.

### Le perdite di dati non avvengono per magia

Oggi, i rischi di sicurezza dei dati sono legati al comportamento umano. I collaboratori mettono i dati in pericolo in vari modi: errori, intenti dolosi o violazioni di account. Le ricerche condotte da Proofpoint nel 2024 mostrano che gli utenti negligenti sono all'origine del 71% delle perdite di dati. Gli utenti in uscita dall'azienda sono responsabili dell'87% delle sottrazioni di file ospitati nel cloud<sup>1</sup>.

La proliferazione dei dati è oggi una delle principali sfide. I lavoratori della conoscenza oggi archiviano i dati su cloud pubblici, servizi di condivisione di file e database on premise. Inoltre, alimentano i modelli linguistici di grandi dimensioni (LLM) con i loro dati. Questa frammentazione limita la visibilità dei team IT e della sicurezza. Una violazione su tre coinvolge dati shadow e comporta un aumento del 16% del costo medio di violazione<sup>2</sup>.

Molti strumenti di sicurezza dei dati non tengono conto delle intenzioni né del comportamento umano, ovvero non sono in grado di distinguere le attività inoffensive dai tentativi di furto di dati. Le conseguenze: un numero elevato di falsi allarmi, tempi di investigazione lunghi e inefficienza dei team della sicurezza. Secondo Gartner, entro il 2027 il 70% dei CISO delle grandi aziende adotterà un approccio consolidato per affrontare il problema dei rischi interni e della sottrazione dei dati<sup>3</sup>.

### Rischi ridotti, costi più bassi e maggior agilità aziendale

Proofpoint trasforma la sicurezza dei dati grazie a un approccio adattivo incentrato sulle persone. Aiuta già 53 aziende della classifica Fortune 100 a ridurre i rischi per la sicurezza informatica, diminuire i costi operativi e migliorare l'agilità aziendale.

La nostra soluzione unificata protegge la tua azienda da utenti negligenti, malintenzionati e compromessi con una precisione senza pari. Analizza i contenuti e i comportamenti su tutti i canali: email, endpoint, applicazioni SaaS (Software-as-a-Service) e archivi di dati nel cloud e on premise. I suoi controlli adattivi e automatizzati rispondono ai rischi emergenti in tempo reale. Ottieni una difesa approfondita contro la sottrazione dei dati, la loro divulgazione e le minacce interne.

# 70%

CISO che adotteranno un approccio consolidato per affrontare il problema dei rischi interni e della sottrazione di dati entro il 2027.

Fonte: Gartner

1. Proofpoint, *report Data Loss Landscape*, 2024.  
2. IBM e Ponemon Institute, *Report sul costo delle violazioni dei dati*, 2025.  
3. Gartner, *Market Guide for Data Loss Prevention* (Guida al mercato per la prevenzione delle fughe di dati), 2025.

**Prodotti**

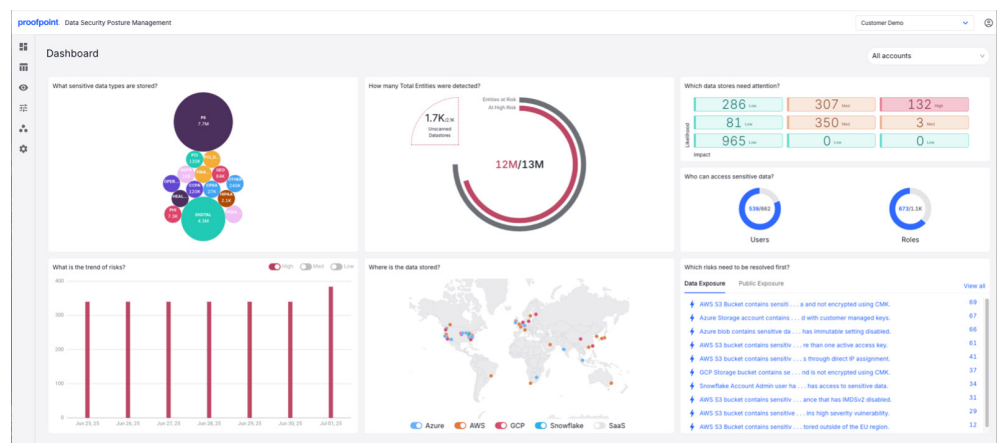
- Proofpoint Enterprise DLP
- Proofpoint Data Security Posture Management
- Proofpoint Insider Threat Management
- Proofpoint Adaptive Email DLP

**Riduzione dei rischi per la sicurezza dei dati**

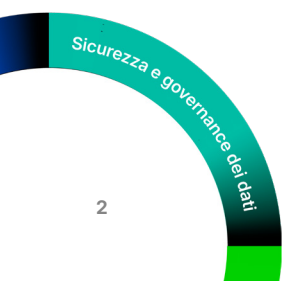
La soluzione Proofpoint di sicurezza dei dati unifica la prevenzione della perdita dei dati (DLP), la gestione del livello di sicurezza dei dati (DSPM) e la gestione delle minacce interne (ITM). Questi componenti unificati ti permettono di identificare, monitorare e mitigare i rischi legati ai dati in modo più efficace. Grazie alla nostra soluzione puoi:

- **Trasformare il tuo programma DLP.** La console unificata con agent singolo per Proofpoint DLP e Proofpoint ITM utilizza l'IA per identificare con precisione le informazioni sensibili. Rileva i comportamenti a rischio grazie alla sua comprensione di contenuti e contesto. Applica controlli adattivi per bloccare la sottrazione di dati e le minacce interne a livello di endpoint, email e cloud.

- **Gestire i rischi interni.** Proofpoint ITM adatta monitoraggio e controlli sulla base dei rischi legati agli utenti. Per velocizzare le indagini, acquisisce prove chiare del comportamento degli utenti.
- **Ridurre l'esposizione dei dati.** Proofpoint DSPM utilizza l'analisi in loco per identificare e classificare i dati sensibili in ambienti cloud e ibridi. Ottieni così visibilità sulla proliferazione dei dati e puoi ridurre l'esposizione dei dati rimuovendo i privilegi eccessivi con un solo clic.
- **Proteggerti contro la perdita di dati via email.** Proofpoint Adaptive Email DLP utilizza l'IA per rilevare e bloccare l'invio di email a un indirizzo errato, i file allegati per errore e le email inviate a account non autorizzati.



**Figura 1.** La dashboard di Proofpoint DSPM mostra i tipi di dati di valore o sensibili, il loro valore finanziario e i rischi, nonché le persone autorizzate a accedervi.



### Precisione del rilevamento ottimizzato dall'IA e valorizzazione più rapida

- Utilizzando un **analizzatore senza agent basato sull'IA**, Proofpoint DSPM offre la classificazione dei dati più precisa sul mercato. Combinando il controllo delle espressioni regolari, l'elaborazione del linguaggio naturale (NLP) e i modelli linguistici di grandi dimensioni (LLM), la soluzione ottimizza le prestazioni e riduce l'utilizzo delle risorse.
- I **classificatori di Proofpoint Nexus AI** identificano con precisione le categorie dei documenti, per esempio, codice sorgente, documenti legali, contabili, risorse umane, ecc. In questo modo le informazioni critiche sono protette.
- Il **rilevamento delle anomalie** identifica le modifiche ai file e le attività degli utenti insolite su cloud ed endpoint. Ciò permette di evitare perdita di dati, minacce interne e violazioni degli account cloud.
- L'**IA comportamentale** di Proofpoint Adaptive Email DLP blocca l'effiltrazione di dati verso account non autorizzati, le email inviate a un indirizzo errato e file allegati per errore che le soluzioni di prevenzione della perdita di dati tramite email basate su regole non sono in grado di rilevare.
- La **ricerca assistita dall'IA** utilizza l'elaborazione del linguaggio naturale per razionalizzare la scoperta e accelerare le indagini.

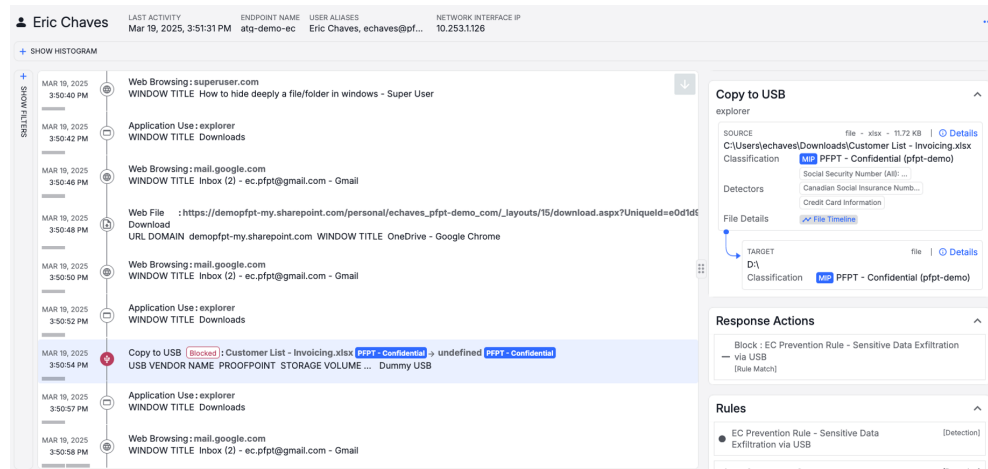
### Incremento dell'efficienza e riduzione dei costi operativi

Proofpoint ti permette di migliorare l'efficienza e l'agilità delle tue operazioni di sicurezza dei dati e protezione contro le minacce interne. La tua soluzione di sicurezza viene così valorizzata più rapidamente e il costo totale di possesso è minore.

### Operazioni efficaci su tutti i canali

Ottimizzato dall'IA e da un'automazione intelligente, la soluzione adattiva e completa di Proofpoint migliora l'efficienza del tuo programma di sicurezza dei dati. L'ampia visibilità, le informazioni ricche sul contesto e l'analisi avanzata eliminano gli avvisi generati da falsi positivi. Il tuo team della sicurezza dispone così di più tempo per concentrarsi sulle iniziative strategiche.

- La sicurezza incentrata sulle persone di Proofpoint riunisce dati di telemetria con la threat intelligence e le informazioni sul comportamento e le intenzioni degli utenti. Puoi distinguere le attività sicure da quelle dannose e rispondere ai rischi in modo efficace.
- Il motore unificato delle policy di Proofpoint applica le policy in modo coerente sulle soluzioni Proofpoint DLP, DSPM e ITM. Le policy adattive si adattano al mutare dei rischi legati all'utente.
- Per aiutarti a stabilire le priorità nella mitigazione dei rischi, Proofpoint DSPM valuta il valore dei dati, la probabilità e le modalità d'attacco potenziali nonché gli accessi associati a privilegi eccessivi. L'eliminazione di privilegi eccessivi in un clic impedisce l'esposizione di dati.
- Proofpoint Data Security Workbench ti aiuta a identificare le minacce prima che si trasformino in violazioni.



**Figura 2.** In questo screenshot della console Data Security Workbench, un utente naviga su un sito web dal titolo "How to hide deeply a file/folder in Windows" (Come nascondere in profondità un file/cartella in Windows), quindi scarica un file dal drive SharePoint dell'azienda. Infine, copia un file riservato intitolato "Customer List - invoicing.xlsx" (Elenco dei clienti - fatturazione.xlsx) su una chiavetta USB. Questa cronologia delle attività dell'utente e dell'identificazione di un contenuto sensibile mostra a un analista che l'utente cerca di eludere le policy dell'azienda e che sono necessarie ulteriori indagini.



# 58%

Proofpoint riduce i costi amministrativi legati alla DLP del 58%.

Fonte: Enterprise Strategy Group

# 182%

Proofpoint Enterprise DLP offre un ritorno sull'investimento del 182% su tre anni.

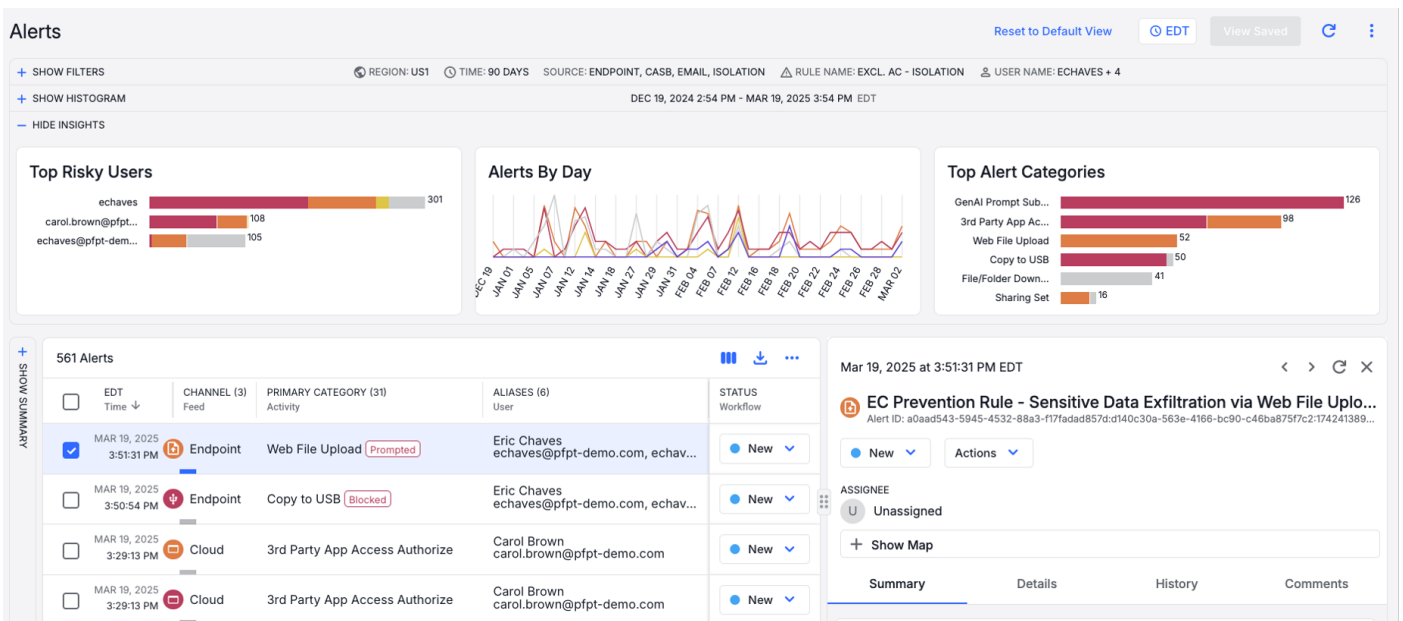
Fonte: Enterprise Strategy Group

### Valorizzazione e costo di possesso senza pari

Il report [Economic Validation of Proofpoint Enterprise DLP](#) del 2025 di Enterprise Strategy Group rileva che Proofpoint riduce i costi amministrativi legati alla DLP del 58% e offre un ritorno sull'investimento del 182%<sup>4</sup>, grazie ai seguenti punti di forza:

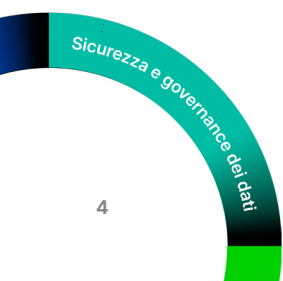
- Il servizio nativo nel cloud di Proofpoint ottimizza implementazione, integrazione e amministrazione.

- La sicurezza dei dati guidata dall'IA, insieme a informazioni sul comportamento degli utenti, riduce i tempi di valorizzazione da mesi a poche settimane rispetto alle soluzioni tradizionali.
- La soluzione unificata di Proofpoint è più redditizia ed efficiente rispetto a un mix di strumenti singoli.
- Proofpoint DSPM identifica e rimuove i dati ridondanti e i backup e le istantanee abbandonate. Questo approccio riduce la superficie d'attacco e diminuisce i costi di archiviazione nel cloud.



**Figura 3.** La console Data Security Workbench razionalizza la gestione degli avvisi a livello di email, cloud e endpoint, senza dover passare da una console all'altra. In questo esempio, un analista filtra gli avvisi per un utente specifico. La dashboard mostra che l'utente ha caricato dati sensibili sul suo account email aziendale e ha cercato di copiare un file su una chiavetta USB prima di essere bloccato.

4. Enterprise Strategy Group, *Analyzing the Economic Value of Proofpoint Enterprise DLP* (Analisi del valore economico di Proofpoint Enterprise DLP), giugno 2025.



## Agilità in un ambiente aziendale in evoluzione

Che la tua azienda sia in fase di ristrutturazione, espansione geografica o stia adottando nuove tecnologie, la soluzione Proofpoint di sicurezza dei dati protegge le tue informazioni sensibili. Grazie a Proofpoint puoi:

- **Facilitare il cambiamento organizzativo** riducendo i rischi per la proprietà intellettuale, le informazioni riservate e altri dati sensibili, tra cui le informazioni associate a fusioni, acquisizioni o ristrutturazioni. Grazie a una maggior visibilità sugli ambienti delle aziende acquisite, puoi colmare le lacune di sicurezza ereditate. Le funzionalità di automazione permettono di applicare policy e standard di sicurezza. Le policy adattive si adattano in tempo reale ai rischi in evoluzione.
- **Assicurare un utilizzo sicuro e conforme dell'IA** impedendo la condivisione di dati sensibili con gli strumenti di IA generativa, i modelli linguistici di grandi dimensioni e gli agent di IA. Limita l'inclusione di informazioni protette nei prompt di IA generativa lanciati dai browser e dalle applicazioni installate. Impedisci l'utilizzo dei dati riservati nell'addestramento di modelli linguistici di grandi dimensioni personalizzati.

- **Promuovere la produttività degli utenti finali** assicurando le prestazioni dell'endpoint e l'accesso alle applicazioni. Grazie all'agent singolo e leggero in modalità utente di Proofpoint DLP e Proofpoint ITM eviti i conflitti software, il blocco dei sistemi e il calo delle prestazioni degli endpoint associati agli agent in modalità kernel. Invece di bloccare in modo generico le applicazioni, puoi fornire agli utenti semplici suggerimenti, come un promemoria in tempo reale che ricorda loro di non inserire informazioni sensibili in un prompt ChatGPT. Puoi anche richiedere agli utenti di fornire una giustificazione in caso di copia di dati sensibili.

## Massimizzazione dell'impatto dei programmi di sicurezza dei dati e gestione delle minacce interne

In qualità di partner strategico, Proofpoint si impegna a aiutarti a garantire il successo del tuo programma a livello di persone, processi e tecnologia. I servizi Premium di Proofpoint possono aiutarti a ottimizzare e sviluppare i tuoi programmi di sicurezza dei dati e di gestione delle minacce interne. Dalla consulenza, all'assistenza tecnica e alla guida operativa continua fino alla gestione pratica della sicurezza dei dati, Proofpoint ti offre le competenze di cui hai bisogno nel momento in cui ne hai bisogno.



**Figura 4.** La dashboard di Proofpoint Adaptive Email DLP mostra le statistiche relative al rilevamento e prevenzione della perdita di dati sensibili. Tali dati includono metriche relative all'invio di email a un indirizzo errato, alle sottrazioni di dati tramite l'email, alle policy personalizzate applicate e agli utenti con un comportamento particolarmente anomalo.

## Livelli di servizio della soluzione Proofpoint di sicurezza dei dati

La soluzione è disponibile in tre livelli di servizio: Data Security Core, Data Security Core Plus e Data Security Complete. Le principali funzionalità dei diversi livelli sono riportate nella tabella.

PRINCIPALI FUNZIONALITÀ	DATA SECURITY CORE	DATA SECURITY CORE PLUS	DATA SECURITY COMPLETE
Contesto dettagliato su utenti e file	✓	✓	✓
Tracciamento delle minacce per un rilevamento e indagini proattivi	✓	✓	✓
Agent unico configurabile in modalità utente per la gestione delle minacce interne e la DLP	✓	✓	✓
Rilevamenti DLP arricchiti (RegEx, OCR, IDM, EDM) e classificazione MIP	✓	✓	✓
Monitoraggio e rilevamento degli spostamenti dei file con tracciabilità dei dati	✓	✓	✓
Rilevatori estesi delle applicazioni cloud	✓	✓	✓
Gestione unificata degli allarmi e configurazione DLP	✓	✓	✓
Controlli granulari della privacy dei dati e degli accessi	✓	✓	✓
Integrazione nell'ecosistema di sicurezza (SIEM/SOAR/Teams)	✓	✓	✓
Rilevamento e analisi dei dati sensibili nelle email e negli allegati	✓	✓	✓
Crittografia dinamica delle email esterne e interne	✓	✓	✓
Analisi dell'impronta digitale dei documenti sensibili nelle email	✓	✓	✓
Identificazione e classificazione degli archivi di dati		✓	✓
Rilevamento e correzione dei rischi di esposizione negli archivi di dati		✓	✓
Prevenzione ottimizzata dall'IA della perdita di dati accidentale e intenzionale tramite l'email			✓

# 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](http://www.proofpoint.com/it).

Seguici: [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

Proofpoint è un marchio registrato o nome commerciale 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 →**