proofpoint.

# Guida all'acquisto delle soluzioni di prevenzione della perdita di dati

Questa guida all'acquisto mette in evidenza le funzionalità più importanti di una soluzione moderna di protezione delle informazioni. Riassume ciò che Proofpoint ha appreso dalla creazione di programmi efficaci di prevenzione della perdita dei dati (DLP) per aziende di tutte le dimensioni in tutto il mondo e in tutti i settori. Vuole essere una guida di riferimento pratica sia che tu stia iniziando il percorso di prevenzione della perdita di dati o che desideri modernizzare i tuoi sistemi DLP esistenti.

## Sicurezza incentrata sulle persone

Per proteggere i dati dalle minacce comuni e uniche, hai bisogno di una piattaforma che supporti un modello di sicurezza incentrata sulle persone, ovvero una piattaforma che offre visibilità completa sulle interazioni degli utenti con i dati sensibili e il monitoraggio dei comportamenti a rischio. Ti fornisce importanti informazioni di contesto sulle loro intenzioni in caso di perdita o furto di dati, o quando compiono azioni sospette.

Grazie a una soluzione incentrata sulle persone puoi valutare rapidamente i rischi di perdita di dati tramite email, endpoint e applicazioni cloud come Microsoft 365, Google Workspace e Salesforce. Queste informazioni ti permettono di agire rapidamente e adottare le misure necessarie per prevenire qualsiasi incidente di perdita di dati.

## Elementi chiave di una soluzione DLP moderna

Se desideri gestire la perdita di dati e bloccare le minacce interne, devi essere in grado di rilevare, analizzare, prevenire e neutralizzare gli incidenti. Solo compiendo tutte queste azioni in modo coordinato puoi ridurre i tuoi rischi.

### Monitoraggio

Per proteggere i dati, non puoi concentrarti solo sui contenuti. Devi avere visibilità sulle interazioni degli utenti con i dati. Quando controlli l'attività dei dati di tutti gli utenti tramite endpoint, email, cloud e web, disponi di una panoramica globale e informazioni contestualizzate.

**85%**

Aziende che hanno segnalato una o più perdita di dati nel 2023

**50%**

Lavoratori adulti che hanno cambiato lavoro nel corso degli ultimi due anni che hanno ammesso di aver portato con loro dei dati

### Rilevamento

Hai bisogno di una soluzione in grado di rilevare, in tempo reale o quasi, le azioni pericolose di un utente o la potenziale esposizione dei dati, anche se non si trasformano in un vero e proprio incidente. Le funzionalità di rilevamento devono trovare il giusto equilibrio tra avvisi tempestivi e fruibili e il rischio di calo della vigilanza a causa della proliferazione degli avvisi.

### Analisi

Grazie a dati analitici efficaci, puoi analizzare le tendenze nei comportamenti degli utenti e tracciare le minacce. Ma puoi farlo solo se la soluzione DLP combina le attività degli utenti su diversi canali. In questo modo puoi individuare qualsiasi comportamento a rischio degli utenti. Benché questo processo possa essere automatizzato, è fondamentale rivolgersi a degli analisti che possano esaminare i dati in modo approfondito.

### Risposta

È importante indagare e rispondere in modo rapido ed efficiente agli incidenti. Più tempo è necessario per neutralizzare una minaccia interna, più danni può causare in termini di risultati finanziari e reputazione. Una soluzione DLP moderna può applicare automaticamente le policy e neutralizzare le minacce. L'automazione mantiene al sicuro i tuoi dati più preziosi e aumenta l'efficienza del tuo team della sicurezza.

### Prevenzione

Si tratta della capacità di evitare che un utente violi involontariamente o deliberatamente le policy di sicurezza della tua azienda. Per farlo, devi formare gli utenti, inviare promemoria in tempo reale e bloccare le attività di alcuni utenti, se necessario.

## 3 principali scenari di perdita di dati

DI seguito tre scenari comuni di perdita di dati. Tutti sono causati da un intervento umano. Una piattaforma di protezione delle informazioni incentrata sulle persone deve poter identificare:

- Gli utenti che danno prova di negligenza con i dati sensibili
- Gli utenti negligenti che espongono i dati sensibili quando utilizzano applicazioni di IA generativa
- Gli utenti interni malintenzionati che cercano di danneggiare l'azienda

**3,5 miliardi$** Spesa complessiva prevista per la prevenzione della perdita di dati nel mondo entro il 2025[1].

**77 GIORNI** Giorni necessari per eliminare le minacce interne[2].

**85%** Aziende colpite da attacchi basati sul cloud[3].

**56%** Incidenti causati dalla negligenza degli utenti[4].

## 1: utenti negligenti e errori comuni

Secondo il nostro report Data Loss Landscape 2024, gli utenti negligenti sono la principale causa di perdita di dati. Questi utenti non intendono provocare una perdita di dati, ma desiderano solo svolgere il loro lavoro nel modo più efficiente possibile. Tuttavia, i loro errori possono avere gravi conseguenze: interruzione delle attività, danni alla reputazione, indebolimento della posizione concorrenziale, violazioni normative e sanzioni, cause legali, ecc.

Ecco alcuni esempi di azioni a rischio di questi utenti:

- Invio di email al destinatario errato, con o senza allegati
- Consultazione di siti phishing
- Installazione di software non autorizzati
- Condivisione pubblica di file e dati sensibili
- Invio tramite email di informazioni personali a un account email personale
- Archiviazione di dati aziendali sensibili su dispositivi personali

### Protezione contro i comportamenti negligenti

Un sistema di protezione delle informazioni incentrato sulle persone efficace deve bloccare le attività a rischio. Deve inoltre formare gli utenti negligenti per aiutarli a comprendere cosa c'è di sbagliato nel loro comportamento affinché possano cambiarlo.

Elementi indispensabili:

- **Classificazione.** Verifica che email, dati e contenuti vengano monitorati costantemente sia manualmente che con l'intelligenza artificiale (IA) per identificare e classificare gli utenti a rischio. Se l'utente è considerato a rischio elevato, il sistema assegnerà un punteggio di rischio per proteggere i dati di conseguenza.
- **Rilevamento.** Il sistema deve monitorare email, documenti e dati, valutando costantemente i rischi di non conformità. Poiché i contenuti si spostano tra vari canali (endpoint email, cloud o web) devono essere analizzati per assicurarsi che tale spostamento o condivisione non violi le policy della tua azienda. Se viene rilevata una violazione nell'email, il sistema dovrebbe consentire ai team della sicurezza di bloccare l'email o monitorarla per ulteriori indagini.
- **Prevenzione.** Dovrebbe essere impedito agli utenti di esfiltrare dati sensibili tramite i diversi canali e dispositivi: email inviate al destinatario errato con o senza allegati, chiavette USB, caricamento su web, sincronizzazione cloud, stampa, ecc. Se commettono un errore, dovrebbero ricevere immediatamente un messaggio di avvertimento contestuale, permettendo loro di correggerlo e prevenire la perdita di dati in tempo reale senza intervento dell'amministratore. Se necessario, gli utenti possono spiegare perché hanno bisogno di accedere ai dati. Di conseguenza, il team della sicurezza può autorizzare o rifiutare tale richiesta.

1 The Radicati Group, "Data loss prevention (DLP) market value revenue forecast worldwide from 2019 to 2025" (Previsione delle entrate del mercato della prevenzione della perdita dei dati su scala mondiale dal 2019 al 2025), maggio 2022.
2 Ponemon Institute, "2022 Cost of Insider Threats Global Report" (Report 2022 sul costo delle minacce interne a livello mondiale), febbraio 2022.
3 Assaf Friedman and Itir Clarke (Proofpoint) "How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps." (Come i criminali informatici utilizzano gli account compromessi per creare e distribuire applicazioni OAuth), maggio 2021.
4 Ponemon Institute, "2022 Cost of Insider Threats Global Report" (Report 2022 sul costo delle minacce interne a livello mondiale), febbraio 2022.

## 2: utenti negligenti e applicazioni di IA generativa

Sebbene ChatGPT e altri strumenti di IA generativa consentano agli utenti di migliorare notevolmente la loro produttività, Sono spesso all'origine delle perdite di dati. Per prevenire la perdita di dati senza nuocere alla produttività, hai bisogno di solide misure di protezione dei dati. Il punto è che non puoi applicare policy d'uso accettabili per l'IA generativa se non comprendi i tuoi contenuti e come i collaboratori vi interagiscono.

### Protezione contro l'utilizzo negligente dell'IA generativa

L'adozione di solide misure di protezione dei dati è importante per prevenire la perdita di dati sensibili attraverso gli strumenti di IA generativa. Non puoi semplicemente bloccare completamente l'accesso agli strumenti di IA generativa. È importante consentire agli utenti di accedervi, poiché questi strumenti aumentano la produttività e favoriscono l'innovazione.

Se desideri che i collaboratori utilizzino gli strumenti di IA generativa senza mettere i dati in pericolo, devi adottare un approccio incentrato sulle persone alla prevenzione della perdita di dati. Una soluzione basata su questo approccio autorizza e impedisce in modo preciso ai collaboratori di utilizzare gli strumenti di IA generativa in base al loro comportamento e contributi, anche se i dati sono stati manipolati o sono passati attraverso diversi canali.

Elementi indispensabili:

- **Identificazione dei contenuti sensibili.** Quando un sistema è in grado di identificare quale contenuto è importante proteggere, può bloccare la perdita di dati in modo più efficace. Scegli metodi avanzati di identificazione e classificazione dei contenuti, come il riconoscimento ottico dei caratteri, la corrispondenza esatta dei dati e la corrispondenza dei documenti indicizzati.
- **Monitoraggio degli utenti.** Devi sapere chi utilizza strumenti di IA generativa nel tuo ambiente e i metodi utilizzati. Il sistema dovrebbe essere in grado di rilevare, bloccare e segnalare gli innumerevoli tipi di azioni degli utenti, tra cui il caricamento di file di codice sorgente e l'incollatura di elementi di proprietà intellettuale aziendale.
- **Gestione proattiva dei rischi.** Creando e registrando esplorazioni personalizzate, i tuoi team possono andare alla ricerca di esfiltrazioni di dati e altre attività rischiose associate agli strumenti di IA generativa.

## 3: utenti malintenzionati

Gli utenti malintenzionati sono pericolosi perché si trovano nella posizione ideale per appropriarsi di dati sensibili. I collaboratori in uscita dall'azienda sono il tipo di utenti interni più a rischio. Nel corso di nove mesi nel 2023, i collaboratori in uscita dall'azienda hanno causato l'87% delle esfiltrazioni di file sospette tramite tenant cloud che utilizzano la piattaforma Proofpoint Information Protection. Questi utenti spesso ritengono di avere il diritto di portare con sé le informazioni quando lasciano l'azienda dato il tempo che hanno dedicato ai loro progetti.

Ciò che rende gli utenti interni malintenzionati una tale minaccia, è che possono restare in attesa e utilizzare il loro accesso con privilegi per trovare dati preziosi e falle nella sicurezza. Inoltre, le aziende spesso si complicano la vita da sole consentendo ai collaboratori di consultare e archiviare i dati sui loro dispositivi personali, facilitando il furto di dati sensibili.

Un sistema incentrato sulle persone monitora più da vicino alcuni utenti rispetto ad altri e applica controlli di sicurezza più rigorosi agli utenti più a rischio

### Protezione contro gli utenti malintenzionati

Un sistema incentrato sulle persone monitora più da vicino alcuni utenti rispetto ad altri, applica controlli di sicurezza più rigorosi agli utenti più a rischio e blocca proattivamente le azioni dannose in base ai fattori di rischio, come in caso di dimissioni o licenziamento.

Elementi indispensabili:

- **Visibilità.** La visibilità su endpoint, email, cloud e web fornisce una visione olistica e informazioni contestualizzate sulle attività di un utente. Dovrebbero essere raccolti dati di telemetria sulle interazioni degli utenti con i dati e i sistemi, come quando rinominano un file sensibile o lo caricano su un sito web non autorizzato o in una cartella sincronizzata nel cloud. Se un utente installa o esegue delle applicazioni non autorizzate, anche queste attività dovrebbero essere monitorate. Il team della sicurezza dovrebbe essere in grado di identificare in tempo reale chiunque faccia scattare un allarme.
- **Indagini.** Hai bisogno di una libreria di avvisi per i casi di utilizzo più comuni (frode sull'orario di lavoro, esfiltrazione di dati, elusione dei controlli di sicurezza). In questo modo puoi agire rapidamente. I team della sicurezza devono ricevere avvisi con metadati dettagliati e schermate dell'attività degli utenti. Una vista cronologica contestualizzata degli eventi aiuta i team incaricati dell'indagine a comprendere i dettagli ("chi, cosa, quando, dove") delle attività degli utenti.
- **Architettura moderna.** Il vantaggio di una piattaforma nativa nel cloud è che può supportare centinaia di migliaia di utenti. Quando include funzioni come i controlli d'accesso basati su attributi, mascheramento e anonimizzazione dei dati e supporto dei data center multiregionali, puoi soddisfare i requisiti di privacy e residenza dei dati. Inoltre, un sistema moderno completerà il tuo sistema di sicurezza, poiché potrà essere integrato facilmente con diversi strumenti, tra cui:
  - Orchestrazione, automazione e risposta agli incidenti di sicurezza (SOAR)
  - Gestione degli eventi e delle informazioni di sicurezza (SIEM)
  - Risposta agli incidenti
  - Gestione dei ticket

# Funzionalità richieste

Ora che sai come i sistemi DLP moderni incentrati sulle persone ti aiutano a proteggerti, esaminiamo più da vicino le funzionalità indispensabili, che ricadono in tre categorie:

- Rilevamento e prevenzione dei rischi di perdita di dati
- Analisi e risposta agli incidenti
- Distribuzione e implementazione

## Rilevamento e prevenzione dei rischi di perdita di dati

Quando i team della sicurezza dispongono di informazioni sul comportamento degli utenti e sui contenuti sensibili, possono gestire i rischi legati ai dati in modo appropriato e con maggior precisione.

| ESIGENZA DEL CLIENTE | FUNZIONALITÀ RICHIESTE |
|---|---|
| Rilevamento di contenuti sensibili | Rilevamento e analisi dei dati sensibili nelle email, sugli endpoint, nel cloud e nel web |
| | Funzionalità integrata di classificazione dei dati sensibili in base al contenuto aziendale |
| | Classificazione dei dati basata sull'IA con modelli linguistici di grandi dimensioni (LLM) |
| | Metodi avanzati di identificazione:<br>• Riconoscimento ottico dei caratteri (OCR)<br>• Corrispondenza esatta dei dati (EDM)<br>• Corrispondenza dei documenti indicizzati (IDM) |
| | Policy predefinite per rilevare i dati sensibili, come:<br>• Dati a carattere personale<br>• Standard PCI, legge SOX, legge GLBA, termini rilevanti di insider trading definiti dalla SEC<br>• Informazioni di identificazione sanitaria, legge HIPAA, ICD-9, ICD-11 codice nazionale dei farmaci americano<br>• GDPR, UK-DPA, EU-DEPD, PIPEDA |
| | Capacità di impostare policy per leggere e applicare etichette di riservatezza Microsoft Information Protection (MIP) per identificare i dati aziendali critici |

| ESIGENZA DEL CLIENTE | FUNZIONALITÀ RICHIESTE |
|---|---|
| Monitoraggio del comportamento degli utenti | Approccio incentrato sulle persone che permette agli analisti di rispondere rapidamente grazie alle seguenti informazioni:<br>• Intento degli utenti<br>• Schemi di accesso ai dati<br>• Schemi di accesso alle applicazioni |
| | Capacità di monitorare le interazioni degli utenti con i dati a livello di endpoint gestiti e non gestiti e cloud:<br>• Ridenominazione dei file<br>• Modifica delle estensioni dei file<br>• Caricamento e download web<br>• Copia su chiave USB<br>• Sincronizzazione di condivisioni cloud<br>• Apertura di documenti<br>• Attività sospette sui file |
| | Monitoraggio dell'utilizzo di siti web e applicazioni:<br>• Caricamento, inserimento o digitazione di contenuti su siti di IA generativa<br>• Download e installazione di strumenti di backup dei dati o di pirateria |
| | Monitoraggio del comportamento degli utenti interni più a rischio per comprendere l'intento e limitare i rischi, come la manipolazione del registro Windows per rimuovere i controlli |
| | Monitoraggio proattivo degli utenti a rischio tramite semplici schermate in caso di attivazione di un allarme per garantire la privacy |
| | Formazione degli utenti e richiesta di una motivazione in caso di accesso ai dati sensibili, invece di un blocco che potrebbe influenzare negativamente la loro produttività (email, endpoint, cloud, web) |
| Prevenzione della perdita di dati | Formazione di sensibilizzazione alla sicurezza informatica che aiuta a modificare il comportamento degli utenti insegnando come evitare i rischi per la sicurezza informatica e proteggere i dati sensibili |
| | Prevenzione dell'esfiltrazione dei dati sensibili dagli endpoint gestiti, come:<br>• Copia di file su una chiavetta USB non autorizzata<br>• Caricamento di file su una cartella cloud personale<br>• Stampa di documenti sensibili<br>• Copia e incolla di contenuti sensibili dagli appunti<br>• Condivisioni di rete |
| | Controllo della condivisione eccessiva di file nelle applicazioni cloud e limitazione automatica delle autorizzazioni di condivisione dei file |
| | Protezione dell'accesso ai file sensibili in applicazioni cloud approvate dall'IT da dispositivi non gestiti |
| | Rilevamento e prevenzione automatica delle email inviate al destinatario errato, con o senza un allegato |
| | Rilevamento e prevenzione automatica delle email inviate al destinatario corretto, ma con l'allegato sbagliato |
| | Prevenzione della condivisione di dati sensibili non ancora predefiniti con account email personali e altri account non autorizzati |

## Analisi e risposta agli incidenti

É importante che i team della sicurezza risolvano rapidamente gli incidenti per tutti i canali. L'obiettivo è limitare l'esposizione dei dati e proteggere la privacy.

| ESIGENZA DEL CLIENTE | FUNZIONALITÀ RICHIESTE |
|---|---|
| Risoluzione degli incidenti per tutti i canali | Console unificata per tutti i canali (email, endpoint e cloud) che effettua le seguenti operazioni:<br>• Classificazione degli avvisi per priorità<br>• Indagini<br>• Esplorazioni su misura<br>• Risposta |
| | Analisi per tutti i canali che mostrano:<br>• Attività degli utenti nel tempo<br>• Attività dei file nel tempo (creazione, modifica, condivisione) |
| | Funzionalità di esplorazione proattiva che forniscono visibilità in tempo reale sui comportamenti degli utenti a rischio |
| | Integrazione con la piattaforma SIEM della tua azienda che consente di classificare per priorità i flussi di lavoro con i tuoi strumenti esistenti |
| | Capacità di rilevare e neutralizzare automaticamente i rischi di perdita di dati legati a utenti compromessi tramite:<br>• Chiusura delle sessione<br>• Reimpostazione delle password<br>• Correzione dei rischi<br>• Identificazione dell'impatto |
| Privacy | Flessibilità dei controlli d'accesso assicurando che gli analisti vedano solo ciò che è assolutamente necessario |
| | Anonimizzazione delle informazioni di identificazione dell'utente e mascheramento dei contenuti sensibili per proteggere i dati e eliminare il pregiudizio degli analisti |

## Distribuzione e implementazione

Dopo aver scelto la miglior soluzione DLP per la tua azienda dovrai implementarla. Per un processo di implementazione senza problemi, è fondamentale scegliere i partner giusti per aiutarti nel tuo percorso DLP.

| ESIGENZA DEL CLIENTE | FUNZIONALITÀ RICHIESTE |
|---|---|
| Implementazione | Soluzione nativa nel cloud che può essere implementata rapidamente |
| | Soluzione altamente scalabile che può essere facilmente estesa a centinaia di migliaia di utenti per tenant |
| | Soluzione facile da gestire che richiede manutenzione e alimentazione minime, grazie a una comunicazione chiara degli aggiornamenti e a un'assistenza del fornitore in caso di necessità |
| | Centralizzazione di policy e amministrazione che soddisfano i requisiti multiregionali in termini di residenza dei dati |
| | Piattaforma flessibile che si integra con il tuo ecosistema di sicurezza, incluse le soluzioni seguenti:<br>• Microsoft<br>• Okta e Sailpoint<br>• CrowdStrike<br>• Splunk e Service Now<br>• Zscaler e Citrix ShareFile |
| | Un agent endpoint leggero in modalità utente che:<br>• Rafforza la visibilità sulle potenziali minacce interne<br>• Migliora la produttività degli utenti<br>• Elimina i problemi di stabilità<br>• Non entra in conflitto con altre soluzioni |
| Implementazione | Servizi professionali che possono aiutarti a velocizzare la distribuzione grazie a un team di esperti di lunga data che adatta il tuo sistema alle tue esigenze. L'implementazione di una soluzione DLP avviene in diverse fasi:<br>• Raccolta di requisiti<br>• Design<br>• Personalizzazione della soluzione<br>• Test e ottimizzazione<br>• Formazione di amministratori e utenti<br>• Documentazione |
| DLP gestito | Le aziende di ogni dimensione dovrebbero prendere in considerazione anche l'utilizzo di una soluzione DLP gestita. I servizi gestiti ti forniscono l'aiuto di esperti accreditati, sempre disponibili, che progettano, implementano e co-gestiscono il tuo programma. |

## PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.



1207-013-05-01 7/24