proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Enterprise DLP

Trasforma il tuo programma e la tua architettura di sicurezza dei dati

Vantaggi principali

- Prevenzione della perdita di dati tramite email, cloud, endpoint e applicazioni di IA generativa
- Accelerazione della risoluzione degli incidenti, con classificazione degli avvisi DLP per priorità, indagini e risposta
- Implementazione rapida, scalabilità automatica e manutenzione semplificata
- Rispetto dei requisiti in materia di privacy dei dati negli Stati Uniti e in altre regioni

Oggi i collaboratori mettono a rischio i dati in diversi modi. Utilizzano dispositivi personali per accedere alle applicazioni cloud e condividere dati tramite email, endpoint e strumenti di collaborazione. Inoltre, gli strumenti di IA generativa non approvati sono spesso accessibili con un semplice clic del browser. I team della sicurezza sono sempre più impegnati a proteggere la privacy, mantenere la conformità con le normative e promuovere un'adozione responsabile dell'IA generativa. Oggi le violazioni comportano conseguenze sempre più gravi a livello finanziario, della reputazione e delle verifiche.

Le aziende hanno bisogno di una migliore visibilità sui dati sensibili. Devono inoltre osservare come gli utenti gestiscono questi dati a livello di email, cloud, endpoint e applicazioni di IA generativa. Tuttavia, gli strumenti di prevenzione della perdita di dati (DLP) di vecchia generazione sono spesso isolati, difficili da scalare e incoerenti tra i diversi canali. Inoltre, non sono in grado di far fronte ai rischi emergenti legati all'IA.

Proofpoint Enterprise DLP favorisce un approccio unico e adattivo alla prevenzione della perdita di dati (DLP). Aiuta a prevenire la perdita di dati causata dalle persone tramite email, cloud, endpoint e applicazioni di IA. Aiuta inoltre i team della sicurezza a lavorare in modo più efficiente.

Proofpoint identifica i contenuti sensibili e mostra come i collaboratori li utilizzano. La console unificata ti aiuta a gestire gli avvisi e indagare sugli incidenti su tutti i canali. Le analisi e la classificazione dell'IA aiutano i team a valutare i rischi legati ai dati, a prendere decisioni migliori e a agire rapidamente. La soluzione funziona nel cloud, si adatta automaticamente alle esigenze ed è facile da implementare e gestire. Dispone inoltre di moderni controlli della privacy e di un agente estremamente stabile.

Riduci i rischi per la sicurezza dei dati su tutti i canali

Una visione chiara del comportamento degli utenti

Proofpoint monitora il modo in cui i collaboratori utilizzano i dati a livello di email, endpoint gestiti e non gestiti, strumenti di IA generativa e applicazioni cloud (Microsoft 365, Google Workspace, Salesforce, ecc.). Rivela le intenzioni dell'utente e rileva e previene le sottrazioni. Tra gli esempi, la copia di file su una chiavetta USB non autorizzata, il caricamento di file sensibili su una cartella cloud personale o la condivisione di informazioni riservate tramite prompt di IA.

Proofpoint aiuta le aziende a adottare l'IA generativa in modo sicuro. Rileva, blocca e oscura i dati sensibili prima che vengano condivisi con applicazioni di IA approvate o non approvate. I team possono applicare le policy nelle applicazioni di IA di browser e desktop. Misure correttive intelligenti e esperienze utente guidate aiutano gli utenti a rimanere produttivi.

Proofpoint monitora e controlla quanto segue:

- Caricamento di file in applicazioni di IA
- Attività di copia e incolla che coinvolgono dati sensibili
- Prompt di IA contenenti informazioni regolamentate o proprietarie
- Allegati sensibili condivisi tramite email e strumenti di collaborazione cloud
- Comportamenti a rischio degli utenti su endpoint e servizi cloud

Proofpoint si integra con LDAP e Active Directory. Puoi utilizzare i gruppi presenti di queste directory per definire e applicare dinamicamente policy dettagliate di crittografia delle email. La nostra soluzione tiene traccia di comportamenti quali:

- **Modifiche ai file**, tra cui il cambio di nome di file contenenti dati sensibili o la modifica delle loro estensioni
- **Utilizzo insolito di siti web e applicazioni**, incluso il download di backup dei dati o strumenti di pirateria
- **Azioni pericolose di utenti ad alto rischio**, tra cui la manipolazione del registro di Windows per disabilitare i controlli di sicurezza

Identificazione accurata dei contenuti e classificazione tramite IA

Proofpoint migliora la precisione del rilevamento con oltre 110 classificatori pronti all'uso guidati dall'IA. Questi identificano le categorie dei documenti e aggiungono contesto aziendale agli avvisi DLP. Operano con tecnologie di corrispondenza dei modelli, corrispondenza esatta dei dati (EDM), corrispondenza di documenti indicizzati (IDM), riconoscimento ottico dei caratteri (OCR) e analisi dell'impronta digitale. Questa combinazione riduce i falsi positivi e migliora la protezione su tutti i canali.

La classificazione personalizzata autonoma di Proofpoint utilizza modelli linguistici di grandi dimensioni (LLM) per identificare i contenuti sensibili di ciascuna azienda, senza regolazioni manuali. I team possono individuare e proteggere rapidamente i dati proprietari (codice sorgente, modelli finanziari, documenti tecnici, fascicoli dei clienti, ecc.). Ciò semplifica la creazione delle policy e accelera la valorizzazione.

I motori di rilevamento condivisi guidati dall'IA offrono una protezione coerente su tutti i canali DLP aziendali. Le aziende possono rilevare e classificare i dati di identificazione personale, le informazioni sanitarie protette (PHI), i dati del settore delle carte di pagamento, le credenziali d'accesso, la proprietà intellettuale e le informazioni commerciali riservate. Gli avvisi arricchiti dagli LLM aggiungono contesto che consente ai team di indagare e rispondere più rapidamente.

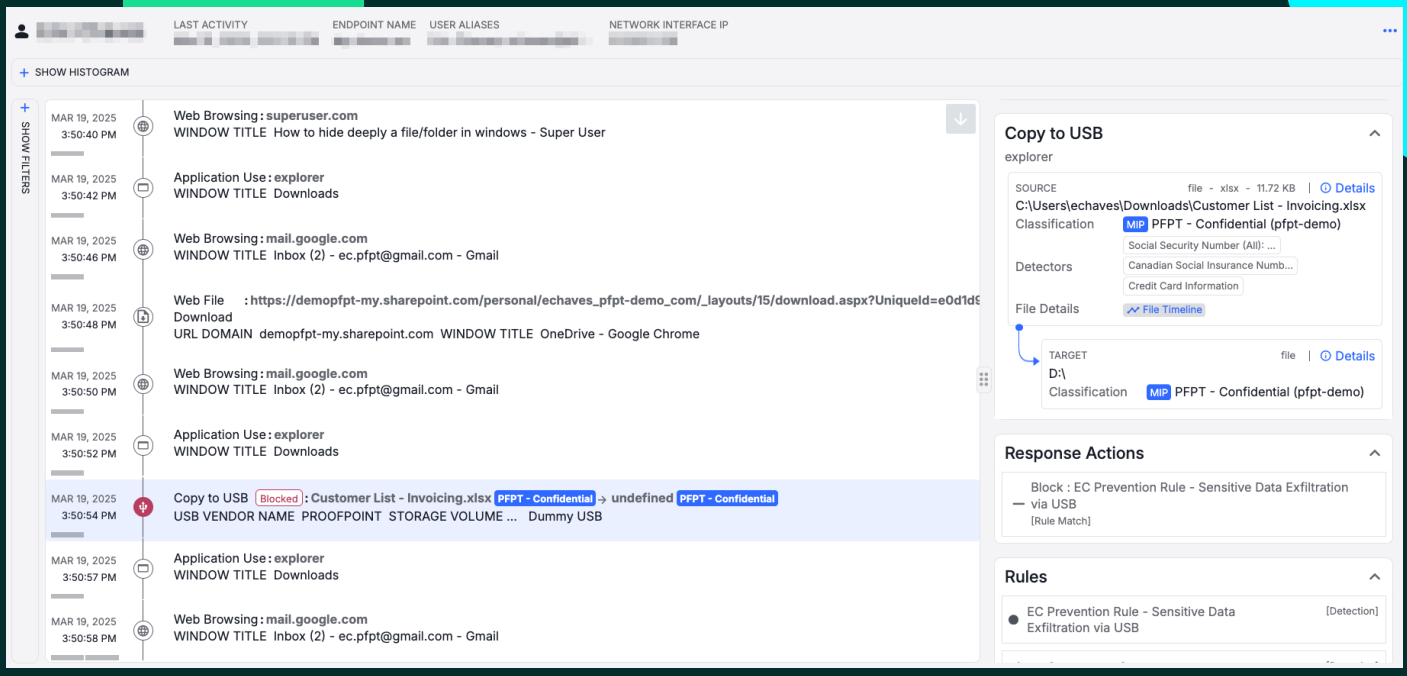

Figura 1. Questo esempio di Data Security Workbench mostra una sequenza a rischio di azioni degli utenti. L'utente cerca dei modi per nascondere un file, scarica un file sensibile da SharePoint e tenta di copiarlo su una chiavetta USB. Le azioni e la tempistica suggeriscono una possibile elusione delle policy, che necessita di ulteriori verifiche.

Applicazione adattiva delle policy e applicazione di misure correttive guidata

Proofpoint offre l'applicazione condivisa delle policy su tutti i canali DLP. I team possono definire le policy una sola volta e applicarle in modo coerente.

Le policy adattive aiutano i team a monitorare gli utenti ad alto rischio, a comprenderne le intenzioni e ad automatizzare le risposte. Quando viene visualizzato un avviso, queste policy raccolgono più metadati e prove visive. Informazioni più chiare consentono agli analisti di condurre indagini più rapidamente e di ridurre il costo totale di proprietà.

Proofpoint previene inoltre la perdita di dati sensibili tramite prompt di IA generativa. La nostra soluzione guida gli utenti verso un utilizzo più sicuro dell'IA. Corregge automaticamente la condivisione estesa di file nelle applicazioni cloud. Richiede inoltre agli utenti di giustificare la copia di dati sensibili in una cartella cloud o in un'unità di rete.

Riduci i costi operativi e accelera la risoluzione degli incidenti

Operazioni DLP efficaci su tutti i canali

I team che utilizzano strumenti DLP obsoleti e isolati si trovano spesso ad affrontare indagini lente, visibilità frammentata e violazioni delle policy non rilevate. Proofpoint centralizza rilevamento, policy e controlli di governance su tutti i canali DLP. Data Security Workbench centralizza anche i dati di telemetria e gli avvisi. Questo aiuta i team a valutare, indagare e rispondere più rapidamente.

La console Data Security Workbench offre i seguenti vantaggi:

- Visualizzazioni cronologiche delle interazioni degli utenti con dati sensibili (vedere la figura 1)
- Gestione unificata degli allarmi e configurazione della DLP (vedere la figura 2)
- Indagini legate a livello di email, cloud, endpoint e applicazioni di IA
- Monitoraggio della tracciabilità dei file al momento della loro creazione, modifica e condivisione
- Tracciamento delle minacce per individuare e analizzare i rischi in anticipo
- Dashboard per dirigenti e report di verifica

Sicurezza proattiva dei dati

Data Security Workbench consente di cercare e filtrare i rischi legati ai dati. Puoi creare viste personalizzate per gestire questi rischi prima che si aggravino. Puoi ricercare i tentativi di sottrazione di dati e altre attività a rischio, come l'utilizzo di applicazioni di IA generativa non approvate. La cronologia degli utenti mostra chi ha fatto cosa, dove, quando e perché.

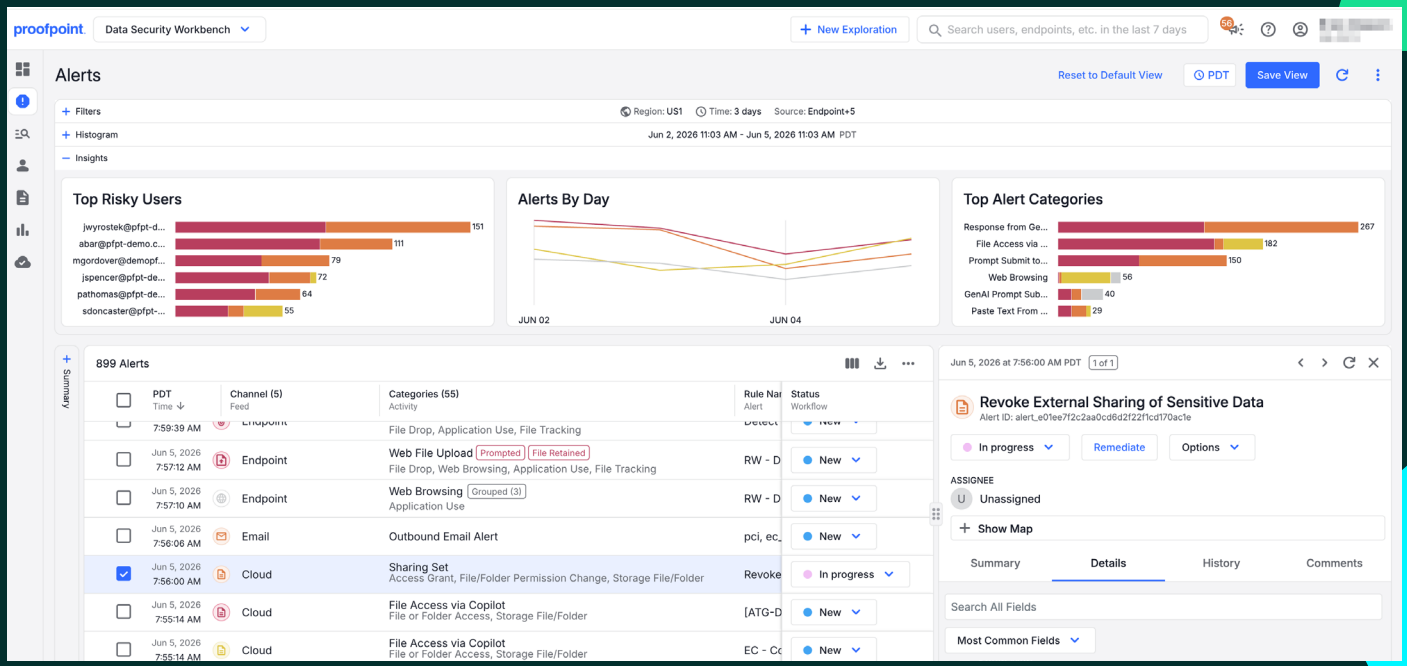

Figura 2. In Data Security Workbench, puoi creare esplorazioni personalizzate dei rischi legati ai dati.

Migliora l'agilità con un'architettura moderna

Le soluzioni Proofpoint vengono fornite come servizi, consentendoti di risparmiare tempo prezioso. Si implementano rapidamente, scalano automaticamente e semplificano la manutenzione. Sono modulari e utilizzano servizi cloud condivisi. Le nostre soluzioni cloud native supportano più tenant e API. Sono progettate per scalare. Possono supportare centinaia di migliaia di utenti per tenant. La piattaforma Proofpoint si integra con partner quali Microsoft, Okta, Splunk e ServiceNow.

Controlli granulari della privacy dei dati

Proofpoint offre una console globale cloud native e può archiviare dati in diverse regioni. I controlli di accesso basati su attributi limitano chi può consultare gli avvisi e le indagini in base al ruolo, alla funzione o alla regione. L'offuscamento dei dati e l'anonimizzazione degli utenti (vedere figura 3) contribuiscono al rispetto delle normative regionali in materia di privacy e residenza dei dati.

Agent endpoint estremamente stabile

Il nostro agent leggero in modalità utente è stabile e rapido da implementare. La sua particolarità risiede nel modo in cui rileva la perdita di dati e le possibili minacce interne. Puoi modificare il comportamento dell'agente aggiornando le policy sulla piattaforma. A differenza degli agent in modalità kernel, l'agente Proofpoint offre un'esperienza utente affidabile. Questo può ridurre il numero di richieste di assistenza e far risparmiare tempo agli amministratori.

Valorizzazione più rapida grazie alla nostra competenza

La prevenzione della perdita di dati richiede competenze tecniche e di prodotto, oltre a solide competenze in materia di governance dei dati. I servizi Proofpoint Applied ti aiutano a ottenere maggiore valore dal tuo investimento, a supportare la continuità operativa e a far evolvere il tuo programma di protezione dei dati.

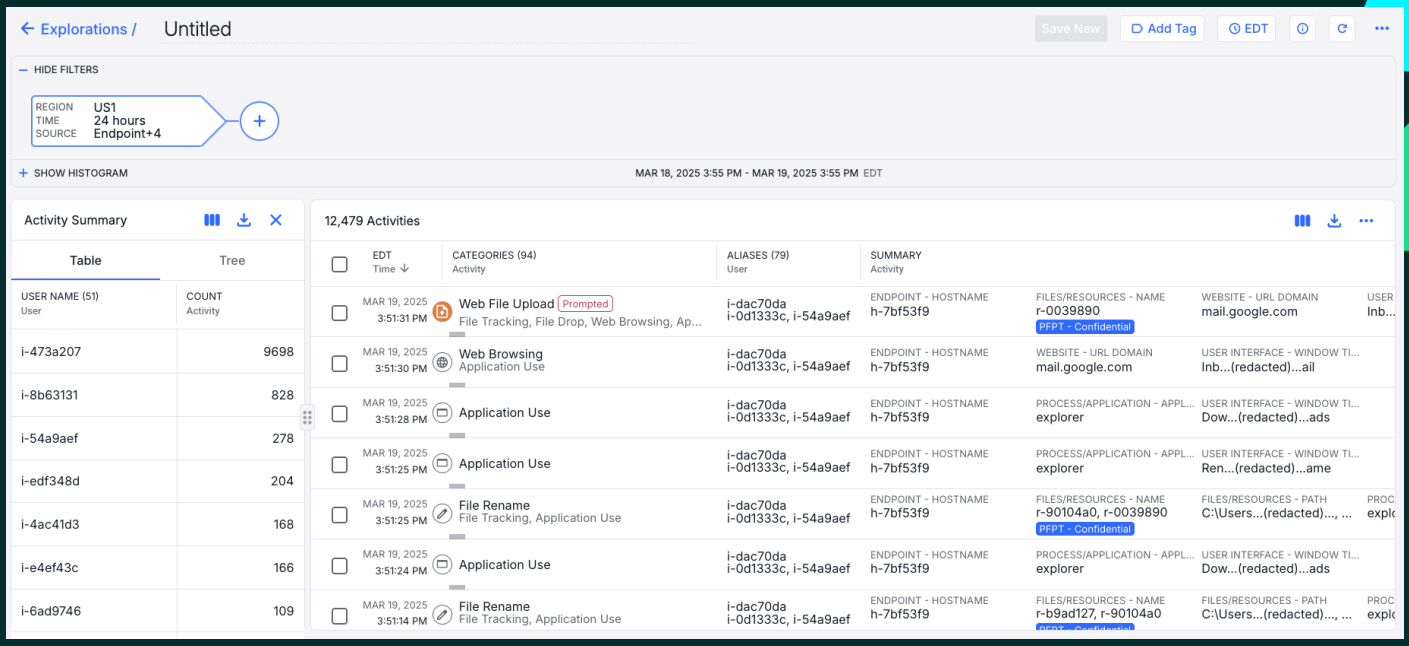

Figura 3. La console è in grado di anonimizzare le informazioni degli utenti durante le indagini. Ciò tutela la privacy e contribuisce a ridurre i pregiudizi degli analisti.

Principali funzionalità	**Proofpoint DLP Transform livello 1**	**Proofpoint DLP Transform livello 2**	**Componenti aggiuntivi**
Contesto dettagliato su utenti e file	✓	✓	
Tracciamento delle minacce per individuarle e indagarle più tempestivamente	✓	✓	
Agent unico configurabile in modalità utente per la gestione delle minacce interne e la DLP	✓	✓	
Rilevatori DLP avanzati (RegEx, OCR, IDM, EDM) e classificazione MIP	✓	✓	
IA pronta all'uso e classificatori autonomi guidati dall'IA	✓	✓	
Tracciabilità dei dati per monitorare e rilevare gli spostamenti dei file	✓	✓	
API, proxy di inoltro e inverso	✓	✓	
Rilevatori estesi delle applicazioni cloud	✓	✓	
Gestione unificata degli allarmi e configurazione della 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 o interne		✓	
Analisi dell'impronta digitale di documenti sensibili nelle email		✓	
Prevenzione basata sull'IA della perdita di dati accidentale e intenzionale tramite l'email			✓
Identificazione e classificazione degli archivi di dati			✓
Rilevamento e riduzione dell'esposizione ai rischi negli archivi di dati			✓
Acquisizione visiva delle minacce interne			✓

Per saperne di più

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

proofpoint.