proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Data Loss Prevention

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

Vantaggi principali

- Prevenzione della perdita di dati a livello di email, cloud e endpoint
- 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 nazionali/regionali in materia di privacy dei dati

Oggi, i collaboratori possono mettere i dati in pericolo in molti modi diversi. Utilizzano sempre più strumenti di produttività non autorizzati come l'IA generativa (GenAI). Utilizzano anche dispositivi personali per accedere alle applicazioni cloud della loro azienda. I team della sicurezza dei dati faticano sempre più a tenere il passo, poiché viene loro chiesto di fare di più con meno per assicurare la privacy dei dati. Allo stesso tempo, le conseguenze delle violazioni dei dati sono sempre più devastanti, che si tratti di perdite finanziarie, danni alla reputazione e mancata conformità alle normative. Le aziende hanno bisogno di una miglior visibilità sui loro dati a livello di email, cloud e endpoint nonché sul comportamento dei loro utenti. Tuttavia, gli strumenti di prevenzione della perdita dei dati (DLP) di vecchia generazione non soddisfano queste esigenze. Ancora peggio, spesso sono isolati, costosi e difficili da mantenere e da scalare.

Le soluzioni Proofpoint Data Loss Prevention (DLP) ti consentono di trasformare il tuo programma e la tua architettura di sicurezza dei dati. Le nostre soluzioni favoriscono un approccio adattivo alla DLP. Puoi così prevenire in modo più efficace la perdita di dati di origine umana a livello di email, cloud e endpoint.

Proofpoint identifica in modo preciso i contenuti sensibili e offre una visibilità estesa sui comportamenti degli utenti. Un'unica console unificata ti aiuta a gestire gli avvisi e indagare sugli incidenti su tutti i canali. Utilizzando analisi potenti, puoi rapidamente valutare i rischi legati ai dati, ottenere verdetti estremamente affidabili e adottare le misure appropriate. Le nostre soluzioni si basano su un'architettura cloud-native che offre controlli moderni della privacy e un agent estremamente stabile. Scalano automaticamente e sono semplici da implementare e gestire.

Riduci i rischi per la sicurezza dei dati a livello di email, cloud e endpoint

Visibilità estesa sui comportamenti degli utenti

Proofpoint monitora il modo in cui i tuoi collaboratori interagiscono con i dati a livello di email, endpoint gestiti e non gestiti e applicazioni cloud come Microsoft 365, Google Workspace e Salesforce. Forniamo informazioni sull'intento degli utenti che ti aiutano a rispondere in modo appropriato ai rischi per i dati. Rileviamo e preveniamo anche la sottrazione di dati sensibili, tra cui la copia di file su una chiavetta USB non autorizzata o il caricamento in una cartella cloud personale.

Tramite l'integrazione con LDAP e Active Directory, Proofpoint ti aiuta a definire e applicare in modo dinamico policy granulari di crittografia delle email. Raccogliamo anche dati di telemetria sui seguenti comportamenti:

- **Manipolazione di file**, come il cambio di nome di file che contengono dati sensibili o la modifica delle loro estensioni
- **Utilizzo di siti web e applicazioni**, come il download di strumenti di backup dei dati o di strumenti di pirateria informatica dal web e loro installazione
- **Comportamenti pericolosi degli utenti più a rischio**, come la manipolazione del registro Windows per disattivare i controlli di sicurezza

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.

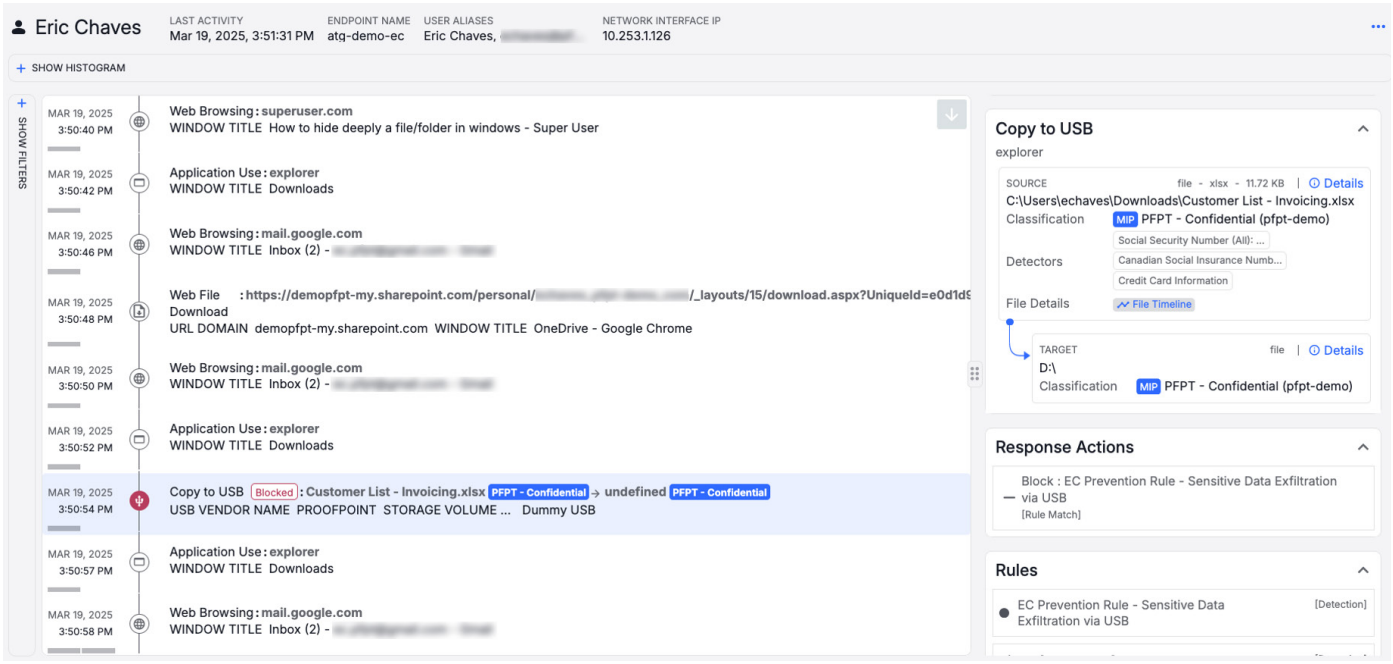

Figura 1. In questa schermata della console Data Security Workbench, un utente visita un sito web dal titolo "How to hide deeply a file/folder in Windows" (Come nascondere un file/cartella in profondità in Windows). L'utente quindi scarica un file da un drive SharePoint dell'azienda. Infine, copia un file riservato denominato "Customer List – invoicing.xlsx" (Elenco dei clienti - fatturazione.xlsx) su una chiavetta USB. La cronologia delle attività dell'utente e l'identificazione di un contenuto sensibile indicano a un analista che l'utente cerca di eludere le policy dell'azienda e che sono necessarie ulteriori indagini.

Identificazione precisa dei contenuti

Proofpoint utilizza metodi avanzati di identificazione dei contenuti per proteggere i tuoi dati. Per esempio, nel cloud, la corrispondenza esatta dei dati e il riconoscimento ottico dei caratteri (OCR) possono rilevare i numero di cartelle cliniche sulle immagini. Ciò può aiutare una struttura sanitaria, per esempio, a ridurre i falsi positivi e i falsi negativi.

Puoi creare delle policy DLP che integrano classificatori basati su modelli linguistici di grandi dimensioni (LLM). Potrai così proteggere i contenuti sensibili sviluppati di recente senza classificazione preventiva e risparmiare tempo. Combinando classificatori LLM corrispondenza dei modelli puoi ridurre i falsi positivi.

Gli avvisi LLM semplificano la categorizzazione dei documenti. Per esempio, se la corrispondenza di modelli di numeri della previdenza sociale attivare un allarme, Proofpoint può stabilire se il documento in questione è una dichiarazione d'imposta, un modulo del paziente o una richiesta di credito, accelerando così la classificazione per priorità e le indagini.

Applicazione adattativa delle policy

Grazie alle informazioni sul comportamento degli utenti e sullo spostamento dei dati sensibili, puoi rispondere ai rischi legati ai dati con maggior precisione. Proofpoint previene la perdita di dati sensibili attraverso prompt di IA generativa. Le nostre soluzioni insegnano agli utenti a modificare il loro comportamento, favorendo anche un utilizzo accettabile dell'IA. Correggono automaticamente la condivisione estesa dei file nelle applicazioni cloud. Richiedono inoltre agli utenti di fornire una giustificazione quando copiano dei dati sensibili in una cartella cloud o su un drive di rete.

Le regole adattive ti consentono di monitorare gli utenti a alto rischio più da vicino. Disponi così di un contesto approfondito e di una miglior comprensione delle intenzioni dei tuoi utenti. Invece di adattare manualmente le policy, puoi automatizzare la risposta ai comportamenti a rischio. Queste regole dinamiche ti permettono di raccogliere metadati aggiuntivi e prove visive delle attività degli utenti quando viene generato un avviso. Grazie a una maggior visibilità e informazioni fruibili, acceleri il processo di indagine e riduci il tuo costo totale di possesso.

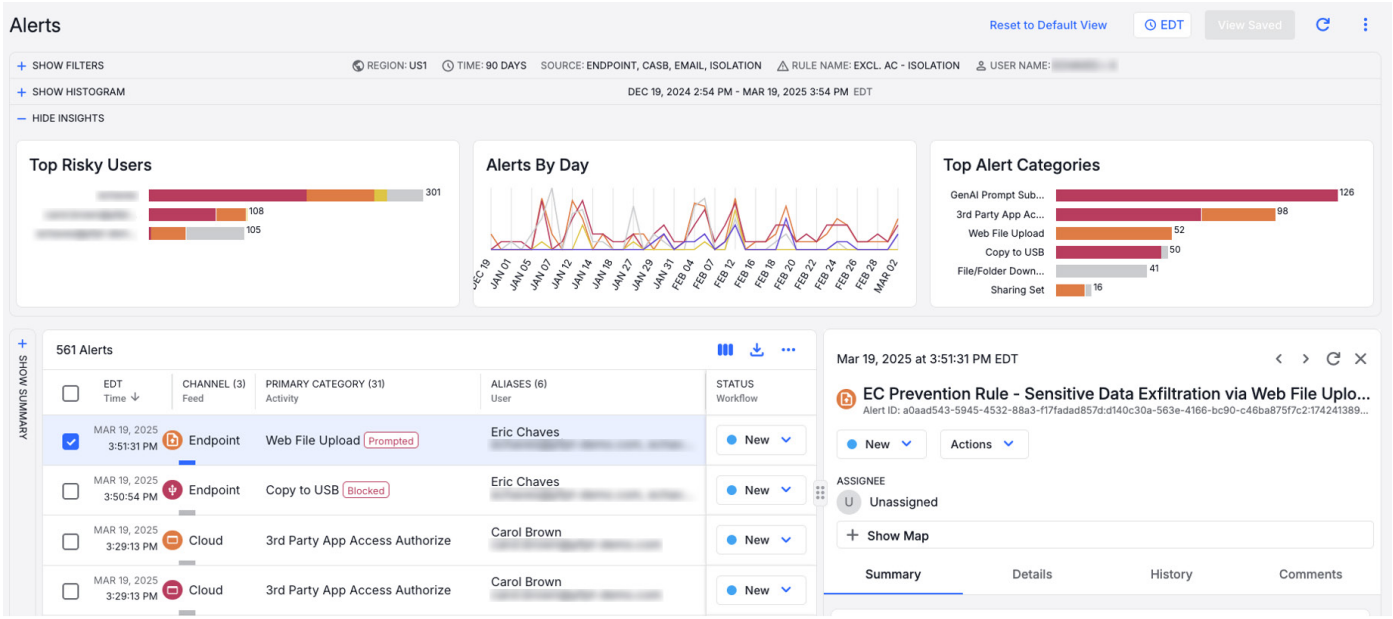

Figura 2. La console Data Security Workbench razionalizza la gestione degli avvisi a livello di email, cloud e endpoint, in modo che tu non debba passare da una console all'altra. In questo esempio, un analista ha filtrato gli avvisi per un utente specifico. La console mostra che l'utente ha scaricato dati sensibili sul suo account email aziendale e ha poi cercato di copiare un file su una chiavetta USB prima di essere bloccato.

Riduci i costi operativi e accelera la risoluzione degli incidenti

Operazioni DLP efficaci su tutti i canali

I team della sicurezza che utilizzano strumenti DLP isolati o di vecchia generazione possono subire un allungamento dei tempi di indagine e non rilevare le violazioni delle policy. Per offrirti una visibilità multicanale completa sui rischi per i dati in modo centralizzato, Proofpoint acquisisce dati di telemetria a livello di applicazioni cloud, endpoint e email. Ciò consente di razionalizzare la classificazione degli avvisi per priorità su tutti i canali e di accelerare le indagini e la risposta agli incidenti. La console Data Security Workbench fornisce analisi potenti, visualizzazioni intuitive e flussi di lavoro efficienti che ti aiutano a:

- Indagare sulle interazioni degli utenti con i dati all'interno di una vista cronologica per stabilire le loro intenzioni e il loro livello di rischio (figura 1)
- Classificare per priorità e correlare gli avvisi (figura 2)
- Tracciare il ciclo di vita di un file (creazione, modifica, condivisione)
- Coordinare la risposta agli incidenti
- Utilizzare dei report di sintesi pronti all'uso per dimostrare l'efficacia e la copertura nonché generare report personalizzati a fini di verifica
- Implementare e gestire policy DLP coerenti e controlli amministratore per l'accesso ai dati e la privacy su tutti i canali

Sicurezza proattiva dei dati

La console Data Security Workbench dispone di una funzionalità avanzata di ricerca e filtraggio. Ti aiuta a creare esplorazioni personalizzate affinché tu possa gestire i rischi per i dati in modo proattivo. 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 delle attività degli utenti ti aiuta a comprendere tutte le informazioni (chi, cosa, dove, quando e perché) di ogni incidente di sicurezza.

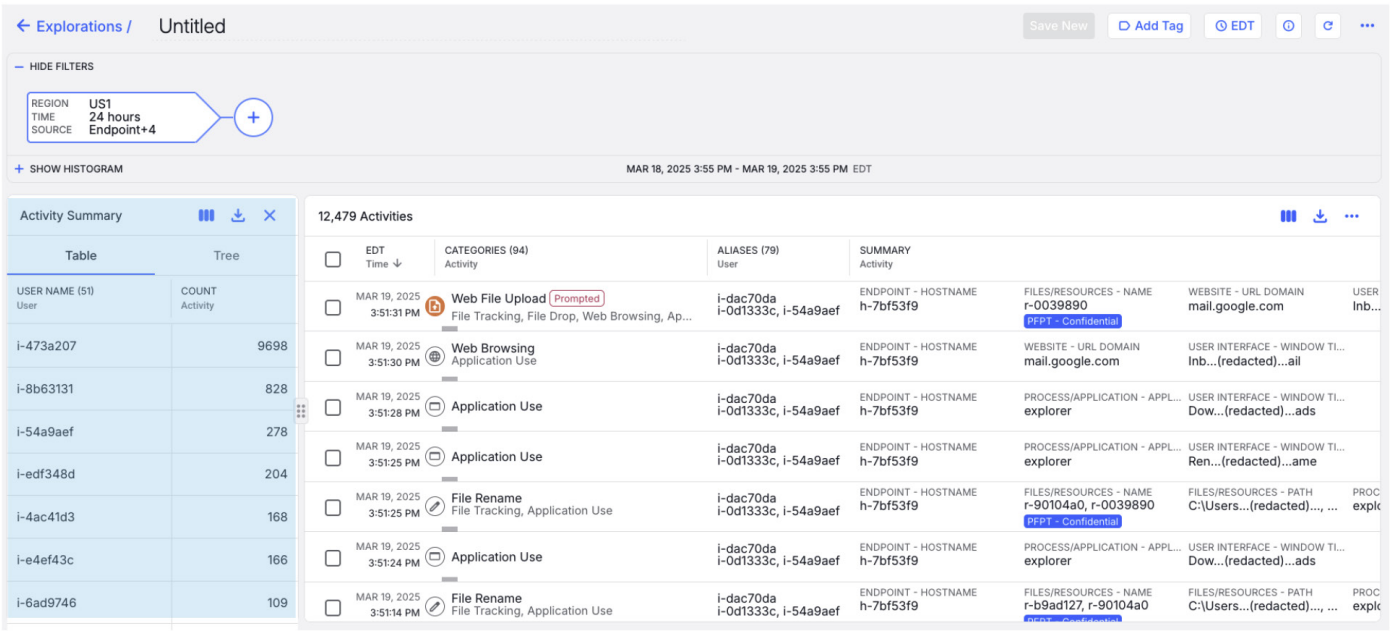

Figura 3. Come si evince dalla schermata, la console anonimizza i nomi degli utenti. Ciò protegge la privacy degli utenti che sono sotto indagine e elimina i bias da parte degli analisti.

Migliora l'agilità con un'architettura moderna

Disponibili come servizi, le nostre soluzioni ti consentono di risparmiare tempo prezioso. Si implementano rapidamente, scalano automaticamente e facilitano la manutenzione. Sono modulari e offrono servizi condivisi nel cloud. Le nostre soluzioni multi-tenant cloud native sono basate su un'API e sono estremamente scalabili. Possono supportare centinaia di migliaia di utenti per tenant. La piattaforma Proofpoint supporta le integrazioni di API con partner dell'ecosistema come Microsoft, Okta, Splunk e ServiceNow.

Controlli granulari della privacy dei dati

Anche se Proofpoint offre una console globale cloud native, può archiviare dati in diverse regioni. Puoi utilizzare controlli d'accesso basati su attributi per gestire gli avvisi e le indagini per tutte le funzioni e i ruoli regionali. Puoi anche mascherare i dati sensibili e anonimizzare le informazioni che permettono di identificare gli utenti (figura 3). Potrai così rispettare i requisiti specifici di ogni area del mondo in termini di residenza e riservatezza dei dati.

Agent endpoint estremamente stabile

Il nostro agent leggere in modalità utente è stabile e rapido da implementare. È in grado di rilevare le perdite di dati e migliorare la tua visibilità sulle potenziali minacce interne. Modificando le policy nella piattaforma, puoi modificare il comportamento dell'agent. A differenza degli agent in modalità kernel, l'agent Proofpoint offre un'esperienza utente affidabile. Riduci così il numero dei ticket dell'assistenza e permetti agli amministratori di risparmiare tempo.

Valorizzazione più rapida grazie alla nostra competenza

La prevenzione della perdita di dati non è un'impresa da poco. Richiede conoscente tecniche e di prodotto, nonché di una comprensione approfondita della governance e dell'amministrazione dei dati. Proofpoint può diventare il tuo partner affidabile per assicurare il successo del tuo programma DLP. I nostri servizi Applied ti offrono la competenza di cui hai bisogno per ottimizzare il tuo investimento tecnologico, supportare la continuità delle tue operazioni e far evolvere la tua strategia di protezione dei dati.

Principali funzionalità delle soluzione Proofpoint DLP

Confronta le nostre soluzioni per trovare la più adatta al tuo azienda.

PRINCIPALI FUNZIONALITÀ	PROOFPOINT DLP TRANSFORM	PROOFPOINT DLP TRANSFORM ADVANCED	COMPONENTI AGGIUNTIVI
Contesto dettagliato su utenti e file	✓	✓	
Tracciamento delle minacce per 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 la tracciabilità dei dati	✓	✓	
API, proxy di inoltro e inverso	✓	✓	
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		✓	
Prevenzione basata sull'IA della perdita di dati accidentale e intenzionale tramite l'email			✓
Identificazione e classificazione degli archivi di dati			✓
Rilevamento e correzione dei rischi di esposizione negli archivi di dati			✓
Acquisizione visiva delle minacce interne			✓

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

SCOPRI LA PIATTAFORMA PROOFPOINT →