Proofpoint Endpoint DLP e Proofpoint ITM

Beneficia di una protezione incentrata sulle persone contro la perdita di dati e le minacce interne a livello di endpoint

Vantaggi principali

- Riduzione del rischio di perdita di dati sensibili e di minacce interne
- Semplificazione della risposta agli incidenti di perdita di dati e alle violazioni alle policy
- Valorizzazione più rapida dei programmi di prevenzione delle minacce interne e delle perdite di dati

Le perdite di dati non avvengono per magia. Sono sempre innescate dalle persone. Questo è il motivo per cui i prodotti Proofpoint Endpoint Data Loss Prevention (DLP) e Proofpoint Insider Threat Management (ITM) adottano un approccio incentrato sulle persone per gestire le minacce interne e prevenire la perdita di dati a livello di endpoint.

Aiutano i team dedicati all'IT e alla sicurezza informatica a svolgere le seguenti attività:

- Identificare i comportamenti a rischio degli utenti e gli spostamenti di dati sensibili sospetti
- Rilevare e prevenire gli incidenti di sicurezza di origine interna e le perdite di dati dagli endpoint
- Rispondere più rapidamente agli incidenti causati dagli utenti

Quando si verificano degli incidenti di sicurezza o di perdita di dati di origine interna, è necessario essere in grado di analizzarli e bloccarli rapidamente. Più rapidamente si pone rimedio a un incidente, minore è il danno per l'azienda, il marchio e i risultati finanziari.

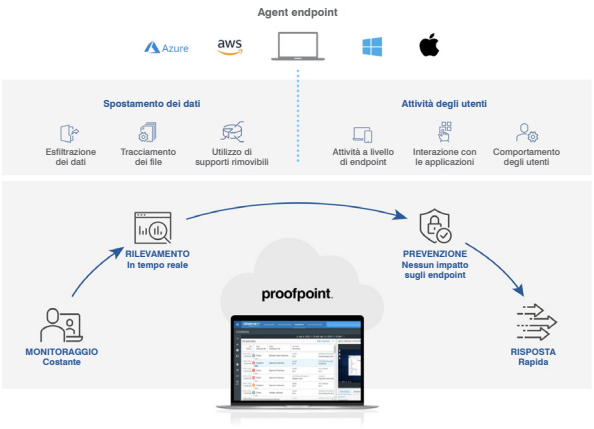

Figura 1. L'efficacia di Proofpoint Endpoint DLP e Proofpoint ITM si basa sugli stessi sensori.

Quando anche ogni secondo conta, visibilità, rilevamento, prevenzione e contesto sono fondamentali. Gli strumenti DLP legacy offrono una visibilità limitata sugli incidenti causati dagli utenti. Non rilevano i segnali critici di esfiltrazione non approvata dei dati e di altre violazioni delle policy. Inoltre, non forniscono le informazioni contestuali necessarie (chi, cosa, dove, quando e perché) per distinguere gli allarmi e gli eventi sospetti dalla normale attività aziendale.

Proofpoint Endpoint DLP e Proofpoint ITM estendono le funzionalità della piattaforma Proofpoint Information and Cloud Security all'endpoint. Grazie alla loro architettura moderna, leggera e condivisa, questi prodotti permettono di gestire i comportamenti a rischio a livello degli endpoint con le seguenti funzionalità:

- Visibilità e contesto sull'attività degli utenti e lo spostamento dei dati
- Identificazione dei contenuti sensibili spostati dagli utenti dall'endpoint
- Rilevamento e segnalazione dei comportamenti a rischio degli utenti e degli spostamenti dei dati in tempo reale
- Prevenzione di esfiltrazione dei dati a rischio dall'endpoint
- Velocizzazione della risposta agli incidenti e delle relative indagini
- Semplificazione dell'implementazione grazie a un sistema di backend esclusivamente SaaS e a un'architettura di agent leggera

Visibilità e contesto sulle attività degli utenti e sugli spostamenti dei dati

Per valutare i rischi di un'azienda è fondamentale comprendere il contesto relativo alle attività digitali degli utenti. Ma l'analisi dei file di log può richiedere troppo tempo e in genere non fornisce le informazioni di cui i tuoi esperti analisti hanno bisogno per intervenire.

Visibilità con Proofpoint Endpoint DLP

Proofpoint Endpoint DLP raccoglie dati telemetrici sulle interazioni degli utenti con i dati sui loro endpoint. Non si limita a segnalare ai team IT e della sicurezza gli spostamenti di dati sospetti. Fornisce informazioni relative al contesto attraverso una vista cronologica che mostra come gli utenti accedono ai dati e ai file, li spostano e li utilizzano. La telemetria si concentra sugli elementi seguenti:

- Identificazione dei dati sensibili tramite l'analisi dei contenuti a livello di endpoint e la lettura delle etichette di classificazione dei dati (comprese quelle di Microsoft Information Protection)

Figura 2. Contesto sui movimenti di file e dati, dall'origine fino alla destinazione.

- Interazione dell'utente con file e dati (tagliare, incollare, copiare, rinominare, spostare, ecc.)
- Nome, estensione e dimensione dei file
- Etichette per la classificazione dei dati (basate sulle etichette di Microsoft Information Protection)
- Tracciamento di file e dati (origine, posizione intermedia, destinazione, ecc.)
- Canale di esfiltrazione (nome di dominio e URL se i dati sono stati spostati tramite un canale web, ecc.)
- Contenuti degli appunti del sistema operativo

Questo approccio incentrato sulle persone offre una visibilità più granulare sull'interazione dei tuoi utenti con i tuoi dati sensibili rispetto a quella fornita dagli strumenti DLP per gli endpoint tradizionali. Inoltre, gli strumenti DLP legacy non forniscono visibilità sullo spostamento dei dati, a meno che un'azione non faccia scattare un allarme. Inoltre non correlano gli utenti alle azioni. A causa di queste carenze, ti saresti perso gli spostamenti di dati apparentemente innocui che, contestualizzati, sono indicativi di comportamenti pericolosi.

Visibilità con Proofpoint ITM

Per comprendere il contesto degli incidenti causati dagli utenti, è necessario avere visibilità su tutte le loro attività, inclusi gli spostamenti di dati. Ecco perché Proofpoint ITM offre una visibilità più completa sulle attività a livello di endpoint. Oltre gli spostamenti dei dati acquisiti da Proofpoint Endpoint DLP, Proofpoint ITM ti fornisce le seguenti informazioni:

- Come gli utenti accedono alle applicazioni web, ai supporti rimovibili, alle applicazioni virtuali e ai desktop e come li utilizzano
- Utilizzo del mouse e della tastiera a livello dell'endpoint
- Acquisizione di schermate delle attività a livello dell'endpoint

Insieme, questi elementi permettono di comprendere tutti gli aspetti positivi e negativi (chi, cosa, dove, quando e perché) delle attività a rischio. Grazie a queste informazioni contestuali, puoi comprendere meglio le intenzioni degli utenti in caso di perdita di dati o di violazione delle policy.

Contesto delle minacce

La visualizzazione del contesto delle minacce che colpiscono gruppi di utenti specifici può aiutarti a gestire meglio i rischi legati agli utenti. I nostri prodotti per gli endpoint consentono di creare elenchi di controllo degli utenti sulla base di criteri come i seguenti:

- Sensibilità del ruolo dell'utente e dei dati con cui interagisce
- Vulnerabilità dell'utente al phishing e ad altre tecniche di social engineering
- Posizione dell'utente
- Variazioni delle funzioni dell'utente
- Altri fattori legali e legati alle risorse umane

Analisi dei contenuti e classificazione dei dati

Puoi identificare i dati sensibili in movimento, quando sono più vulnerabili, grazie all'analisi dei contenuti in movimento e alla lettura dei tag di classificazione dei dati, come quelli di Microsoft Information Protection.

Sfruttando gli investimenti esistenti in materia di classificazione dei dati, puoi identificare le informazioni aziendali sensibili come la proprietà intellettuale senza creare un flusso di lavoro separato per i team di sicurezza e gli utenti finali.

Nei casi in cui la classificazione dei dati non permette di identificare i dati regolamentati e i dati dei clienti in modo affidabile, puoi sfruttare i rilevatori di contenuti comprovati e all'avanguardia di Proofpoint CASB e Proofpoint Email DLP. Puoi eseguire la scansione dei contenuti mentre gli utenti li spostano via web, dispositivi USB e cartelle di sincronizzazione cloud.

Rilevamento in tempo reale dei comportamenti a rischio degli utenti e dei movimenti di dati sospetti

Biblioteca degli allarmi

Proofpoint Endpoint DLP e Proofpoint ITM includono librerie di allarmi pronte all'uso che semplificano la configurazione e velocizzano la valorizzazione. Sia Proofpoint ITM che Proofpoint Endpoint DLP possono avvisarti di interazioni e spostamenti di dati sospetti a livello dell'endpoint. Inoltre, Proofpoint ITM è in grado di segnalarti una gamma più ampia di minacce interne.

Biblioteca degli allarmi Proofpoint Endpoint DLP e Proofpoint ITM

SPOSTAMENTO DEI DATI	ATTIVITÀ DEGLI UTENTI (SOLO PROOFPOINT ITM)
Oltre 40 avvisi relativi a interazioni con i dati e la loro esfiltrazione, tra cui: • Caricamento di file sul web • Copia di file su chiavette USB • Copia di file in una cartella di sincronizzazione cloud locale • Stampa di file • Copia e incolla di file/cartelle/testo • Attività svolte su file (ridenominazione, copia, spostamento, cancellazione) • Tracciamento dei file (da Web a USB, da Web a Web, ecc.) • Download di file dal Web • Invio di un file come allegato email • Download di un file da un'email/endpoint	Oltre 100 avvisi relativi a una vasta gamma di attività degli utenti a livello di endpoint, tra cui: • Mascheramento delle informazioni • Accesso non autorizzato • Aggiramento dei controlli di sicurezza • Negligenza • Creazione di una backdoor • Violazione del copyright • Strumenti di comunicazione non autorizzati • Compito amministrativo non autorizzato • Attività DBA non autorizzate • Preparazione di un attacco • Sabotaggio informatico • Elevazione dei privilegi • Furto di identità • Attività GIT sospette • Utilizzo inaccettabile

Motore di regole flessibile

Puoi creare regole e allarmi personalizzati in base al tuo ambiente partendo da zero o adattare i nostri scenari delle minacce predefiniti. Inoltre puoi modificare gli scenari per gruppi di utenti, applicazioni, data/ora, categorie dei siti web e grado di sensibilità, etichette di classificazione, fonti e destinazioni, canali di spostamento e tipo di dati.

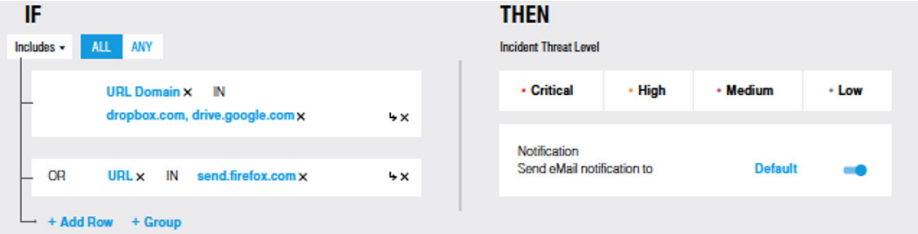

Figura 3. Impostazione di avvisi grazie a semplici istruzioni di tipo if-then.

Tracciamento delle minacce con un semplice clic

Le nostre potenti funzionalità di ricerca e filtraggio ti aiutano a tracciare in modo proattivo le minacce grazie a esplorazioni dei dati personalizzate. Puoi ricercare le attività e i comportamenti a rischio relativi alla tua azienda o imparare a conoscere i nuovi rischi. Come con le nostre funzionalità di rilevamento, puoi adattare uno dei modelli di esplorazione delle minacce pronti all'uso o crearne uno tuo.

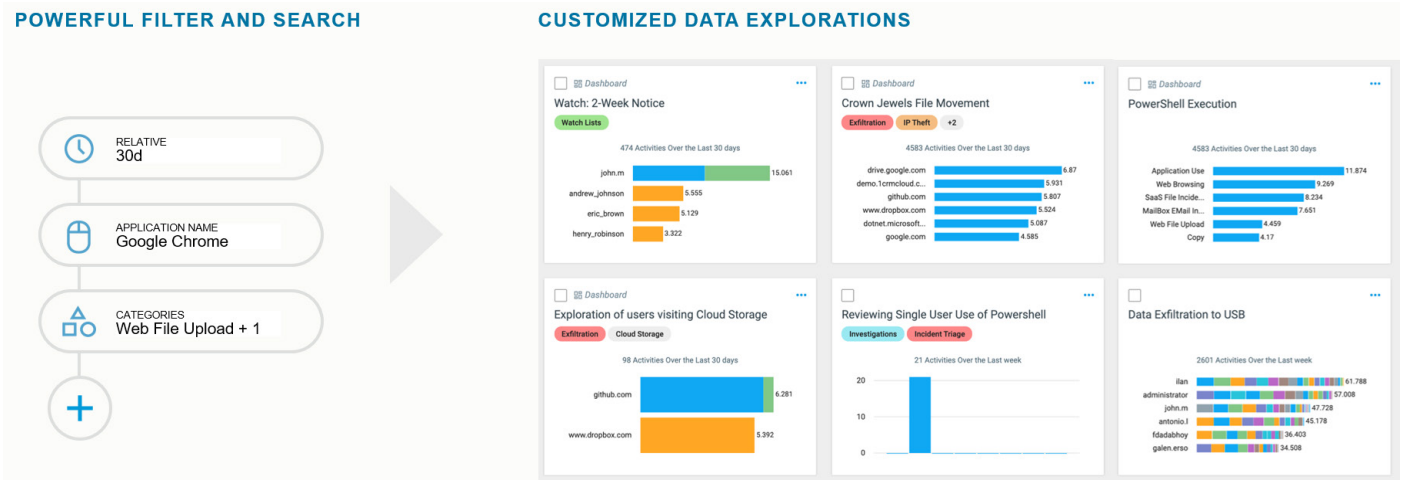

Figura 4. Tracciamento di comportamenti potenzialmente pericolosi o insoliti.

Prevenzione di esfiltrazioni non autorizzate di dati dall'endpoint

Rilevare i comportamenti a rischio degli utenti e gli spostamenti di dati sospetti non è sempre sufficiente. Devi anche bloccare la perdita di dati in tempo reale. La nostra piattaforma ti permette di prevenire le interazioni non conformi alle policy degli utenti con dati sensibili tra cui:

- Trasferimento verso e da dispositivi USB
- Sincronizzazione di file con altri terminali e il cloud

Personalizza la prevenzione in base a utenti, gruppi di utenti, gruppi di endpoint, nomi di processi, dispositivi USB, numeri di serie USB, etichette di classificazione dei dati, URL sorgenti e risultati dell'analisi del contenuto. Puoi estendere le funzionalità DLP all'email, al cloud e alle applicazioni Web con altri componenti della piattaforma Proofpoint Information and Cloud Security.

Supporto per la risposta agli incidenti e alle indagini

Indagare e risolvere gli allarmi causati dagli utenti interni può essere un processo lungo e costoso. Inoltre, spesso coinvolge anche dipartimenti non tecnici come le risorse umane, la conformità, l'ufficio legale e i responsabili delle divisioni.

Proofpooint Endpoint DLP e Proofpoint ITM si basano sulla piattaforma Proofpoint Information and Cloud Security per aiutarti a semplificare la risposta agli incidenti e le indagini sugli incidenti attribuibili agli utenti.

Ottieni tre potenti funzionalità:

- Visualizzazione di dati contestuali di facile comprensione
- Esportazione e condivisione con le risorse umane per flussi di lavoro più fluidi
- Acquisizione delle schermate opzionale delle attività degli utenti (solo Proofpoint ITM)

Acquisizione delle schermate (solo Proofpoint ITM)

Quando si tratta di indagini sulla sicurezza e sulla perdita di dati, un'immagine a volte vale più di mille parole. Proofpoint ITM permette di acquisire schermate delle attività degli utenti. Ciò fornisce ai responsabili delle risorse umane, dell'ufficio legale e di divisione delle prove chiare e indiscutibili di comportamenti dolosi o negligenti, in modo che possano prendere decisioni informate.

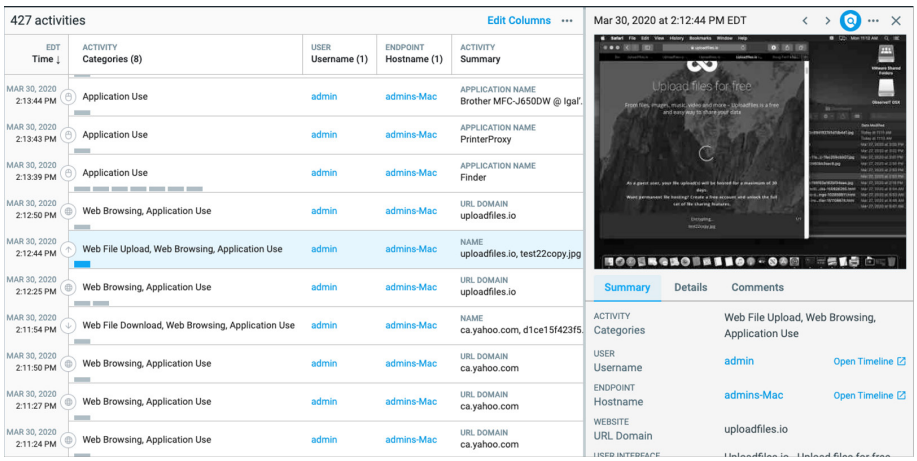

Figura 5. Vista cronologica delle attività dell'utente con acquisizione della schermata dell'endpoint dell'utente.

Classificazione degli avvisi per priorità

Le visualizzazioni dei dati nella piattaforma Proofpoint Information and Cloud Security forniscono informazioni contestuali sugli incidenti imputabili agli utenti in un modo comprensibile anche dai team non tecnici. Le viste cronologiche aiutano a correlare gli avvisi e gli incidenti, e la potente funzionalità di ricerca aiuta i team a estrarre rapidamente i dati rilevanti. I team della sicurezza possono identificare rapidamente quali eventi necessitano di ulteriori indagini e quali possono chiudere immediatamente.

Flusso di lavoro dell'indagine

Il flusso di lavoro principale e le funzionalità di condivisione delle informazioni integrate nella piattaforma Proofpoint Information and Cloud Security semplificano la collaborazione interfunzionale. Puoi esportare i record delle attività a rischio per diversi eventi in file di formato comune, come ad esempio dei PDF. Grazie a Proofpoint ITM, queste esportazioni in formato PDF dalla piattaforma includono screenshot e informazioni contestuali.

Semplificazione dell'implementazione grazie a una distribuzione esclusivamente SaaS e a un'architettura di agent leggera

Proofpoint Endpoint DLP e Proofpoint ITM si basano su agent endpoint condivisi e sulla nostra moderna piattaforma nativa nel cloud Proofpoint Information and Cloud Security. Per Proofpoint Endpoint DLP, l'agent cattura gli spostamenti dei dati. Per Proofpoint ITM, l'agent acquisisce gli spostamenti dei dati e le attività degli utenti.

Architettura di agent leggera

Proofpoint Endpoint DLP and Proofpoint ITM sono basati su agent endpoint leggeri e condivisi che raccolgono la maggior parte dei dati di telemetria in modalità utente. In altre parole, funzionano in parallelo con le transazioni degli endpoint, senza interferire con esse. I prodotti intercettano unicamente le transazioni durante le azioni di prevenzione delle perdite dei dati. L'agent non ostacola la produttività dell'utente e non entra in conflitto con altri strumenti di sicurezza a livello di kernel. Fornisce anche una visibilità indipendente dalle applicazioni sull'attività degli utenti sui loro endpoint.

Facile integrazione in ambienti di sicurezza complessi

L'architettura della piattaforma Proofpoint Information and Cloud Security è guidata da microservizi. I webhook integrati nella nostra piattaforma permettono ai tuoi strumenti SIEM e SOAR di assorbire gli allarmi di Proofpoint Endpoint DLP e Proofpoint ITM, permettendoti di identificare e ordinare per priorità gli incidenti più velocemente.

Le aziende con infrastrutture di sicurezza complesse possono avere la necessità di mantenere una sola fonte di riferimento per tutti i sistemi. Semplifichiamo questo processo grazie all'esportazione automatica dei dati di Proofpoint Endpoint DLP e Proofpoint ITM in spazi di archiviazione AWS S3 di tua proprietà e gestione.

Funzionamento di Proofpoint Endpoint DLP e Proofpoint ITM

La gestione delle minacce interne e la prevenzione della perdita di dati a livello dell'endpoint è fondamentale nell'ambiente competitivo attuale. Tuttavia, la maggior parte delle aziende non ha bisogno di acquisire costantemente dati telemetrici su tutte le attività di tutti gli utenti.

Piuttosto, raccomandiamo un approccio più adattivo e basato sui rischi. Otterrai così informazioni su alcune attività per tutti gli utenti e su tutte le attività di alcuni utenti (quelli con il livello di rischio più elevato). Tra questi utenti possono essere inclusi i dipendenti presenti su un elenco di sorveglianza, utenti con privilegi elevati, collaboratori esterni e utenti mirati come i dirigenti.

I nostri prodotti ti offrono tale flessibilità. Utilizzando un unico set di policy e lo stesso agent endpoint, è possibile:

- Limitare la raccolta alle attività legate ai dati sensibili con Proofpoint Endpoint DLP
- Includere informazioni contestuali sugli utenti con un rischio elevato con Proofpoint ITM

Con una semplice modifica della configurazione delle policy, puoi regolare la quantità e il tipo di dati acquisiti per ogni utente o gruppo di utenti. Questo approccio adattivo ti aiuta a analizzare gli allarmi e a rispondere in modo più efficace, senza raccogliere una quantità astronomica di dati.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint 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 più della metà delle Fortune 1000, 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**.