proofpoint.

PANORAMICA SULLA SOLUZIONE

Proofpoint Insider Threat Management

Proteggi la tua azienda dagli utenti interni a rischio

Vantaggi principali

- Difesa contro i danni finanziari e al marchio causati da utenti interni negligenti, malintenzionati e compromessi
- Rilevamento proattivo dei comportamenti a rischio grazie a una visibilità granulare sugli indicatori comportamentali
- Accelerazione delle indagini grazie a prove inconfutabili
- Collaborazione efficace con le risorse umane, l'ufficio legale e le altre parti interessate
- Protezione della privacy degli utenti finali e garanzia di obiettività durante le indagini
- Valorizzazione rapida grazie a una distribuzione semplice e a un agent endpoint leggero

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.

Il personale moderno e distribuito lavora da qualsiasi luogo. I collaboratori, le terze parti e i fornitori non hanno mai avuto accesso a così tanti dati, sia sui loro dispositivi, nell'email o nel cloud. I cambiamenti organizzativi, come fusioni e acquisizioni, cessioni e ristrutturazioni, causano un'incertezza che può innescare minacce interne. Le tensioni geopolitiche ed economiche d'altro canto favoriscono lo spionaggio informatico condotto da utenti interni.

Queste dinamiche aumentano i rischi di minacce interne che possono portare al furto di segreti commerciali e proprietà intellettuale, frode, spionaggio e sabotaggio dei sistemi. Tutte queste minacce possono causare danni materiali, finanziari, reputazionali e strategici a un'azienda. Per affrontare efficacemente i rischi interni, i team della sicurezza hanno bisogno di informazioni contestuali sui comportamenti a rischio.

Proofpoint Insider Threat Management (ITM) offre una visibilità completa sugli utenti interni negligenti, malintenzionati e compromessi. Aiuta i team della sicurezza a identificare i comportamenti a rischio e a indagare in modo efficiente sugli incidenti di origine interna. Proofpoint ITM offre un approccio incentrato sulle persone fornendo informazioni granulari sul comportamento e sulle intenzioni degli utenti. Ti consente di definire delle policy, ordinare per importanza gli avvisi, monitorare le minacce e rispondere agli incidenti da una console centralizzata. Grazie a prove forensi, puoi indagare in modo rapido e efficiente sulle violazioni di origine interna. Più rapidamente si risolve un incidente, minore è il danno per la tua azienda, il tuo marchio e i tuoi risultati finanziari.

Riduci proattivamente i rischi per la sicurezza

Visibilità completa sui rischi legati agli utenti

Le minacce interne possono provenire da qualsiasi posto e in qualsiasi momento. Questo le rende una delle principali preoccupazioni di sicurezza informatica dei CISO di tutto il mondo. Utilizzando Proofpoint Human Risk Explorer (HRE) con Proofpoint ITM, puoi visualizzare il punteggio dei segnali di rischio correlati per identificare e ridurre in modo proattivo i rischi emergenti. Proofpoint HRE offre una comprensione completa dei rischi legati agli utenti analizzando diverse dimensioni in un unico luogo. Queste includono le vulnerabilità, i comportamenti, l'esposizione agli attacchi, la gestione dei dati sensibili, la sensibilizzazione alla sicurezza e l'identità dei collaboratori.

Proofpoint HRE utilizza anche informazioni basate sui dati per formulare raccomandazioni. Ad esempio, se un utente adotta un comportamento rischioso, come il download di grandi volumi di informazioni sensibili, è possibile intervenire immediatamente applicando controlli di sicurezza più rigorosi, assegnando formazione mirata o rafforzando il monitoraggio. Concentrandoti in primis sugli utenti ad alto rischio, puoi ridurre significativamente i rischi di incidenti e migliorare il tuo livello di sicurezza complessivo.

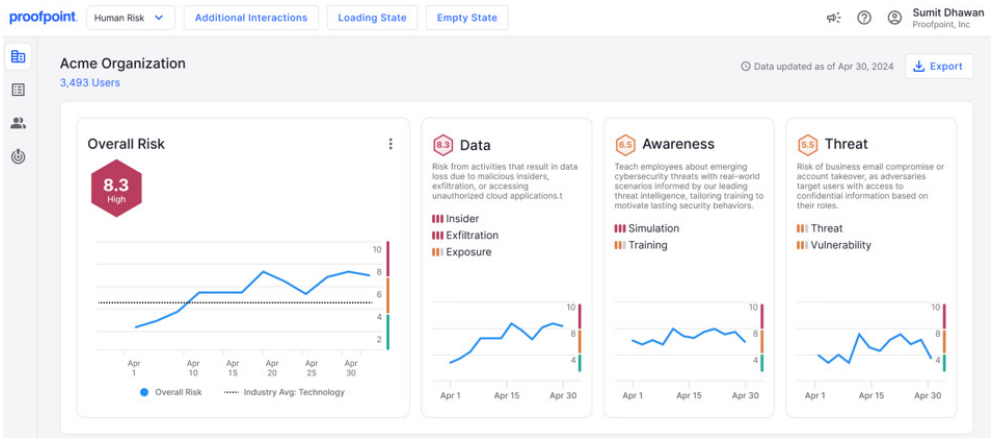


Figura 1. Utilizzando Proofpoint Human Risk Explorer, puoi comprendere facilmente il rischio complessivo per la tua azienda e confrontarlo con quello di altri protagonisti del settore. Puoi anche ottenere informazioni sui rischi associati agli utenti interni, alle sottrazioni di dati e all'esposizione dei dati.

Approccio adattivo basato sui rischi

Per mitigare i rischi interni, la maggior parte delle aziende identifica i gruppi di rischio comuni. Si tratta di individui o team i cui ruoli, comportamenti o circostanze suggeriscono che potrebbero rappresentare un rischio maggiore per l'integrità dei sistemi e dei dati. I gruppi di rischio comuni includono i collaboratori in procinto di lasciare l'azienda, i nuovi assunti, gli utenti con accesso con privilegi, i dirigenti, i collaboratori, gli utenti più inclini a farsi ingannare e altri ancora.

Ma che dire degli utenti a rischio sconosciuti? La maggior parte delle aziende non ha bisogno di raccogliere costantemente dati di telemetria su tutte le attività di tutti gli utenti. Al contrario, Proofpoint propone un approccio adattivo basato sui rischi. Le policy statiche e manuali vengono sostituite da policy che si adattano automaticamente in tempo reale, in base al comportamento degli utenti.

Con un approccio adattivo, le policy dinamiche regolano il monitoraggio degli utenti in base ai comportamenti, e non secondo caratteristiche di rischio predefinite. Ad esempio, prendiamo un utente che non fa parte di alcun gruppo di rischio. Quando questo utente inizia a copiare dati sensibili su un dispositivo USB, Proofpoint ITM genera un avviso, attivando un monitoraggio rafforzato. La policy di monitoraggio rafforzata acquisisce metadati dettagliati e schermate per un periodo di tempo specifico. Il monitoraggio avviene solo quando è necessario, assicurando la privacy e razionalizzando gli avvisi per gli analisti della sicurezza. Con un approccio adattivo basato sui rischi, risparmi tempo e migliori la precisione del rilevamento.

Agent endpoint estremamente stabile e flessibile

Per offrire un approccio adattivo e basato sui rischi, Proofpoint utilizza un unico agent endpoint leggero che previene la perdita di dati e offre informazioni approfondite sul comportamento degli utenti. Puoi regolare la quantità e i tipi di dati raccolti per ogni utente o gruppo di utenti. Questo aiuta a rilevare le minacce tempestivamente e a indagare sugli avvisi e rispondere in modo efficiente, con costi di elaborazione e archiviazione inferiori. L'agent in modalità utente di Proofpoint non entra in conflitto con altre soluzioni e non richiede una potenza di elaborazione elevata, garantendo stabilità, produttività degli utenti e prestazioni.

Ottieni informazioni in tempo reale sui comportamenti a rischio

Visibilità granulare sugli utenti a rischio

Per aiutarti a rilevare i comportamenti a rischio, Proofpoint fornisce una visione dettagliata degli spostamenti dei dati sugli endpoint. Ciò include gli utenti che cercano di spostare dati sensibili, ad esempio caricandoli su siti web non autorizzati o copiandoli in cartelle di sincronizzazione cloud. Include anche gli utenti che manipolano i tipi di file (ad esempio cambiando le estensioni dei file) o rinominano file contenenti dati sensibili. Queste attività potrebbero indicare che gli utenti nascondono le loro attività a rischio.

Se associate a un contesto aggiuntivo, come ad esempio un collaboratore che dà le dimissioni e passa alla concorrenza, queste attività potrebbero evidenziare un utente ad alto rischio che necessita di ulteriori indagini.

Proofpoint fornisce anche visibilità sull'uso delle applicazioni e della navigazione web. I segnali di comportamenti a rischio includono l'installazione e l'esecuzione di strumenti non autorizzati, lo svolgimento di attività di amministrazione della sicurezza, la manipolazione dei controlli di sicurezza o il download di software dannosi. Proofpoint fornisce approfondimenti dettagliati per comprendere tutti i dettagli (chi, cosa, dove e quando) delle attività a rischio. Grazie a contesto e informazioni, puoi discernere meglio le intenzioni degli utenti quando si verificano comportamenti insoliti.

Analisi dei contenuti e classificazione dei dati

I dati sensibili sono più esposti quando vengono condivisi o trasferiti. Proofpoint analizza i dati in transito e interpreta le etichette di classificazione, come Microsoft Information Protection (MIP), per garantire che siano applicate le policy corrette.

Sfruttando i tuoi investimenti esistenti in termini di classificazione dei dati, puoi identificare le informazioni aziendali sensibili, come la proprietà intellettuale , senza creare un flusso di lavoro separato per i team della sicurezza e gli utenti finali. Tuttavia, 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 avanzati di Proofpoint, tra cui la corrispondenza esatta dei dati (EDM) per i dati strutturati e la corrispondenza dei documenti indicizzati (IDM) per i contenuti non strutturati come la proprietà intellettuale. Questi metodi avanzati migliorano la precisione del rilevamento e proteggono le tue informazioni più critiche.

Motore di regole flessibile e libreria di avvisi

Con Proofpoint ITM, puoi creare nuove regole e nuovi trigger adatti al tuo ambiente. o modificare i nostri scenari di minacce predefiniti. Puoi modificare questi scenari per gruppi di utenti, applicazioni, nonché per data e orario e livello di sensibilità dei dati, etichette di classificazione, fonti e destinazioni, vettori di movimento e tipi di dati.

Proofpoint ITM include anche librerie di avvisi pronte all'uso che semplificano la configurazione e velocizzano la valorizzazione. Possono avvisarti dei movimenti di dati a rischio o interazioni sospette sugli endpoint. Proofpoint può anche rilevare una gamma più ampia di comportamenti di utenti interni a rischio. La libreria di minacce interne include oltre 150 regole basate sulle linee guida dell'Istituto CERT e sulle ricerche comportamentali, offrendoti un modo rapido e semplice per rilevare i comportamenti a rischio.

SPOSTAMENTO DEI DATI	**COMPORTAMENTI**
Avvisi relativi alle interazioni con i dati e alle sottrazioni, 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 sui file (rinomina, copia, spostamento, eliminazione) • 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 email/endpoint	Avvisi relativi ai comportamenti, tra cui: • Mascheramento delle informazioni • Accesso non autorizzato • Elusione dei controlli di sicurezza • Negligenza • Creazione di una backdoor • Violazione del copyright • Strumenti di comunicazione non autorizzati • Compito amministrativo non autorizzato • Attività non autorizzate degli amministratori di database (DBA) • Preparazione di un attacco • Sabotaggio informatico • Incremento dei privilegi • Furto d'identità • Attività GIT sospetta • Utilizzo inaccettabile

Prevenzione della sottrazione non autorizzata di dati dagli endpoint

Il rilevamento degli utenti a rischio e degli spostamenti dei dati sospetti non è sempre sufficiente. Devi anche bloccare la perdita di dati in tempo reale. La nostra soluzione ti consente di prevenire interazioni non conformi alle policy da parte degli utenti con dati sensibili: trasferimento di dati da e verso dispositivi USB, sincronizzazione di file in cartelle cloud, caricamento sul web, copia e incolla, stampa e copia su dispositivi mobili, schede SD, condivisioni di rete, ecc. Puoi anche impedire agli utenti di inviare dati sensibili tramite siti di IA generativa.

Puoi personalizzare la prevenzione in base a utenti, gruppi di utenti, gruppi di endpoint, nomi di processi, dispositivo USB, numeri di serie USB, fornitore USB, etichette di classificazione dei dati, URL di origine e corrispondenza dell'analisi del contenuto.

Semplifica e accelera le indagini

Console unificata

Proofpoint ti aiuta a ottimizzare la risposta agli incidenti di origine interna e le indagini. Per una visibilità multicanale, puoi raccogliere i dati di telemetria da endpoint, email e cloud in modo centralizzato. Questa console unificata, denominata Data Security Workbench, fornisce visualizzazioni chiare per aiutare a monitorare l'attività, correlare gli avvisi, gestire le indagini, tracciare le minacce e coordinare la risposta agli incidenti. Questa vista centralizzata ti permette di ridurre i costi operativi.

Le potenti funzionalità di ricerca e filtro di Proofpoint aiutano a tracciare proattivamente le minacce grazie a esplorazioni dei dati personalizzate. Puoi ricercare i comportamenti e le attività a rischio che si applicano alla tua azienda o familiarizzare con i nuovi rischi. Puoi accelerare le indagini grazie alla ricerca assistita dall'IA utilizzando prompt in linguaggio naturale. Come per le nostre funzionalità di rilevamento, puoi adattare uno dei modelli di esplorazione delle minacce pronti all'uso o creare il tuo.

Triage degli avvisi

L'analisi e la risoluzione degli avvisi di sicurezza causati da utenti interni non sono sempre facili. Questo processo può essere lungo e costoso. Inoltre, spesso coinvolge anche dipartimenti non tecnici come le risorse umane, la conformità, l'ufficio legale e i responsabili delle divisioni.

Con Proofpoint, puoi analizzare ogni avviso in modo approfondito. Puoi visualizzare metadati e informazioni contestualizzate grazie a viste cronologiche. I team della sicurezza possono identificare quali eventi necessitano di ulteriori indagini e quali possono chiudere immediatamente. Le informazioni contestualizzate acquisite prima, durante e dopo un incidente di origine interna forniscono contesto sulle intenzioni di un utente. Comprendere se un utente è negligente, malintenzionato o compromesso è fondamentale per decidere i passi successivi.

Il flusso di lavoro e le funzionalità di condivisione delle informazioni permettono di ottimizzare la collaborazione interfunzionale.

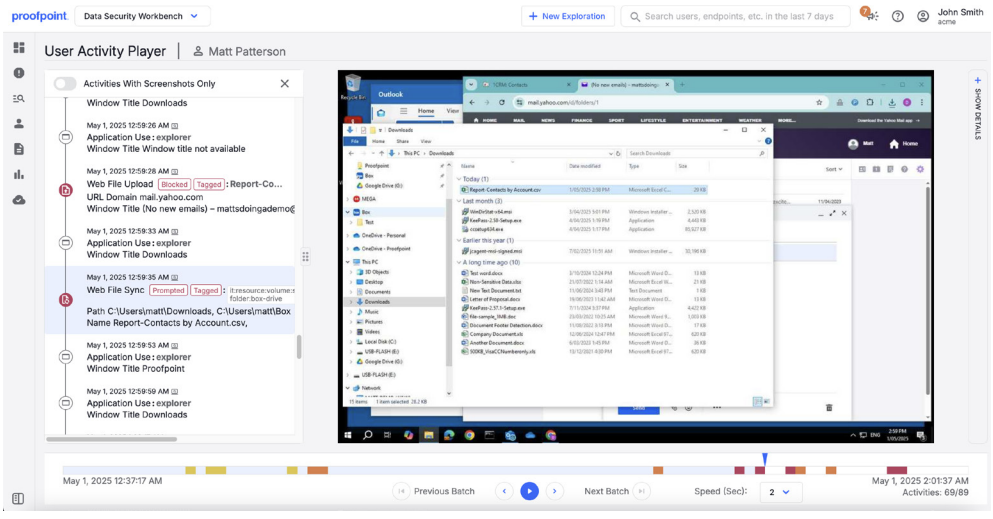


Figura 2. Dal Data Security Workbench puoi visualizzare cosa è accaduto prima, durante e dopo un incidente di origine interna grazie a una vista cronologica. Puoi visualizzare facilmente delle schermate per ottenere ulteriore contesto e prove forensi.

Puoi esportare i record delle attività a rischio relative a più eventi in file di formati comuni, inclusi i PDF. Queste esportazioni includono schermate e informazioni contestuali. Ciò può aiutare i team non tecnici, come le risorse umane e l'ufficio legale, a interpretare i dati per le indagini forensi e prendere decisioni informate.

Acquisizione di schermate per la raccolta di prove forensi

Un'immagine vale più di mille parole. Proofpoint può acquisire schermate dell'attività degli utenti. Le risorse umane, l'ufficio legale e i direttori dispongono così di prove chiare e inconfutabili dei comportamenti dannosi o negligenti per prendere decisioni informate.

Se hai un'infrastruttura di sicurezza complessa potresti avere la necessità di mantenere una sola fonte di riferimento per tutti i sistemi e quindi conservare schermate, estratti o file per scopi investigativi nel tuo archivio. Proofpoint semplifica questa operazione grazie a esportazioni automatiche dei dati verso gli spazi di archiviazione AWS S3, Microsoft Azure e Google Cloud Platform di tua proprietà o che utilizzi.

Trova il giusto equilibrio tra privacy e controlli di sicurezza

Un programma efficace di gestione dei rischi interni bilancia la privacy dell'utente e la sicurezza dei dati in conformità con le normative sulla privacy dei dati. Proofpoint adotta un approccio privacy-by-design che integra la privacy nel processo di progettazione del prodotto. Questo ti aiuta a proteggere i diritti dei collaboratori, a rispettare le leggi sulla privacy e a prevenire pregiudizi durante le indagini.

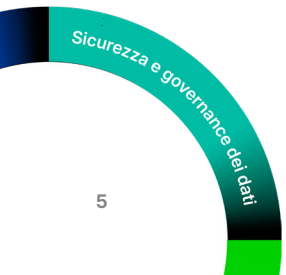
Residenza e archiviazione dei dati

Proofpoint dispone di data center in molteplici regioni per aiutarti a soddisfare i requisiti di privacy e residenza dei dati. Attualmente disponiamo di data center negli Stati Uniti, in Canada, Europa, Emirati Arabi Uniti, Australia e Giappone.

Puoi controllare l'archiviazione dei dati degli endpoint grazie ai raggruppamenti degli endpoint. Ogni raggruppamento può essere associato a un data center per l'archiviazione. I clienti possono così separare facilmente i dati da un punto di vista geografico.

Controlli di accesso basati sugli attributi

Per soddisfare i requisiti in termini di privacy, hai bisogno di flessibilità e controllo sull'accesso ai dati. Con Proofpoint, puoi assicurarti che gli analisti della sicurezza visualizzino solo i dati di cui hanno bisogno. Per esempio, puoi concedere a un analista l'accesso solo ai dati di un utente specifico o limitare la durata dell'accesso a tali dati.



Anonimizzazione e mascheramento dei dati

L'anonimizzazione delle informazioni personali garantisce la privacy degli utenti e rimuove i pregiudizi dalle indagini. Proofpoint anonimizza i dati degli utenti che raccoglie e non memorizza i nomi completi né gli identificativi degli utenti che generano avvisi. Invece, gli analisti indagano sugli avvisi in base a identificatori unici e anonimizzati. Quando è necessario conoscere l'identità di un utente, l'analista della sicurezza può richiedere la de-anonimizzazione dei dati, che può essere concessa da un amministratore.

Anche il mascheramento dei dati permette di mantenere la loro riservatezza. Puoi mascherare dati sensibili come le informazioni di identificazione sanitaria e i dati a carattere personale. In questo modo i dati non sono identificabili nell'interfaccia utente. Solo le persone che hanno bisogno di accedere ai dati possono vederli integralmente.

Migliora l'agilità con un approccio moderno

Scalabilità rapida e semplice

Proofpoint è una soluzione nativa del cloud che può scalare facilmente e si adatta all'evoluzione delle esigenze aziendali. Può supportare centinaia di migliaia di utenti per tenant. Inoltre, si implementa rapidamente ed è facile da gestire. Questo assicura una rapida valorizzazione. Proofpoint si integra facilmente anche nel tuo ecosistema esistente grazie a un approccio basato su API. I webhook semplificano l'acquisizione di avvisi da parte del tuo sistema di gestione degli eventi e delle informazioni di sicurezza (SIEM) e dei tuoi strumenti di orchestrazione, automazione e risposta della sicurezza (SOAR), permettendoti di identificare e gestire rapidamente gli incidenti.

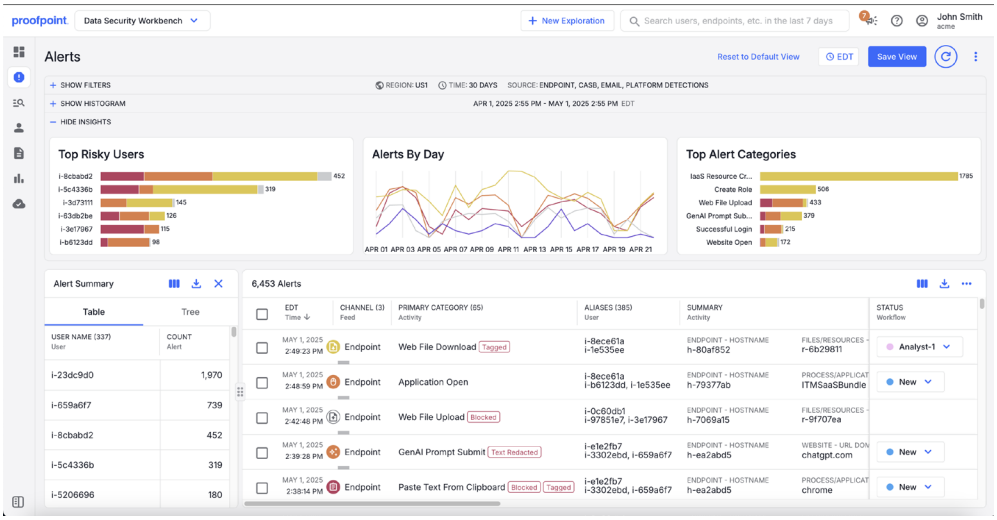


Figura 3. L'anonimizzazione protegge l'identità degli utenti, contribuendo a garantire la privacy e a eliminare i pregiudizi durante le indagini.

Supporto dei cambiamenti a livello aziendale

I cambiamenti organizzativi possono generare dubbi e incertezze, creando un ambiente ideale per le minacce interne. Le fusioni e le acquisizioni, i licenziamenti imminenti o le nuove tecnologie come l'IA generativa possono trasformare i rischi interni in minacce interne. I team di gestione dei rischi interni hanno bisogno di visibilità e controlli per supportare i cambiamenti quando si verificano. A tal fine, Proofpoint offre loro un approccio adattivo basato sui rischi che permette rilevamento e prevenzione proattivi.

Creazione e sviluppo del tuo programma

Un programma efficace di gestione dei rischi interni è una combinazione di persone, processi e tecnologia. Proofpoint può diventare il tuo partner di fiducia per garantire il successo del tuo programma di gestione dei rischi interni. I nostri servizi Premium forniscono l'esperienza di cui hai bisogno per ottimizzare il tuo programma, sfruttare i tuoi investimenti tecnologici e garantire il coinvolgimento e l'adesione delle parti interessate. I servizi Advisory ti forniscono consulenza strategica e servizi continuativi mentre crei e migliori il tuo programma. I servizi Applied ti aiutano a ottimizzare il tuo investimento tecnologico, supportare le operazioni continue e sviluppare il tuo programma di gestione dei rischi interni.

proofpoint.

SCOPRI LA PIATTAFORMA PROOFPOINT →