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

Prodotti

- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management

Vantaggi principali

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

La moderna forza lavoro può lavorare da qualsiasi luogo. Collaboratori, fornitori e terze parti hanno accesso a un maggior numero di dati rispetto al passato, che si trovino sui loro notebook, nell'email o nel cloud. Il rischio di perdita di dati è, di conseguenza, sempre più elevato. Le perdite di dati, tuttavia, non avvengono per magia. Sono sempre innescate dalle persone.

Gli utenti che esfiltrano i dati possono essere classificati in tre categorie: utenti negligenti, utenti malintenzionati e utenti compromessi. Per poter implementare policy adeguate, devi in primo luogo comprendere il contesto del comportamento degli utenti. Questo ti aiuterà a determinare le azioni da intraprendere in caso si verifichi un incidente di origine interna.

Proofpoint Endpoint Data Loss Prevention (DLP) e Proofpoint Insider Threat Management (ITM) offrono 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

Proofpoint Endpoint DLP previene la perdita di dati causate dagli utenti giornalieri. Proofpoint ITM include la stessa protezione, ma previene anche le minacce legati agli utenti a rischio, fornendo una visibilità estesa sulle attività degli utenti. Entrambe le soluzioni fanno parte della piattaforma Proofpoint Information and Cloud Security. Questa piattaforma completa, contestualizzata e nativa nel cloud offre una visibilità e informazioni su tutti i canali. Ti consente di definire delle policy, ordinare per importanza gli avvisi, monitorare le minacce e rispondere agli incidenti da una console centralizzata. La piattaforma permette di bloccare le fughe di dati e di indagare sulle violazioni di origine interna in modo rapido ed efficace. Più rapidamente si pone rimedio a un incidente, minore è il danno per l'azienda, il marchio e i risultati finanziari.

Monitoraggio degli utenti giornalieri e a rischio

Flessibilità grazie a un unico agent endpoint

Nell'attuale ambiente competitivo, devi essere in grado di gestire le minacce interne e le fughe di dati a livello di endpoint. 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 determinate attività per tutti gli utenti e su tutte le attività degli utenti che presentano il rischio più elevato.

Per soddisfare questa esigenza, Proofpoint ha sviluppato un agent endpoint leggero che impedisce la perdita di dati e fornisce una visibilità estesa sulle attività degli utenti. 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 permette di analizzare gli avvisi e rispondere più efficacemente, senza dover acquisire un'enorme quantità di dati.

Gli utenti giornalieri sono generalmente utenti aziendali medi. Dato il loro basso livello di rischio, puoi monitorarli con Proofpoint Endpoint DLP per ottenere informazioni sullo spostamento dei dati e sul contesto delle attività degli utenti. Per esempio, puoi definire regole per generare degli avvisi quando un utente cerca di esfiltrare dati sensibili copiandoli su una chiavetta USB o caricandoli in una cartella di sincronizzazione cloud.

Gli utenti a rischio richiedono un'attenzione maggiore. Può trattarsi di collaboratori che lasciano l'azienda o ne entrano a far parte, i fornitori di servizi terzi, i titolari di account con privilegi e gli utenti presi di mira, come i dirigenti di alto livello. Devi disporre di informazioni dettagliate per comprendere le loro motivazioni e intenzioni. Il loro monitoraggio deve tenere conto del loro comportamento o delle circostanze. Proofpoint ITM acquisisce dati approfonditi sulle attività di questi utenti. Tali dati possono fornire delle informazioni contestuali sulle loro intenzioni prima, durante e dopo un incidente.

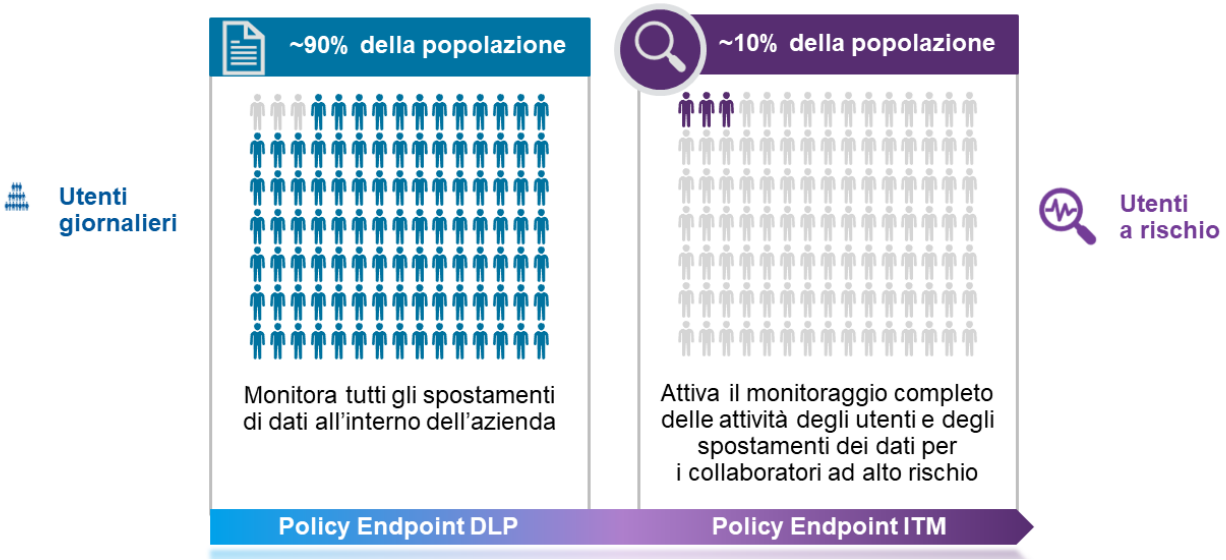

Figura 1. Agent endpoint leggero che offre la flessibilità necessaria per il monitoraggio degli utenti giornalieri e a rischio

Le informazioni dettagliate fornite da Proofpoint ITM 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.

Elenchi di sorveglianza degli utenti

Gli elenchi di sorveglianza intelligenti ti aiutano a organizzare e dare priorità agli utenti in base alla loro tolleranza ai rischi in funzione del loro profilo. Questi elenchi di sorveglianza possono basarsi su criteri come la sensibilità del ruolo dell'utente e i dati a cui accede. Possono anche basarsi sulla vulnerabilità dell'utente al phishing e ad altre minacce di social engineering. I criteri possono anche tener conto della posizione dell'utente, dell'evouzione del suo lavoro e di altri fattori legali e legati alle risorse umane.

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

Visibilità sugli utenti giornalieri e a rischio

Proofpoint Endpoint DLP e Proofpoint ITM offrono entrambi visibilità sulle interazioni degli utenti con i dati. Per contro, non acquisiscono gli stessi tipi né la stessa quantità di dati.

Proofpoint Endpoint DLP raccoglie dati telemetrici sulle interazioni degli utenti con i dati sull'endpoint. Registra azioni come la manipolazione di tipi di file (ad esempio, la modifica dell'estensione di un file) o la modifica del nome dei file contenenti dati sensibili. Registra anche i tentativi di spostamento dei dati sensibili, per esempio quando gli utenti li caricano su un sito web non autorizzato o lo copiano in una cartella di sincronizzazione cloud.

Proofpoint ITM offre una visione più completa delle attività degli endpoint in modo che tu possa monitorare gli utenti a rischio. Tiene traccia delle interazioni con i dati acquisiti da Proofpoint Endpoint DLP, offre visibilità sull'utilizzo delle applicazioni e fornisce screenshot delle attività a livello dell'endpoint e di altri comportamenti a rischio. Tali comportamenti possono includere l'installazione e l'utilizzo di strumenti non autorizzati o l'esecuzione di attività di amministrazione della sicurezza. Le informazioni dettagliate fornite da Proofpoint ITM 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.

L'approccio incentrato sulle persone di Proofpoint offre una visibilità più granulare sulle interazioni dei tuoi utenti con i dati sensibili rispetto a quella fornita dagli strumenti DLP per gli endpoint tradizionali. Infatti, 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, potresti perdere spostamenti di dati apparentemente innocui che, contestualizzati, sono indicativi di comportamenti pericolosi.

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. Quando la classificazione dei dati non è in grado di identificare in modo affidabile i dati regolamentati e quelli dei clienti, puoi sfruttare i rilevatori di contenuti all'avanguardia e comprovati di Proofpoint Cloud App Security Broker (CASB) e Proofpoint Email DLP. Inoltre, Proofpoint Intelligent Classification and Protection (in precedenza Dathena) permette di identificare e classificare automaticamente i dati in tempo reale utilizzando l'intelligenza artificiale.

Puoi configurare regole di analisi dei contenuti per rilevare e prevenire i comportamenti a rischio. Ogni volta che un comportamento viola le policy viene generato un allarme, in modo che tu disponga di informazioni fruibili in tempo reale. Le attività degli utenti a rischio attivano l'analisi dei contenuti. Queste attività possono includere il caricamento su web o il download da web, la copia su chiavetta USB, la sincronizzazione di condivisioni cloud e l'apertura di documenti.

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

Motore di regole flessibile

Puoi creare delle regole e degli attivatori adattati al tuo ambiente partendo da zero, oppure adattare i nostri scenari di minacce predefiniti. Puoi modificare gli scenari per gruppi di utenti, applicazioni e data/ora e grado di sensibilità, etichette di classificazione, fonti e destinazioni, canali di spostamento e tipo di dati. Per garantire la coerenza e risparmiare tempo, le regole definite da Proofpoint ITM possono essere applicate a altri canali, come l'email, il cloud e il web, tramite lo strumento di gestione delle policy unificato della piattaforma.

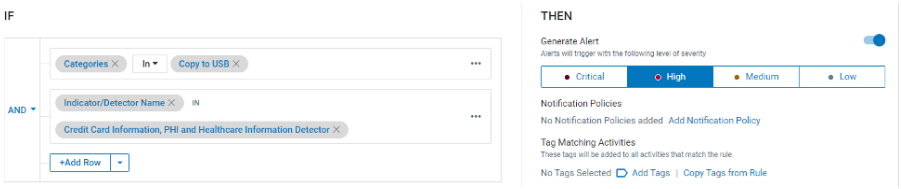

Figura 2. Impostazione di avvisi grazie a semplici istruzioni di tipo if-then.

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. Proofpoint ITM è anche in grado di segnalarti una gamma più ampia di minacce interne.

Biblioteca degli allarmi Proofpoint Endpoint DLP e Proofpoint ITM

SPOSTAMENTO DEI DATI

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
- Attività svolte su file (ridenominazione, 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

ATTIVITÀ DEGLI UTENTI (SOLO PROOFPOINT ITM)

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 non autorizzate degli amministratori di database (DBA)
- Preparazione di un attacco
- Sabotaggio informatico
- Incremento dei privilegi
- Furto d'identità
- Attività GIT sospette
- Utilizzo inaccettabile

Spesso gli utenti non sanno che il loro comportamento è pericoloso. Puoi attivare le notifiche per formarli.

Prevenzione di esfiltrazioni non autorizzate di dati dall'endpoint

Il rilevamento degli utenti a rischio e degli spostamenti dei dati sospetti non è sempre sufficiente. Devi anche bloccare attivamente le fughe di dati in tempo reale. La nostra piattaforma ti permette di prevenire le interazioni non conformi alle policy degli utenti con dati sensibili

Per esempio:

- Trasferimento verso e da dispositivi USB
- Sincronizzazione di file con le cartelle cloud
- Caricamento su siti web non autorizzati
- Stampa di file

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 Protection and Cloud Security.

Formazione degli utenti sui comportamenti a rischio

Spesso gli utenti non sanno che il loro comportamento è pericoloso. Puoi attivare le notifiche per formarli. Per esempio, quando degli utenti cercano di spostare file sensibili, ricevono una notifica che li informa che questa azione viola le regole aziendali. Dovranno quindi fornire una giustificazione. Alla notifica può essere aggiunto un link alle policy aziendali. L'invio di notifiche ai collaboratori relative al loro comportamento permette di preservare la loro produttività e rafforzare i controlli di sicurezza. Le notifiche possono essere personalizzate in base al livello di rischio, funzione o posizione dell'utente.

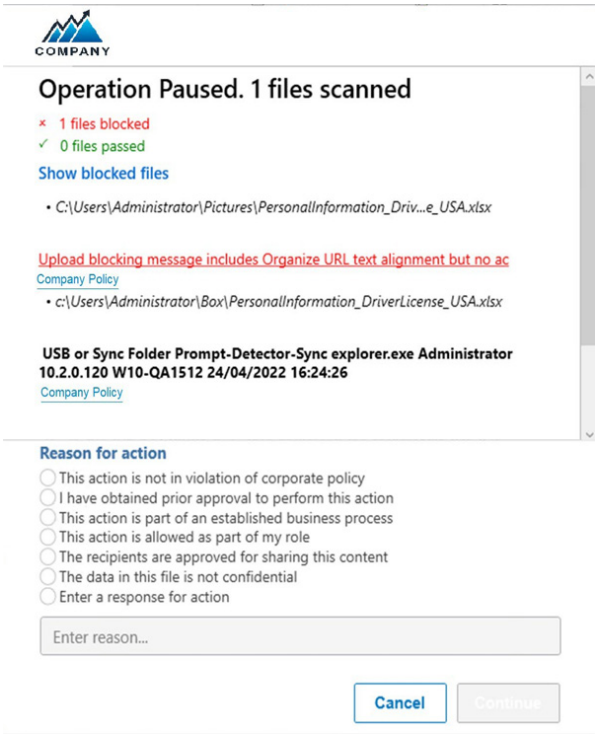

Figura 3. Invio di una notifica agli utenti finali con un comportamento a rischio e richiesta di giustificazione

Accelerazione della risposta a incidenti e delle indagini

Console unificata

Proofpoint Endpoint DLP e Proofpoint ITM sfruttano la piattaforma Proofpoint Information and Cloud Security. Ciò ti permette di ottimizzare la risposta agli incidenti di origine interna e le indagini. La piattaforma acquisisce dati telemetrici dagli endpoint, dall'email e dal cloud per offrire una visibilità multicanale centralizzata. La sua console unificata propone delle visualizzazione intuitive per aiutarti a monitorare le attività, correlare gli avvisi, gestire le indagini, tracciare le minacce e coordinare la risposta agli incidenti.

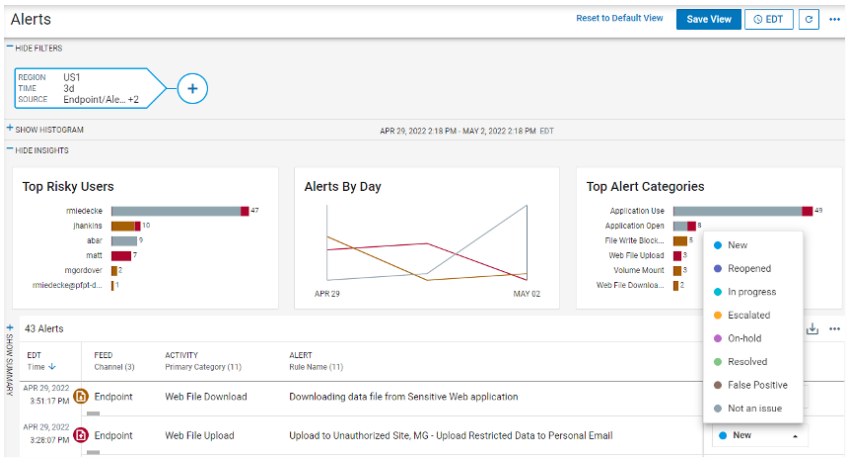

Figura 4. Visualizzazione di tutti gli incidenti e avvisi in una console unificata

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.

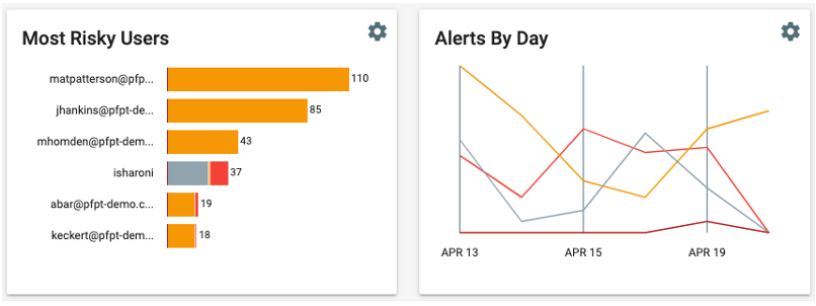

Figura 5. Tracciamento di comportamenti potenzialmente pericolosi o insoliti

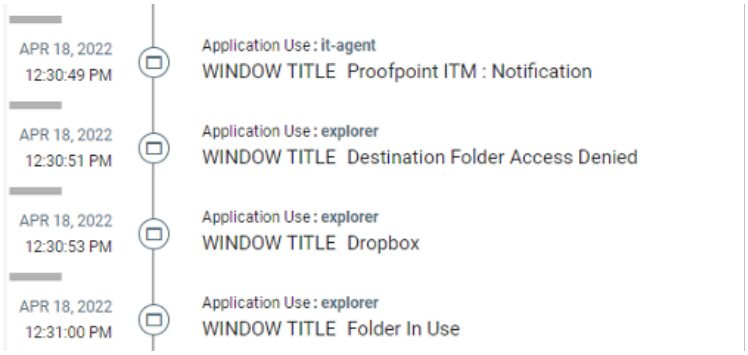

Figura 6. Vista cronologica che fornisce lo storico delle interazioni dell'utente con i dati

Classificazione degli avvisi per priorità

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 Endpoint DLP e Proofpoint ITM puoi analizzare ogni avviso in modo approfondito. Queste soluzioni ti permettono di visualizzare i metadati e di ottenere informazioni contestualizzate grazie a viste cronologiche. I team della sicurezza possono identificare rapidamente quali eventi necessitano di ulteriori indagini e quali possono chiudere immediatamente. Possono essere utilizzati dei tag per raggruppare e classificare gli avvisi per favorire il coordinamento.

Il flusso di lavoro di base e le funzionalità di condivisione delle informazioni ottimizzano 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. Ciò può aiutare i team non tecnici, come le risorse umane e i servizi legali a interpretare i dati per le indagini forensi.

Acquisizione di schermate per gli utenti a rischio

A volte un'immagine 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.

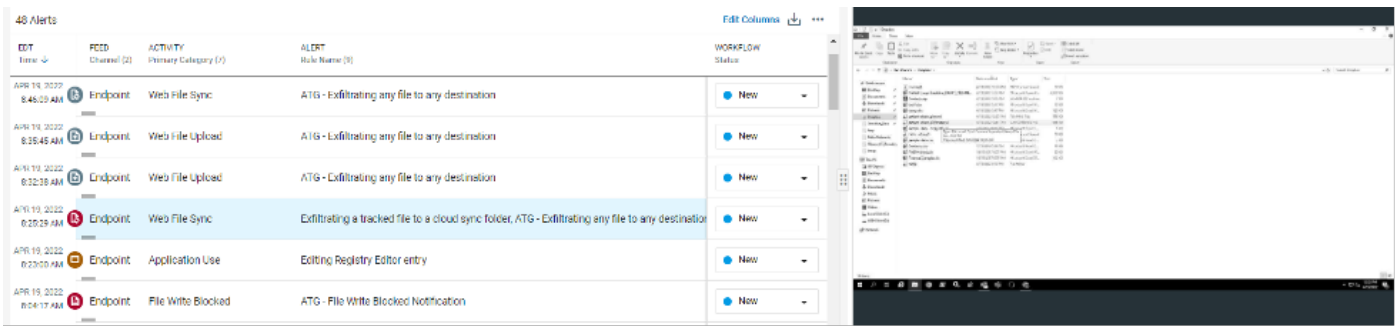

Figura 7. Vista cronologica delle attività dell'utente con acquisizione della schermata dell'endpoint dell'utente

Facile integrazione in ambienti di sicurezza complessi

La piattaforma Proofpoint Information Protection and Cloud Security è guidata dai 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.

Se hai infrastrutture di sicurezza complesse potresti 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.

Risposta alle esigenze in materia di privacy e conformità

Gestione dell'ubicazione e dell'archiviazione dei dati

Supportiamo i data center multiregionali per la piattaforma Proofpoint Information Protection and Cloud Security, per aiutarti a soddisfare i requisiti in termini di ubicazione e riservatezza dei dati. Attualmente disponiamo di data center negli Stati Uniti, in Europa, Australia e Giappone.

Puoi controllare l'archiviazione dei dati degli endpoint grazie a un raggruppamento di endpoint. Ogni raggruppamento può essere collegato a un data center per l'archiviazione. Ciò consente ai clienti di separare facilmente i dati a livello geografico. Per esempio, i dati degli endpoint negli Stati Uniti possono essere gestiti da un raggruppamento negli Stati Uniti, che viene inviato al data center degli Stati Uniti.

Riservatezza garantita grazie a controlli d'accesso basati sugli attributi

Per soddisfare i requisiti di riservatezza, hai bisogno di flessibilità e controllo sull'accesso ai dati. Con Proofpoint Endpoint DLP e Proofpoint ITM puoi facilmente gestire l'accesso per garantire che gli analisti della sicurezza vedano i dati solo quando è assolutamente necessario. Per esempio, puoi definire regole granulari e assegnare l'accesso in modo che un analista della sicurezza con sede in Europa possa vedere solo i dati europei e non quelli degli Stati Uniti o della regione Asia-Pacifico. Hai la flessibilità necessaria per concedere a un analista un accesso limitato ai dati di un utente specifico o limitare la durata dell'accesso a tali dati.

Visibilità e contesto multicanale

Proofpoint Endpoint DLP e Proofpoint ITM sfruttano la potenza della piattaforma Proofpoint Information and Cloud Security. Queste soluzioni adottano un approccio incentrato sulle persone per i contenuti, i comportamenti e le minacce per bloccare le fughe di dati e indagare sulle minacce. Grazie a una console unificata, ottieni visibilità e informazioni contestualizzate su più canali, tra cui endpoint, cloud, email e web.

Puoi definire le policy, tracciare le minacce e analizzare e rispondere agli avvisi, indipendentemente dal canale, da un'unica interfaccia. Non devi passare da uno strumento all'altro per eseguire ogni attività. Puoi anche analizzare i metadati degli avvisi in modo approfondito. Ciò ti aiuterà a capire cosa è successo prima, durante e dopo un incidente. La soluzione nativa nel cloud può anche essere implementata rapidamente, per ridurre il tempo di valorizzazione.

Lavori in modo più efficiente, risparmi tempo prezioso e riduci le interruzioni delle attività causate dalle fughe di dati e da minacce interne grazie alla visibilità e al contesto forniti dalla piattaforma Proofpoint Information Protection and Cloud Security.

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 il 75% 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**.