Proofpoint Insider Threat Management

Gestione delle minacce interne incentrata sulle persone per le aziende moderne

VANTAGGI PRINCIPALI

- Rilevamento delle attività interne a rischio e prevenzione della perdita di dati dagli endpoint
- Semplificazione della risposta alle minacce interne e alle perdite di dati
- Valorizzazione più rapida grazie a un'implementazione SaaS scalabile guidata da un moderno sistema di back-end nativo nel cloud
- Mantenimento della produttività dell'utente con un agent leggero per gli endpoint

PRINCIPALI CASI D'USO DI PROOFPOINT ITM

- Identificazione dei rischi legati agli utenti
- Protezione dalle perdite di dati dall'endpoint
- Accelerazione della risposta agli incidenti attribuibili agli utenti
- Sviluppo di programmi di gestione delle minacce interne

Grazie al suo approccio incentrato sulle persone, Proofpoint Insider Threat Management (ITM) protegge la tua azienda da perdita di dati, azioni dannose e danni al marchio imputabili al personale interno. Ti proteggiamo dalle azioni dannose, negligenti o inconsapevoli degli utenti autorizzati e correliamo le attività degli utenti con gli spostamenti dei dati per proteggerti dalle violazioni dei dati indotte da utenti interni. Inoltre, rileviamo i comportamenti a rischio in tempo reale per fornirti prove irrefutabili di comportamenti dolosi.

Rilevamento e prevenzione in tempo reale dei comportamenti a rischio

Con Proofpoint ITM puoi correlare i comportamenti a rischio a livello di applicazioni, file, desktop, server e ambienti virtualizzati in tempo reale, e non solo dopo che l'incidente si è verificato. Ti offriamo una visibilità in tempo reale che ti permette di correlare, rilevare, e neutralizzare gli incidenti causati da minacce interne.

Scenari delle minacce reali e collaborativi

Puoi rilevare i comportamenti a rischio in tempo reale. tra cui, ad esempio:

- Esfiltrazione dei dati
- Spostamenti laterali a rischio dei dati
- Abuso di privilegi
- Uso improprio delle applicazioni
- Accesso non autorizzato
- Azioni involontarie pericolose

Puoi facilmente creare regole e trigger adattati al tuo ambiente grazie al nostro strumento per la creazione di regole basato sulla logica booleana. Puoi partire con scenari di minacce predefiniti e modificarli oppure iniziare da zero. La nostra ampia gamma di regole di rilevamento delle minacce interne si basa sulle conoscenze della divisione CERT dell'università Carnegie Mellon, del NITTF, del NIST e dei nostri clienti.

Tracciamento delle minacce con un semplice clic

Il tracciamento delle minacce non riguarda soltanto le minacce provenienti dall'esterno. Con Proofpoint ITM puoi identificare gli utenti interni che corrono rischi inutili o che hanno intenzioni dolose. La nostra semplice interfaccia "point and click" rende facile di esplorare e ricercare in modo proattivo i comportamenti anomali.

Grazie al tracciamento delle minacce semplificato puoi:

- studiare i comportamenti e le attività a rischio nel tuo ambiente;
- utilizzare raggruppamenti intelligenti per filtrare migliaia di attività che non sono rilevanti e concentrarti su quelle che lo sono;
- contestualizzare i comportamenti anomali grazie a una visione cronologica delle attività e a prove basate sugli screenshot.

Supporto per la classificazione dei dati

Le nostre soluzioni si integrano con Microsoft Information Protection (MIP). Il nostro agent ITM legge le etichette di riservatezza in tempo reale mentre l'utente interagisce con il file. Puoi definire regole di rilevamento e prevenzione in base all'etichetta di riservatezza MIP del file, alla sua origine, al tipo di file e alla sua destinazione.

Prevenzione della perdita dei dati

Proofpoint ITM aiuta a prevenire l'esfiltrazione di dati sensibili attraverso canali comuni, compresi dispositivi USB come le cartelle di sincronizzazione locali, i dispositivi di archiviazione collegati alla rete, i dispositivi multimediali e i telefoni. La soluzione funziona anche quando l'utente è offline.

Puoi gestire le attività USB per utente, gruppi e host come di seguito:

- Blocco della scrittura di dati su dispositivi USB
- Inserimento in una lista di autorizzazione di alcuni dispositivi USB
- Blocco dei file corrispondenti a un modello di nome di file
- Blocco dei tipi di file
- Blocco delle fonti di file
- Applicazione di regole di prevenzione globali

La suite Proofpoint Enterprise DLP può estendere la protezione all'email e alle applicazioni cloud.

Risposta più rapida agli incidenti

Molte aziende adottano delle misure contro le minacce interne a seguito di un evento di sicurezza. La maggior parte di esse si rende conto che i flussi di lavoro generici dei loro strumenti di sicurezza esistenti non sono efficaci contro le minacce interne. I dati interni sono sensibili e richiedono un livello superiore di collaborazione con altri team che non sono responsabili della cybersecurity.

Contesto immediato e prove irrefutabili

I nostri flussi di lavoro sono personalizzati in base agli eventi indotti dagli utenti. È possibile cercare gli eventi di sicurezza con parole chiave e filtri tra tutte le schermate catturate e i metadati acquisiti. In altre parole, non è necessario imparare un nuovo linguaggio di query. È possibile salvare i filtri per il tracciamento proattivo delle minacce o come riferimento futuro per un'indagine.

Man mano che identifichi gli allarmi e gli eventi critici relativi alle indagini, puoi etichettarli e categorizzarli. Quando hai bisogno di condividere le prove, puoi recuperare gli eventi e gli avvisi pertinenti attraverso quei tag e poi esportarli in formati di file comuni, come ad esempio in PDF. Questi report includono screenshot e informazioni contestuali associate (chi, cosa, dove e quando). Ciò facilità la loro gestione al team della cybersecurity e la loro comprensione ai team delle risorse umane, dell'ufficio legale, della conformità e agli analisti.

I vantaggi dell'architettura di Proofpoint ITM

La nostra architettura cloud è stata progettata pensando alla scalabilità, alla facilità d'uso, alla sicurezza e all'estensibilità. Utilizzando i nostri avanzati agent endpoint leggeri per acquisire l'attività dei dati otterrai una visibilità senza pari indipendente, dalle applicazioni, sulle attività che gli utenti svolgono sui loro sistemi senza interferire con la loro attività.

Implementazione esclusivamente SaaS

Proofpoint Endpoint DLP è una moderna piattaforma SaaS progettata pensando alla scalabilità, all'analisi, alla sicurezza, alla privacy e all'estensibilità. Permette di ridurre i tempi di configurazione e i costi a livello di backend e semplifica la gestione continua da parte degli amministratori della sicurezza in tutta l'azienda. Ciò si traduce in una visibilità immediata sul movimento dei dati.

Due problemi, una soluzione leggera

Proofpoint Endpoint DLP e Insider Threat Management si basano sull'unico agent leggero e su una moderna architettura SaaS. Quando le due soluzioni vengono utilizzate insieme, Proofpoint Endpoint DLP previene i rischi di perdita di dati tra gli utenti quotidiani, mentre Proofpoint ITM estende la protezione a tutti i comportamenti agli utenti malintenzionati e a più alto rischio.

APPROFONDISCI

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