proofpoint.

Controlli d'accesso e della privacy per Proofpoint Information Protection

Soddisfa i requisiti di conformità proteggendo i diritti dei collaboratori e eliminando i pregiudizi

Vantaggi principali

- Protezione della relazione di fiducia con i collaboratori
- Protezione delle informazioni aziendali strategiche
- Conformità con le leggi sulla privacy
- Prevenzione dei pregiudizi nelle indagini

La protezione della privacy dei dati è un'attività sempre più importante e complessa. L'accelerazione della trasformazione digitale, la diffusione del lavoro ibrido e la proliferazione delle applicazioni cloud hanno complicato più che mai la protezione dei dati sensibili. Man mano che le aziende continuano a accumulare volumi di dati sempre più grandi, cresce il loro valore percepito. Purtroppo, questo valore accresciuto comporta anche il rischio di perdita e furto di dati, anche da parte di utenti interni.

Nonostante le crescenti difficoltà, le aziende non possono permettersi passi falsi. Le aziende di tutto il mondo sono sottoposte a una crescente pressione in termini di rispetto delle stringenti leggi sulla privacy dei dati che impongono solide misure di sicurezza e privacy dei dati. Non rispettare la conformità può essere costoso; sanzioni salate e perdite di quote di mercato sono comuni. Secondo più di un terzo dei professionisti della sicurezza le violazioni delle normative e le multe sono una conseguenza della perdita di dati[1].

Proofpoint offre una suite completa di soluzioni studiate per rafforzare la sicurezza dei dati e gestire le minacce interne, assicurando la conformità con le normative sulla privacy dei dati. La famiglia di soluzioni Proofpoint Information Protection implementa solidi controlli d'accesso e privacy. Limita la visibilità solo alle persone che ne hanno veramente bisogno e preserva l'anonimato degli utenti assicurando la riservatezza dei dati identificativi. Pertanto, Proofpoint rafforza la sicurezza dei dati e contribuisce a eliminare i pregiudizi durante le tue indagini. Potrai così beneficiare di un approccio bilanciato alla sicurezza delle informazioni.

Approccio incentrato sulla privacy

Proofpoint Information Protection si basa su principi della privacy-by-design. Questa metodologia segue un approccio proattivo alla protezione dei dati. Pone la privacy in primo piano nella progettazione dei sistemi per garantire che i sistemi IT, l'infrastruttura e i processi aziendali integrino la privacy come aspetto centrale fin da subito. Questo approccio pone visibilità, trasparenza e centralità dell'utente al centro della sua progettazione.

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.

1 Report Data Loss Landscape 2024 di Proofpoint.

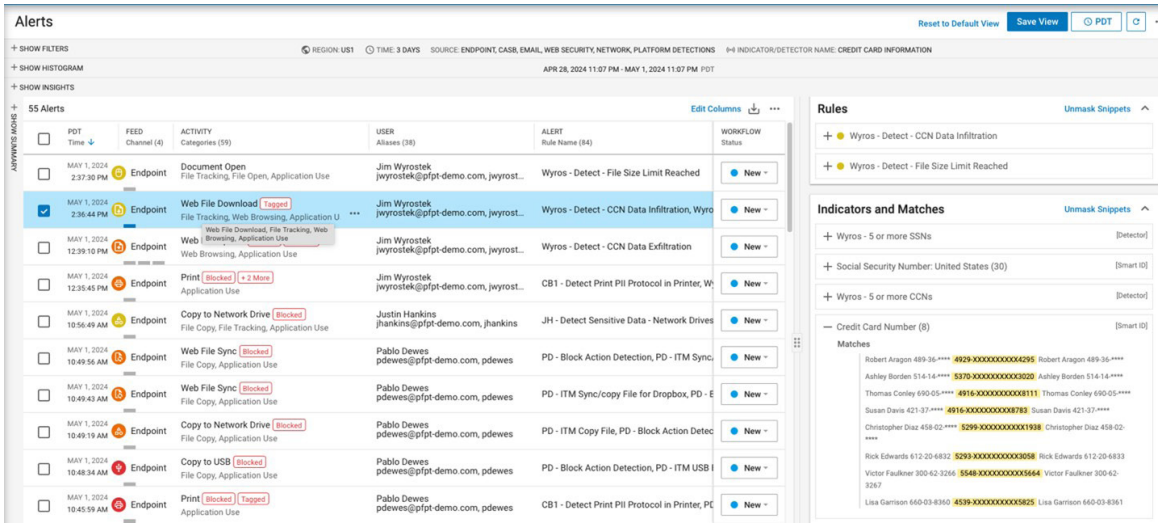

Figura 1. Mascheramento dei numeri della carta di credito in Proofpoint Information Protection

Gestisci l'ubicazione e l'archiviazione dei dati

Proofpoint dispone di data center regionali posizionati strategicamente negli Stati Uniti, in Canada, Europa, Australia e Giappone per rispondere ai requisiti di privacy e ubicazione dei dati. Disponi del pieno controllo del luogo in cui i tuoi dati sono archiviati in tutti questi data center.

Per gestire l'archiviazione dei dati degli endpoint, Proofpoint ti permette di creare raggruppamenti di endpoint. Ogni raggruppamento può essere associato a un data center specifico, permettendoti di separare facilmente i dati a livello geografico. Per esempio, un raggruppamento negli Stati Uniti può gestire i dati degli endpoint negli Stati Uniti, che vengono inviati al data center degli Stati Uniti.

Garantisci la riservatezza grazie a controlli d'accesso basati sugli attributi

I controlli d'accesso basati sugli attributi di Proofpoint Information Protection offrono un modo flessibile ed efficace per gestire l'accesso ai dati. Aiutano a garantire che gli analisti della sicurezza abbiano visibilità sui dati solo se strettamente necessario.

Per esempio, puoi definire regole granulari e assegnare l'accesso in modo che un analista della sicurezza con sede negli Stati Uniti possa vedere solo i dati statunitensi e non quelli provenienti dall'Europa o della regione Asia-Pacifico. Questo livello di controlli d'accesso specifici riduce in modo significativo il rischio di esposizione inutile dei dati. E quando un analista deve accedere ai dati di un utente specifico per un'indagine, l'amministratore di sistema può anche limitare nel tempo tale accesso, ovvero specificare per quanto tempo l'analista può accedere a quei dati.

Assicura la riservatezza dei dati grazie al mascheramento dei frammenti

Proofpoint Information Protection utilizza il mascheramento dei dati per assicurare la riservatezza dei dati. Il mascheramento dei dati oscura i dati di analisi sensibili, come le informazioni sanitarie protette e i dati a carattere personale nella console, rendendo tali informazioni non identificabili. Questo approccio assicura che solo le persone che hanno bisogno di accesso ai dati possono consultarli in forma completa e in chiaro.

Gli amministratori di sistema possono configurare gli identificatori dei dati che desiderano mascherare. Possono, per esempio, decidere di mostrare solo le ultime quattro cifre del numero di una carta di credito e celare tutto il resto. Possono anche decidere il tipo e la quantità di dati cui gli utenti possono accedere in base al loro ruolo. Per esempio, possono specificare che solo gli analisti autorizzati possono visualizzare frammenti di dati sensibili.

Proteggi i dati dell'utente con l'anonimizzazione dei dati

Proofpoint Information Protection protegge anche i dati degli utenti grazie all'anonimizzazione che permette di mascherare l'identità di un utente. Puoi rendere anonimo il nome utente, il nome dell'host, l'indirizzo IP, le informazioni sull'ubicazione e i nomi dei file.

L'anonimizzazione assicura che solo gli analisti della sicurezza autorizzati possano consultare i dati identificativi degli utenti monitorati. Questo processo aiuta anche a eliminare i pregiudizi nelle indagini. Pensiamo all'ipotesi in cui un dirigente ha appena violato una policy aziendale. Se la sua identità è nota, l'incidente potrebbe essere gestito in modo diverso o un analista della sicurezza potrebbe chiudere un occhio sulla violazione.

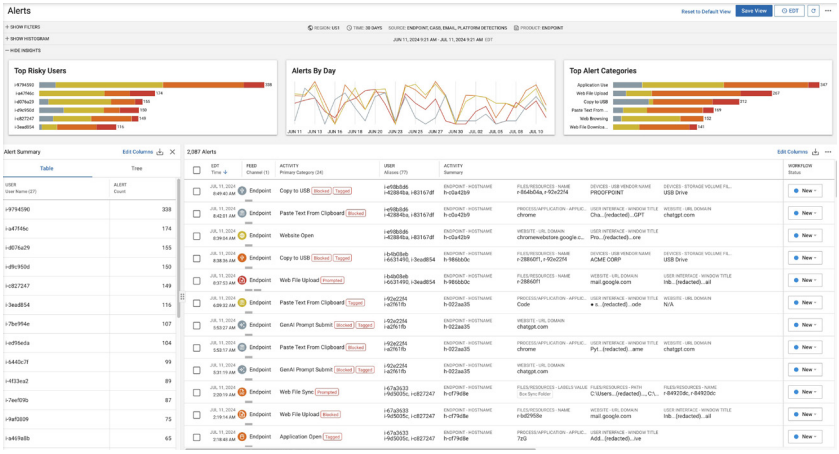

Figura 2. Vista dei dati anonimizzati degli utenti in Proofpoint Information Protection

Quando l'identità di un utente deve essere conosciuta più avanti nel corso di un'indagine, l'analista di sicurezza può richiedere la de-anonimizzazione dei dati, che può essere concessa dall'amministratore.

Trova il giusto equilibrio tra sicurezza e privacy dei dati

Il bilanciamento della sicurezza e della privacy dei dati è importante per ogni azienda. Per ottenerlo, è necessario tenere a mente i seguenti principi:

- **Monitora i principali canali di perdita di dati.** Concentra le tue attività di protezione dei dati sul modo in cui i tuoi utenti lavorano. La maggior parte delle fughe ed esposizioni di dati si verificano tramite email, applicazioni cloud e chiavette USB.
- **Comunica in modo chiaro e trasparente.** Assicurati che i tuoi collaboratori conoscano le policy aziendali relative alla sicurezza e alla privacy dei dati. Spiega in modo chiaro cosa monitori. In questo modo crei un clima di fiducia.
- **Educa gli utenti con notifiche automatiche.** Quando un utente viola una policy aziendale, può essere generata automaticamente una notifica per informarlo. L'invio di una notifica automatica aiuta a informare l'utente del suo comportamento a rischio eliminando la vergogna e le emozioni legate al rapportarsi con il suo responsabile o le risorse umane.
- **Fai delle scelte.** Non devi raccogliere tutti i dati. Decidi quali sono i dati importanti e quanto hai bisogno di sapere sulle attività dei collaboratori.
- **Controlla l'accesso ai dati.** Sebbene amministratori della sicurezza, analisti, responsabili legali e delle risorse umane possano godere di un accesso illimitato ai dati sui collaboratori, non è sempre una buona cosa in termini di privacy, Assicurati perciò di utilizzare i controlli d'accesso inclusi negli strumenti DLP e ITM.

Garantisci la privacy dei dati con Proofpoint

Le soluzioni Proofpoint Information Protection come Data Loss Prevention e Insider Threat Management permettono di mantenere il più elevato livello di protezione dei dati garantendo la conformità con le normative sulla privacy dei dati. Contribuiscono anche a eliminare i pregiudizi nelle tue indagini. Proofpoint Information Protection tiene conto di contenuti e comportamenti in modo che tu possa identificare i dati sensibili o regolamentati nonché segnalare le attività a rischio e le intenzioni dannose, tutto da una console centralizzata che fornisce visibilità sui canali, tra cui endpoint, email, cloud e web.

Proofpoint Managed Information Protection riunisce le persone, i processi e le tecnologie appropriate, permettendoti di progettare, implementare e sviluppare il tuo programma per ottimizzare la protezione e garantire la privacy dei dati.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.