

Proofpoint Cloud DLP

Visibilità e controllo sui dati sensibili nelle applicazioni cloud

Vantaggi principali

- Ottieni visibilità sulle minacce cloud, sugli spostamenti dei dati sospetti, sull'esposizione dei dati cloud e sull'utilizzo a rischio delle applicazioni cloud.
- Proteggi i dati sensibili tramite funzionalità di prevenzione della perdita di dati (DLP) che coprono contenuti, comportamento e dati di telemetria delle minacce.
- Semplifica le operazioni DLP a livello di cloud, email, web ed endpoint grazie a un gestore degli allarmi unificato.
- Proteggiti contro il takeover degli account, gli usi impropri di applicazioni OAuth, gli accessi persistenti e gli attacchi basati su file.
- Rileva i rischi interni legati al cloud grazie a modelli di machine learning appositamente concepiti per rilevare download, condivisioni sospette e sottrazioni di dati insoliti.
- Accelera l'applicazione di misure correttive mediante azioni automatizzate che rimuovono le condivisioni, limitano le autorizzazioni, bloccano gli account, revocano l'accesso OAuth e neutralizzano i rischi.

Grazie al suo approccio incentrato sulle persone, Proofpoint Cloud DLP protegge i tuoi dati sensibili e i tuoi utenti contro le minacce cloud. Aiuta le aziende a monitorare l'esposizione dei dati, governare l'uso dei servizi SaaS e controllare l'accesso alle applicazioni OAuth di terze parti.

La sicurezza del cloud inizia dalla protezione delle applicazioni approvate dall'IT che contengono i tuoi dati più critici, come Microsoft 365, Google Workspace, Salesforce e Box. Proofpoint Cloud DLP ti offre visibilità incentrata sulle persone sulle minacce cloud, sull'esposizione dei dati ai rischi, sul comportamento degli utenti e sullo spostamento dei dati. Le aziende possono così creare e preservare un solido livello di sicurezza cloud.

Integrato nella piattaforma di sicurezza dei dati Proofpoint, Cloud DLP correla le minacce e il comportamento degli utenti, e applica policy DLP coerenti alle applicazioni cloud, all'email, al web e agli endpoint.

Proofpoint Cloud DLP ti aiuta a prevenire la condivisione eccessiva e la perdita di dati sensibili, ridurre i rischi interni e limitare i comportamenti a rischio degli utenti. Puoi così proteggerti contro gli attacchi di takeover degli account, i file annosi e gli utilizzi impropri di OAuth.

Estensione della visibilità incentrata sulle persone alle applicazioni cloud

Proofpoint Cloud DLP ti offre visibilità sulle minacce cloud e email. Il suo approccio incentrato sulle persone ti permette di identificare i tuoi VAP (Very Attacked People™, ovvero le persone più attaccate) e proteggere i loro dati e account cloud. Puoi identificare i file che violano le regole DLP, ma anche chi ne è il proprietario, chi li scarica, li condivide o li modifica. Inoltre, i suoi strumenti di analisi e i controlli adattivi ti aiutano ad assegnare adeguati livelli di accesso agli utenti e alle applicazioni OAuth di terze parti, in base ai fattori di rischio per te più importanti.

Protezione di utenti, applicazioni e dati contro le minacce cloud

Proofpoint Cloud DLP combina il contesto utente con la threat intelligence multicanale di Proofpoint Behavior Graph. Il machine learning e la correlazione delle minacce ti aiutano a rilevare quando un account cloud è stato compromesso e viene utilizzato per attività sospette, per esempio l'invio o l'inoltro di email o la sottrazione di dati.

La dashboard intuitiva di Proofpoint Cloud DLP ti consente di esaminare gli avvisi relativi ai login sospetti, alle attività legate ai file e alle attività di amministrazione. Puoi esportare i dati delle indagini digitali verso una soluzione di gestione degli eventi e delle informazioni di sicurezza (SIEM) per ulteriori analisi, manualmente o tramite l'API REST.

Grazie alle solide policy, agli avvisi in tempo reale e alle risposte automatizzate di Proofpoint Cloud DLP, puoi:

- Proteggere il tuo ambiente contro il takeover degli account cloud e sospendere gli account compromessi
- Implementare un'autenticazione basata sui rischi e sui controlli di accesso adattivi
- Prevenire il furto di dati e l'uso improprio di applicazioni OAuth identificando e revocando l'accesso da parte di terzi a rischio
- Rilevare e mettere in quarantena i file dannosi
- Rimuovere le condivisioni di file e le autorizzazioni inappropriate

- Limitare l'accesso a contenuti sensibili
- Bloccare gli account utente e automatizzare i flussi di applicazione di misure correttive
- Esaminare e neutralizzare le attività sospette sugli account cloud

Proofpoint Cloud DLP permette anche di identificare i rischi interni a livello di cloud. Modelli di machine learning appositamente progettati rilevano comportamenti spesso associati a minacce interne e collaboratori in uscita dall'azienda. Ciò include download anomali, condivisioni eccessive, schemi di accesso ai dati insoliti e potenziali sottrazioni di dati rispetto alle attività di riferimento a livello degli utenti o dell'azienda nel suo complesso.

Il componente aggiuntivo SaaS Isolation consente anche di proteggere gli utenti, applicare le policy DLP ai dispositivi non gestiti e integrare la tua soluzione di gestione delle identità tramite l'autenticazione SAML (Security Assertion Markup Language).

Regole DLP unificate per tutti i canali

Proofpoint Cloud DLP condivide i classificatori DLP con altre soluzioni di sicurezza dei dati Proofpoint. Si tratta di identificatori intelligenti integrati, dizionari, regole, modelli e classificatori personalizzati autonomi (ACC) che utilizzano modelli linguistici di grandi dimensioni (LLM) per scoprire e classificare automaticamente i contenuti sensibili specifici dell'azienda.

Questa condivisione ti aiuta a identificare e proteggere i dati sensibili più rapidamente. Come parte della piattaforma di sicurezza dei dati Proofpoint, puoi implementare policy DLP coerenti sulle applicazioni SaaS, l'email, il web e gli endpoint.

La soluzione combina i dati di analisi dei contenuti, dei comportamenti e delle minacce di questi canali. Puoi così determinare se l'utente che ha attivato l'allarme DLP è stato compromesso, ha intenti dolosi o è semplicemente negligente. Puoi anche unificare la gestione degli avvisi DLP su più canali.

Oltre 240 classificatori integrati coprono i dati soggetti alle normative PCI, GDPR e le normative sui dati di identificazione personale e le informazioni sanitarie personali. Le tecnologie avanzate di rilevamento ti aiutano a creare controlli su misura, come l'esatta corrispondenza dei dati e le policy contestuali. Puoi inoltre limitare l'accesso ai dati da dispositivi non gestiti, impedire il caricamento di file sensibili su applicazioni cloud non approvate e limitare le autorizzazioni di condivisione eccessive. Puoi anche identificare i file sensibili ampiamente esposti e correlare le attività di login sospette con gli incidenti DLP.

Governance delle applicazioni cloud e di terze parti

Proofpoint Cloud DLP mette in evidenza la Shadow IT e identifica le applicazioni cloud nella tua azienda. Il nostro catalogo conta 46.000 applicazioni, ognuna con più di 50 attributi. Puoi categorizzare le applicazioni cloud in base al tipo e al punteggio di rischio, il che ti aiuta a valutare i rischi per la sicurezza, le vulnerabilità legate alla perdita di dati e le lacune di conformità. Puoi bloccare le applicazioni a rischio oppure concedere agli utenti l'accesso in sola lettura.

La soluzione rileva e valuta anche le autorizzazioni OAuth per le applicazioni di terze parti che accedono ai servizi cloud principali approvati dal team IT. La sua funzione di analisi permette di identificare le applicazioni a rischio e ridurre la tua superficie d'attacco. Puoi definire o automatizzare determinate azioni in base al punteggio di rischio e al contesto.

Implementazione rapida

La nostra architettura multimodale ti consente di valorizzare più velocemente il tuo investimento. In meno di quattro settimane, puoi integrare la soluzione con le API cloud, gli strumenti ibridi di gestione delle identità e i prodotti di orchestrazione della sicurezza (compreso Proofpoint Threat Response).

Questa integrazione di permette di rilevare automaticamente le minacce, contenerle e proteggere i dati. L'autenticazione SAML basata sui rischi e la funzione SaaS Isolation aiutano a bloccare gli accessi non autorizzati alle applicazioni aziendali e supportano le strategie BYOD.

I punti di forza di Proofpoint Cloud DLP

Proofpoint Cloud DLP combina, in un'unica soluzione, protezione dei dati, difesa contro le minacce cloud, rilevamento dei rischi interni, visibilità sull'esposizione dei dati cloud e controlli adattivi incentrati sulle persone. Integrando l'attività cloud, il comportamento degli utenti, la threat intelligence e i dati di telemetria DLP, le aziende possono proteggere meglio le informazioni sensibili riducendo la complessità operativa.

Per saperne di più

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

Informazioni su Proofpoint, Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per saperne di più, visita www.proofpoint.com/it.

Seguici: [LinkedIn](#)

Proofpoint è un marchio registrato o nome commerciale di Proofpoint, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.

proofpoint[®]

