Proofpoint Cloud App Security Broker

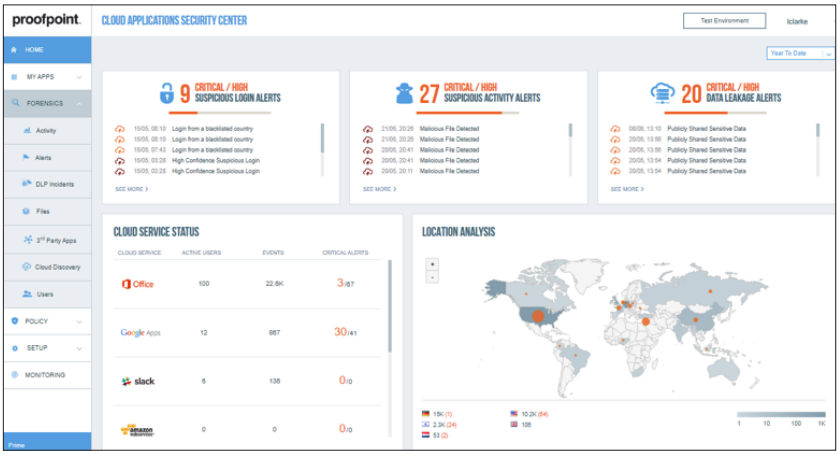
Migliora la visibilità e il controllo sulle tue applicazioni cloud

VANTAGGI PRINCIPALI

- Proteggi gli utenti del cloud grazie a visibilità sulle minacce e a controlli di accesso adattivi per le applicazioni cloud, in base a un approccio incentrato sulle persone.
- Riduci il tempo necessario per rilevare e proteggere i dati cloud regolamentati tramite policy preconfigurate per la prevenzione della fuga di dati.
- Proteggi i dati sensibili e semplifica le operazioni con policy DLP precise e unificate sui due principali vettori delle fughe di dati: le applicazioni cloud e l'email.
- Scopri le applicazioni cloud e controlla il loro utilizzo (Shadow IT), comprese le applicazioni OAuth di terze parti.
- Identifica gli account e le risorse IaaS, monitora gli account per rilevare le attività sospette e gestisci il livello di sicurezza del cloud.
- Installa la soluzione in pochi giorni e ottieni dei risultati concreti in meno di quattro settimane.

Sempre più aziende, e i loro dipendenti, adottano soluzioni cloud di tutti i tipi. Inoltre, nessun perimetro di rete protegge i tuoi utenti, le tue applicazioni e i tuoi dati. I tuoi dipendenti condividono i dati sensibili senza supervisione, e lo fanno da un gran numero di dispositivi personali. Mantenere la sicurezza è una sfida difficile, anche perché gli attacchi informatici continuano a evolversi al fine di violare gli account nel cloud e rubare denaro e dati. Con il suo approccio people-centric, Proofpoint Cloud App Security Broker (Proofpoint CASB) protegge i tuoi utenti dalle minacce nel cloud, tutela i tuoi dati sensibili, rileva le applicazioni non approvate (Shadow IT) e assicura la governance delle applicazioni OAuth cloud e di terze parti.

La sicurezza del cloud deve iniziare con la protezione delle applicazioni autorizzate dall'IT che contengono i tuoi dati più preziosi: Microsoft 365 (precedentemente Office 365), Google G Suite, Salesforce, Box, etc. Ma non è sufficiente. È necessario un approccio integrato e incentrato sulle persone che permetta di correlare le minacce e applicare policy DLP uniformi sia all'email che alle applicazioni cloud. Proofpoint CASB ti protegge dalle violazioni degli account, dalla condivisione eccessiva dei dati, dagli errori di configurazione delle risorse IaaS e PaaS e dai rischi di conformità. La nostra soluzione senza agent offre visibilità sulle minacce incentrata sulle persone, controllo degli accessiadattivo, risposta automatizzata in caso di incidente e sicurezza completa dei dati grazie alla sua funzione di prevenzione della fuga dei dati, senza dimenticare la governance delle applicazioni cloud e di terze parti, compresa la gestione del livello di sicurezza del cloud.



La console di Proofpoint CASB

La visibilità incentrata sulle persone estesa alle applicazioni cloud

Proofpoint CASB offre visibilità sulle minacce legate al cloud e all'email. Il suo approccio incentrato sulle persone ti permette di identificare i tuoi VAP (Very Attacked People™, ovvero le persone più attaccate) e di proteggere i loro dati e account cloud. Non solo: puoi anche identificare quali sono i file nelle tue applicazioni cloud che violano le regole DLP, chi ne è il titolare, chi li scarica, chi li condivide e chi li modifica.

I suoi potenti strumenti di analisi e i controlli adattivi ti aiutano a garantire adeguati livelli di accesso agli utenti e alle applicazioni OAuth di terze parti in base ai fattori di rischio che sono per te più importanti.

Protezione degli utenti contro le minacce nel cloud

Proofpoint CASB combina le nostre informazioni dettagliate sulle minacce raccolte su più canali (cloud, email e altri) con dati contestuali specifici dell'utente, al fine di analizzare i comportamenti degli utenti stessi e rilevare le anomalie fra le applicazioni e i tenant cloud. Grazie al machine learning e a un solido sistema di threat intelligence, ti aiutiamo a individuare le violazioni degli account cloud. Quando si verifica un incidente, puoi analizzare le attività e gli allarmi passati utilizzando la nostra dashboard intuitiva, incluse le attività sospette legate a file o a funzioni amministrative. Puoi inoltre esportare i dati delle indagini digitali manualmente o tramite le API REST in una soluzione di gestione degli eventi e delle informazioni di sicurezza (SIEM) per un'ulteriore analisi.

I nostri controlli adattivi incentrati sulle persone ti aiutano a contrastare diverse minacce cloud. Ti proteggiamo dalle violazioni degli account email (EAC), dallo sfruttamento delle risorse IaaS e dal furto di dati, senza compromettere la produttività degli utenti. Le nostre policy efficaci segnalano i problemi in tempo reale, applicano le misure necessarie agli account violati, mettono in quarantena i file dannosi e applicano un'autenticazione basata sul rischio, quando necessaria. Puoi inoltre integrare le tue soluzioni di gestione delle identità tramite l'autenticazione SAML (Security Assertion Markup Language).

Funzioni DLP unificate fra le applicazioni cloud e gli altri canali

Proofpoint CASB condivide i classificatori DLP (identificatori intelligenti integrati, dizionari, regole e modelli) con gli altri prodotti Proofpoint, velocizzando così il processo di identificazione e protezione dei dati sensibili. Puoi distribuire facilmente policy DLP uniformi fra le applicazioni SaaS, i compartimenti IaaS e l'email. Inoltre, puoi unificare la gestione degli incidenti DLP applicandola a più canali grazie alla console Proofpoint CASB. Oltre 240 classificatori integrati coprono le normative PCI, GDPR e le normative sui dati personali e i dati sanitari personali.

Regole personalizzate sensibili al contesto e tecnologie di rilevamento avanzate, come l'esatta corrispondenza dei dati, consentono di creare policy DLP personalizzate per controllare il modo in cui i dati vengono condivisi o scaricati. Puoi limitare l'accesso ai dati provenienti da dispositivi non gestiti, mettere in quarantena i file e limitare le autorizzazioni di condivisione per file e compartimenti, al fine di mantenere la conformità.

Ti aiutiamo a proteggere i dati a rischio identificando le autorizzazioni estese per i file e la condivisione non autorizzata dei dati. Puoi correlare accessi sospetti o compartimenti AWS S3 con gli eventi DLP.

Governance delle applicazioni cloud e di terze parti

Proofpoint CASB ti offre visibilità sulle applicazioni non approvate (Shadow IT) in tutta l'azienda. Ti aiutiamo a controllare i registri del traffico di rete e a scoprire le applicazioni cloud. Il nostro catalogo include 46.000 applicazioni, con più di 50 attributi per ciascuna. Le applicazioni cloud possono essere categorizzate per tipo e per punteggio di rischio. Questa classificazione ti consente di determinare i rischi per la sicurezza, le vulnerabilità alle fughe di dati e i punti di non conformità. Puoi bloccare le applicazioni a rischio oppure concedere agli utenti l'accesso in sola lettura.

Inoltre rileviamo e valutiamo le autorizzazioni OAuth per le applicazioni e gli script di terze parti che accedono ai servizi cloud di base approvati dal reparto IT. La nostra analisi approfondita ti aiuta a identificare le applicazioni a rischio, comprese quelle dannose, e di ridurre la superficie di attacco. Puoi definire o automatizzare determinate azioni in base al punteggio di rischio e al contesto.

Semplifica la sicurezza e la conformità IaaS multicloud e multi-regione grazie alla gestione centralizzata. Un'unica console consente di gestire il livello di sicurezza della tua infrastruttura IaaS cloud. Ti aiutiamo a individuare gli account e le risorse IaaS autorizzate e quelle non approvate, oltre a rilevare errori di configurazione e problemi di conformità.

Distribuzione rapida con l'architettura senza agent

La nostra architettura senza agent offre un eccezionale valore aggiunto. Le potenti funzionalità integrate funzionano con le tue soluzioni cloud esistenti per prevenire, rilevare e neutralizzare le minacce nel cloud, in modo rapido e automatico. L'autenticazione SAML basata sul rischio e l'isolamento del web aiutano a prevenire le minacce cloud il prima possibile. Puoi inoltre eseguire l'integrazione con le API cloud, con gli strumenti ibridi per la gestione delle identità e con i prodotti per l'orchestrazione della sicurezza (compreso Proofpoint Threat Response) per rilevare e neutralizzare qualsiasi minaccia che viola le difese.

PER SAPERNE DI PIÙ APPROFITTA DI UNA PROVA GRATUITA

Visita **proofpoint.com/it/products/cloud-app-security-broker**.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, 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 più della metà delle Fortune 1000, 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**.