Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (CAD) protegge gli utenti di Microsoft 365 e di Google Workspace dalle violazioni degli account cloud. Proofpoint CAD ti permette di rilevare, analizzare e proteggerti dai criminali informatici che accedono ai tuoi dati sensibili e ai tuoi account approvati. I nostri potenti controlli basati su policy e le nostre funzionalità di analisi forense consentono di monitorare e neutralizzare le minacce sulla base dei fattori di rischio più importanti per l'azienda.

VANTAGGI PRINCIPALI

- Identificazione dei principali utenti a rischio e monitoraggio degli incidenti tramite dashboard dettagliate
- Personalizzazione e assegnazione delle priorità agli avvisi in base ai fattori di rischio importanti per l'azienda
- Correlazione delle minacce per email e cloud per rilevare con precisione gli account compromessi
- Analisi degli incidenti di sicurezza tramite analisi forensi dettagliate e report personalizzabili
- Prevenzione dell'accesso non autorizzato alle applicazioni e ai servizi cloud tramite controlli adattivi degli accessi
- Automazione delle azioni di risposta agli incidenti di sicurezza attraverso controlli basati sulle policy flessibili
- Distribuzione rapida nel cloud
- Pluripremiato servizio di assistenza clienti

Le credenziali di accesso degli utenti sono le chiavi del regno aziendale. Se i criminali informatici riescono a violare le credenziali dei tuoi account Microsoft 365 o Google Workspace, potranno lanciare attacchi all'interno e all'esterno dell'azienda. Possono convincere gli utenti a trasferire denaro o a cedere dati sensibili. E possono accedere a dati critici, come proprietà intellettuale o dati dei clienti. Tutto ciò potrebbe danneggiare la reputazione e le finanze dell'azienda. Inoltre, una volta che i criminali informatici hanno preso piede all'interno dell'azienda, spesso installano backdoor per conservare l'accesso in previsione di attacchi futuri. Nonostante la violazione di un account si verifichi spesso ad opera del phishing, può avvenire anche tramite i seguenti metodi:

- Attacchi di forza bruta che automatizzano la ricerca sistematica delle credenziali di accesso
- Riciclo delle credenziali di accesso, o stuffing, che utilizza coppie di nome utente e password precedentemente rubate
- Malware, come key logger e programmi di furto delle credenziali

Il nostro approccio integrato incentrato sulle persone, che correla l'attività delle minacce nell'ambiente email e cloud, fornisce una protezione efficace contro la violazione degli account cloud. Combiniamo analisi basate sull'accesso al cloud e sul comportamento dell'utente con le nostre informazioni sulle minacce email. Ciò permette di identificare gli utenti a rischio e rilevare gli account compromessi.

Inoltre, preveniamo l'accesso non autorizzato grazie ai nostri controlli adattivi degli accessi per le applicazioni e i servizi cloud approvati dall'IT. Le nostre policy incentrate sulle persone segnalano i problemi in tempo reale e, se necessario, applicano i controlli in base al livello di rischio, come l'applicazione di una rete private virtuale o l'autenticazione a più fattori.

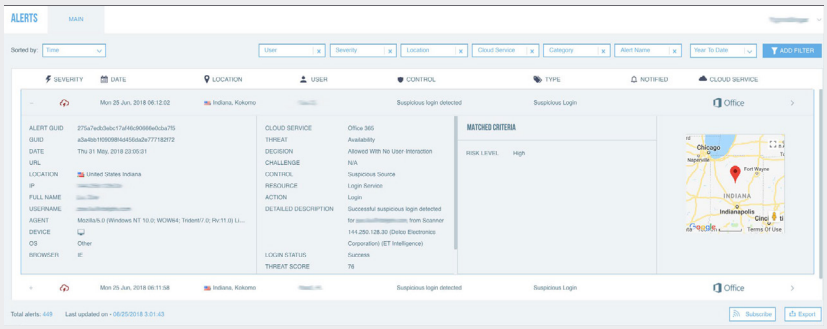
Rilevamento di account compromessi

La soluzione CAD offre visibilità sulle minacce legate al cloud e all'email. Ti aiutiamo a:

- Identificare i tuoi VAP (Very Attacked People, ovvero le persone più attaccate) e a proteggere i loro account cloud
- Rilevare le violazioni utilizzando dati contestuali come la posizione dell'utente, il dispositivo utilizzato, la rete e l'orario di accesso
- Definire comportamenti di base sicuri attraverso l'analisi
- Monitorare le anomalie utilizzando impronte digitali acquisite in precedenza, soglie di allarme e funzionalità avanzate di machine learning, e cercare attività sospette come tentativi di login eccessivi e insoliti, come comportamenti brute-force ed eventi di tipo "too-fast-to-travel" (incoerenza nella localizzazione)

La soluzione CAD combina anche una threat intelligence multivettoriale completa - proposta dal grafico delle minacce Nexus di Proofpoint - con indicatori di rischio specifici per l'utente. Ciò consente di rilevare connessioni da fonti sospette.

Utilizzando le nostre informazioni globali sulle minacce, effettuiamo controlli della reputazione degli IP. Inoltre, correliamo l'attività delle minacce attraverso email e cloud. Le nostre informazioni sulle minacce basate su email consentono di collegare i punti tra gli attacchi tramite email di phishing delle credenziali e i login sospetti. I criminali informatici possono utilizzare un account compromesso per lanciare un attacco di phishing e violare altri utenti dell'azienda. Per identificare altri account compromessi, studiamo l'impronta digitale dell'autore dell'attacco, per individuare le intestazioni User-Agent e le attività insolite, incluso l'inoltro delle email.



Analisi digitali granulari degli incidenti

Quando si verifica un incidente, è possibile indagare le attività passate e gli avvisi attraverso la nostro dashboard intuitiva. Qui è possibile esaminare dati forensi granulari sulle transazioni, come utente, data, ora, indirizzo IP, dispositivo, browser, intestazione User Agent, posizione, minaccia, punteggio di minaccia e altro ancora. È anche possibile visualizzare e analizzare questi dati tramite grafici e report di log dettagliati. Inoltre, è possibile ordinare o filtrare i registri delle attività e degli avvisi per personalizzare i report d'indagine. E puoi ricevere i report su base giornaliera, settimanale o mensile. Per ulteriori analisi, i dati forensi possono essere esportati manualmente o tramite l'integrazione con soluzioni SIEM, con il supporto di API REST.

Protezione degli account Microsoft 365 e Google Workspace tramite policy flessibili

Grazie alle informazioni approfondite ottenute con le nostre analisi forensi dettagliate, è possibile creare policy correttive flessibili basate su un'ampia gamma di parametri, tra cui utente, posizione, rete, dispositivo, attività sospette e altro ancora. Ad esempio, è possibile generare avvisi di accesso per i paesi inclusi in blacklist o per i dispositivi che non soddisfano le linee guida aziendali. Inoltre, quando si esegue il monitoraggio di un servizio ad alto utilizzo come Microsoft 365 o Google Workspace, è necessario assegnare priorità agli avvisi per evitare una minore vigilanza a causa dell'elevato numero di allarmi. La soluzione CAD permette di generare notifiche di avviso in base alla loro gravità. È possibile personalizzare ogni notifica o utilizzare il modello predefinito. È inoltre possibile monitorare più da vicino gli utenti a rischio o sospenderli in caso di accesso sospetto.

I controlli adattivi degli accessi di Proofpoint CAD permettono di applicare in tempo reale misure di sicurezza incentrate sulle persone in base al livello di rischio, al contesto e al ruolo. I tentativi di accesso da siti e reti ad alto rischio e da parte di hacker noti vengono così bloccati automaticamente. Inoltre, puoi applicare controlli basati sui rischi ai VAP e agli utenti con privilegi elevati, tra cui l'autenticazione incrementale e l'applicazione di reti private virtuali.

Distribuzione rapida nel cloud

Le piattaforme basate sul cloud necessitano di una protezione basata sul cloud. La nostra architettura cloud e la protezione basata su API Microsoft 365 o Google Workspace consentono una rapida implementazione e un ritorno immediato in termini di valore.

Implementando i controlli adattivi degli accessi puoi reindirizzare i login alle applicazioni cloud verso il nostro gateway di autenticazione SAML (Security Assertion Markup Language). Questo gateway applica un processo di autenticazione federata agendo come interfaccia tra ogni fornitore di servizi e il provider di identità. La soluzione CAD supporta tutti i servizi cloud approvati dall'IT e federati tramite SAML 2.0. Per garantire un'autenticazione solida, è possibile integrare la soluzione di autenticazione a più fattori o utilizzare la nostra applicazione di autenticazione mobile Proofpoint Mobile Access, inclusa nella soluzione CAD. È possibile proteggere centinaia di migliaia di utenti in pochi giorni, non settimane o mesi.

In qualità di leader del settore nella protezione dalle minacce, utilizziamo il cloud per aggiornare quotidianamente il nostro software e aiutarti a essere sempre un passo avanti rispetto agli aggressori. La nostra distribuzione in cloud offre inoltre la flessibilità di proteggere gli utenti su qualsiasi rete o dispositivo.

APPROFONDISCI

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