proofpoint.

Piattaforma Proofpoint Identity Threat Defense

Blocca l'escalation dei privilegi e gli spostamenti laterali

Prodotti

- Proofpoint Shadow
- Proofpoint Spotlight

Vantaggi principali

- Identificazione, definizione delle priorità e correzione delle vulnerabilità legate alle identità
- Comprensione dei rischi legati alle identità con privilegi e vie d'attacco disponibili nel tuo ambiente
- Visibilità sulle vulnerabilità legate alle identità per Active Directory, Entra ID, AWS Identity Center, Okta, le soluzioni PAM, gli endpoint e LAPS
- Correzione automatica delle vulnerabilità legate alle identità sugli endpoint
- Rilevamento precoce dei criminali informatici e accelerazione delle indagini sulle minacce
- Utilizzo di una tecnologia senza agent che i criminali informatici non possono eludere
- Eliminazione delle lacune lasciate dal rilevamento delle minacce basato su firme e comportamenti
- Integrazione con Proofpoint TAP, TAP ATO e NPRE
- Implementazione SaaS possibile

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.

Gli attacchi sono diventati molto più sofisticati e mirati. Le soluzioni volte a proteggerci non riescono a tenere il passo[1]. Le tendenze suggeriscono che i criminali informatici stanno standardizzando le loro tattiche, tecniche e procedure per concentrarsi sull'identità. Le aziende non sono ancora riuscite a interrompere la catena d'attacco in modo affidabile. Le identità sono un elemento fondamentale della superficie d'attacco che richiede una maggior attenzione.

La piattaforma Proofpoint Identity Threat Defense offre protezione end-to-end contro le minacce legate alle identità. Include i prodotti Proofpoint Shadow e Proofpoint Spotlight. Offre funzionalità di identificazione e correzione delle vulnerabilità legate alle identità nonché rilevamento delle minacce senza agent basato su esche e raccolta di dati forensi. La piattaforma ti consente di individuare, definire le priorità e correggere le identità vulnerabili e ti aiuta a rilevare e neutralizzare le minacce attive.

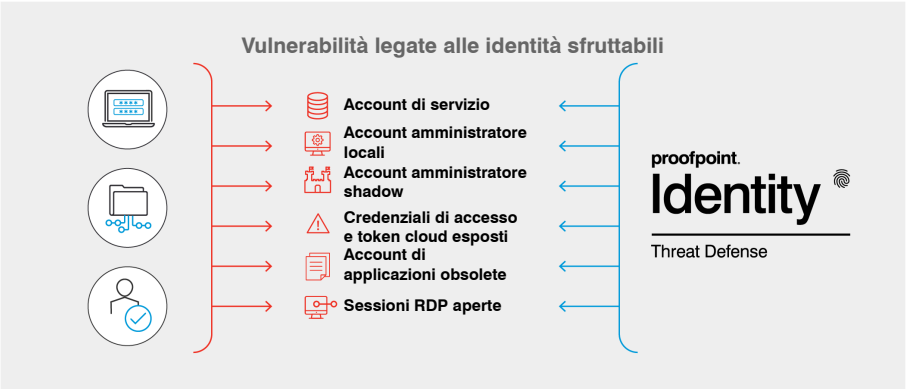

Figura 1. Proofpoint Identity Threat Defense e le vulnerabilità legate alle identità sfruttabili

1 Alcune di queste soluzioni includono la gestione di identità e accessi (IAM), l'autenticazione a più fattori (MFA), il rilevamento e la risposta agli incidenti per gli endpoint (EDR), la gestione degli eventi e delle informazioni di sicurezza (SIEM) e il rilevamento e la risposta avanzata agli incidenti (XDR).

Crisi dell'identità

La maggior parte delle aziende implementa Active Directory. Sfortunatamente, il 79% di queste ha subito una violazione legata alle identità negli ultimi due anni. In base al report di Verizon sulle violazioni dei dati, il 94% degli attacchi andati a buon fine ha utilizzato Active Directory e le identità con privilegi per aumentare i loro privilegi. I criminali informatici utilizzano un'ampia gamma di strumenti. Bloodhound, Cobalt Strike, Mimikatz e ADFind sono solo alcuni esempi. Questi strumenti li aiutano a sfruttare le identità con privilegi in modo rapido e rendono difficile il rilevamento dei loro attacchi.

Secondo le ricerche condotte da Proofpoint, un endpoint aziendale su sei (client e server), contiene identità vulnerabili, anche in presenza di soluzioni tradizionali di gestione delle identità e degli accessi (IAM). I criminali informatici sfruttano queste vulnerabilità per ottenere accesso a privilegi di amministratore. Quando si infiltrano in un host, raramente si tratta dell'obiettivo finale. Cercano di spostarsi lateralmente all'interno della rete alla ricerca delle risorse IT più critiche (di livello 0). Una volta raggiunti tali obiettivi, possono esfiltrare i dati o lanciare attacchi ransomware.

Figura 2. Piattaforma Proofpoint Identity Threat Defense

Molte vulnerabilità legate alle identità derivano dalle normali procedure aziendali e operative IT, come le seguenti:

- **Nomi utente e password.** Le applicazioni degli utenti spesso memorizzano questi dati nella cache sui loro endpoint (browser, SSH, FTP, PuTTY, database, ecc.). Le soluzioni PAM non proteggono queste credenziali d'accesso.
- **Credenziali di accesso dell'amministratore di dominio.** Alcune volte tali credenziali vengono conservate nella memoria di sistema dopo una sessione di assistenza da remoto e vengono spesso memorizzate nella cache in un account di servizio non protetto.
- **Privilegi shadow.** La configurazione di oggetti e gruppi della directory di identità in Active Directory può essere molto complessa. Per questo motivo, ad alcuni utenti possono essere inavvertitamente assegnati privilegi shadow eccessivi.

Visibilità completa sulla sicurezza delle identità

Gli attacchi di successo sfruttano le lacune nella gestione e nella protezione. La nostra piattaforma aiuta i responsabili della sicurezza a individuare e correggere tali lacune. Ecco i vantaggi offerti:

1. **Identificazione.** Beneficia di una visibilità continua sulle vulnerabilità legate alle identità in AD, Entra ID, AWS Identity Center, Okta e gli endpoint.
2. **Definizione delle priorità e correzione.** Ottieni un elenco di vulnerabilità classificato in base al loro livello di priorità. Questi rischi appaiono su una scala che va da "non critico" a "urgente!". Attiva la correzione automatica delle vulnerabilità legate alle identità direttamente dalla piattaforma. Puoi configurare regole per le eccezioni conformi alle tue policy di sicurezza.
3. **Rilevamento e risposta.** Rileva quando i criminali informatici sono attivi nel tuo ambiente. Grazie alle esche senza agent, puoi rilevare attività come Kerberoasting, password spray, uso improprio degli account con privilegi e altro ancora. Puoi utilizzare la raccolta di dati forensi automatizzata per indirizzare la risposta della tua azienda alle minacce attive.

PER SAPERNE DI PIÙ

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

0213-003-05-04 6/24