Proofpoint Spotlight

Identifica, assegna le priorità e corregge automaticamente le vulnerabilità legate alle identità prima che i criminali informatici le sfruttino

Vantaggi principali

- Identificazione dei rischi legati alle identità in varie fasi della catena d'attacco
- Visibilità sulle identità, tra cui: Active Directory, Entra ID (in precedenza Azure AD), PAM, Endpoint, LAPS
- Conseguimento automatico di una lista di priorità delle vulnerabilità legate alle identità sugli endpoint
- Correzione manuale o automatica delle vulnerabilità come gli amministratori shadow
- Visibilità sui rischi di tutte le filiali e delle entità di nuova acquisizione grazie a una mappa dei domini e delle approvazioni dell'azienda
- Generazione intelligente di report sulle tendenze dei rischi nel tempo per migliorare il livello di sicurezza delle tue identità

Il furto e l'abuso delle credenziali di accesso rappresentano una minaccia onnipresente e crescente. I criminali informatici si focalizzano sulle identità piuttosto che sui sistemi. Possono eseguire questi attacchi in ore o minuti, senza lasciare alcuna traccia di violazione o malware.

Nonostante l'implementazione della gestione degli account con privilegi (PAM) e dell'autenticazione a più fattori (MFA), un endpoint aziendale sui sei presenta identità vulnerabili. Si tratta di obiettivi primari per i criminali informatici. I ransomware e altre minacce mirate si concentrano sulle identità con privilegi per raggiungere i loro obiettivi.

Proofpoint Spotlight può contribuire a ridurre il rischio che le tue identità vengano utilizzate contro di te. La soluzione è parte della piattaforma Proofpoint Identity Threat Defense. Fornisce un'identificazione continua e completa delle vulnerabilità legate alle identità e corregge automaticamente queste minacce. Proofpoint Spotlight blocca le minacce legate alle identità prima che possano trasformarsi in violazioni su larga scala.

I progettisti della difesa nazionale hanno sviluppato Proofpoint Spotlight per aiutare i team della sicurezza a dare priorità alle attività di correzione automatica delle minacce. L'obiettivo degli avvisi è quello di evitare qualsiasi impatto sulle attività. Tuttavia, il crescente volume di questi avvisi ha portato a un aumento delle informazioni non necessarie, che i team della sicurezza devono prioritizzare.

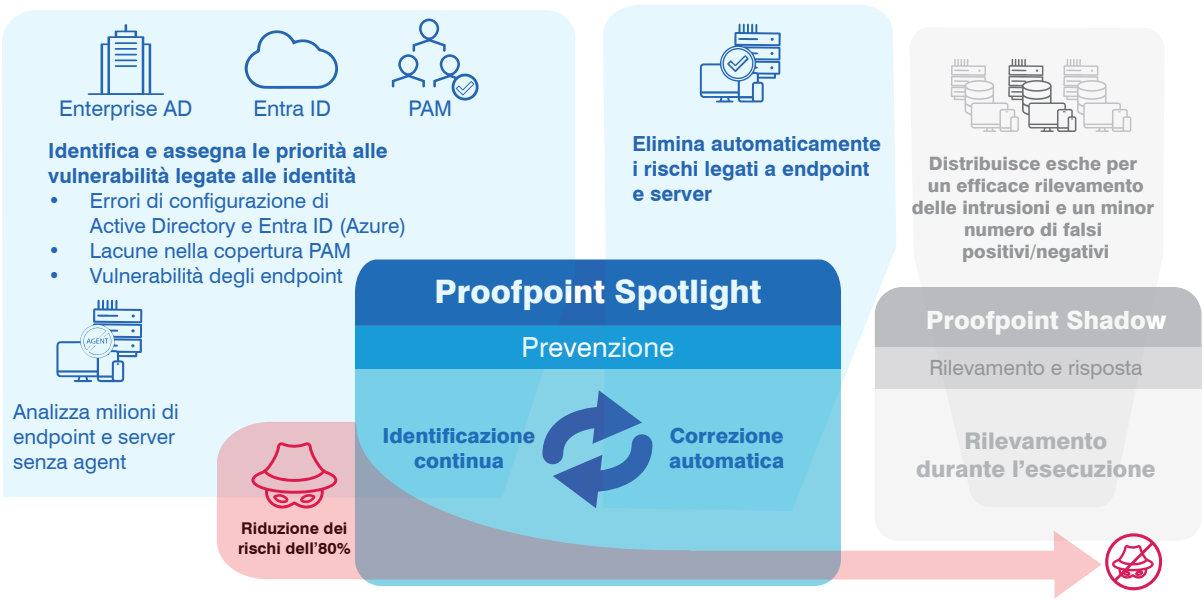

Figura 1. Componente della piattaforma Proofpoint Identity Threat Defense, Proofpoint Spotlight offre identificazione e correzione delle vulnerabilità legate alle identità con privilegi e delle violazioni delle policy.

Come i criminali informatici sfruttano le identità con privilegi

Quando i criminali informatici si infiltrano in un host, generalmente non si tratta dell'obiettivo finale. Nella maggior parte degli attacchi, i criminali informatici cercano di elevare i privilegi. Quindi si spostano lateralmente nell'ambiente per raggiungere il loro obiettivo reale senza essere rilevati. Utilizzano strumenti come Bloodhound, Cobalt Strike, Mimikatz e ADFind per sfruttare rapidamente le credenziali d'accesso con privilegi e nascondere la loro presenza.

Nelle nostre ricerche, abbiamo scoperto che oltre il 90% delle aziende ha subito una violazione legata alle identità nel corso dell'anno scorso. Inoltre, gli attacchi ransomware hanno raggiunto livelli record. Numerosi fattori spiegano questo aumento. In primo luogo, le distribuzioni di sistemi di gestione delle identità e degli accessi sono estremamente complesse. Inoltre, le identità evolvono costantemente. Le aziende non dispongono di una visibilità completa sulle lacune nel loro ambiente.

Altri fattori sono i seguenti:

- Configurazione PAM e gestione delle credenziali d'accesso degli account di servizio, degli amministratori locali e dei domini con privilegi insufficienti o errati
- Creazione involontaria di account amministratore shadow che dispongono di privilegi eccessivi
- Interruzione impropria delle sessioni RDP
- Applicazioni utente (browser, SSH, FTP, PuTTY, database, ecc.) che memorizzano credenziali e token d'accesso nella cache sugli endpoint

Esempio reale: Attacco contro una compagnia di assicurazioni

Un criminale informatico ha utilizzato la tecnica di riciclaggio delle credenziali d'accesso (credential stuffing) per accedere a una rete tramite il protocollo RDP (Remote Desktop Protocol). Per l'accesso iniziale, il criminale informatico ha utilizzato credenziali d'accesso rubate.

Quindi ha elevato i privilegi a amministratore di dominio. I dati critici sono stati cifrati e una parte sono stati esfiltrati. L'azienda ha pagato un riscatto di 40 milioni di dollari per riprendersi dall'attacco.

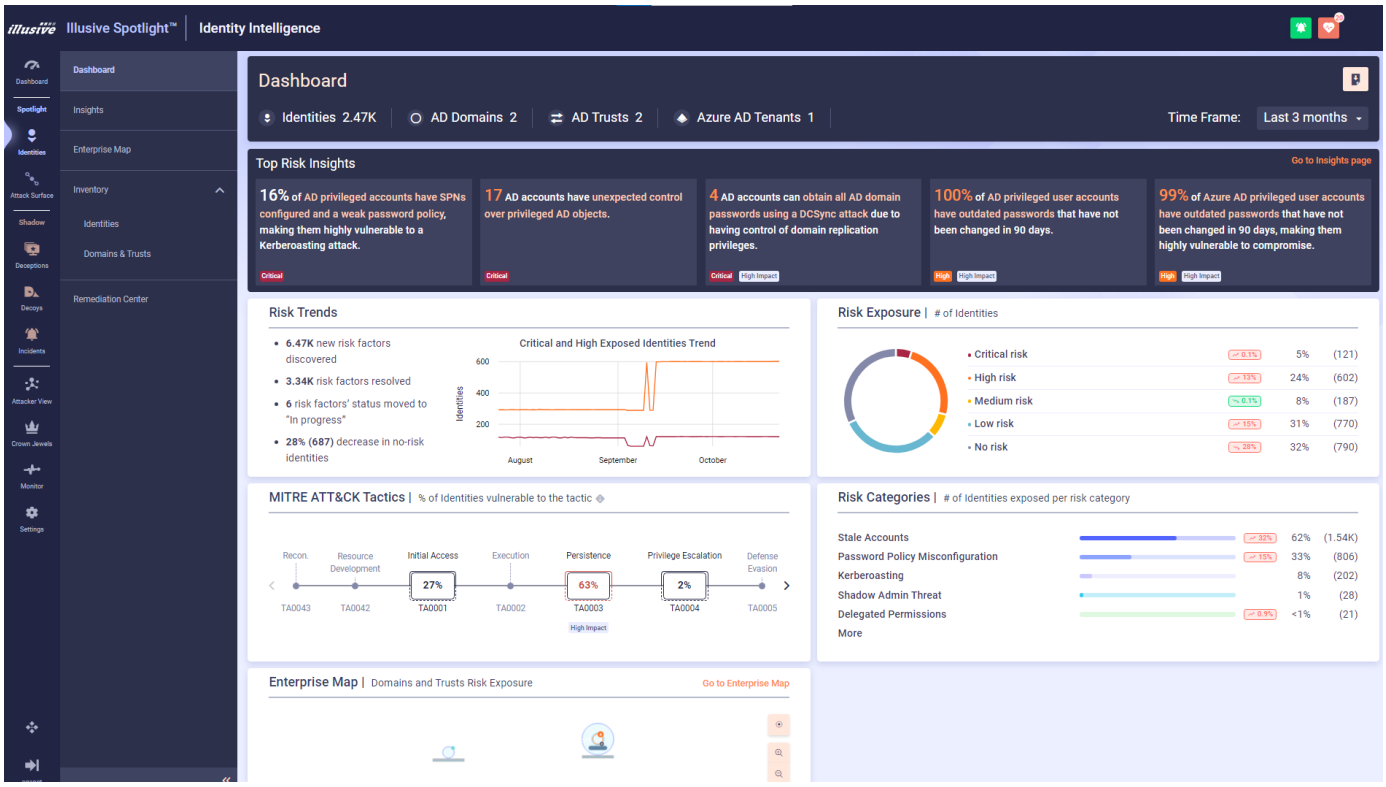

Figura 2. Dashboard dei rischi legati alle identità di Proofpoint Spotlight.

Identificazione, prioritizzazione e correzione delle identità vulnerabili

Proofpoint Spotlight rivela le lacune tra le tue policy di sicurezza delle identità e i tuoi ambienti reali. Analizza i seguenti sistemi per fornire visibilità e prioritizzazione complete delle attuali vulnerabilità legate alle identità:

- **Strutture della directory.** Active Directory e Entra ID (in precedenza Azure AD)
- **Soluzioni PAM.** CyberArk e Delinea Centrify.
- **Endpoint.** Client e server.
- **Attività.**

Proofpoint Spotlight permette di prevenire gli attacchi eliminando le vulnerabilità legate alle identità di cui i criminali informatici hanno bisogno per eseguire attacchi che possono trasformarsi in violazioni su larga scala.

PER SAPERNE DI PIÙ

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

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, 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 il 75% delle Fortune 100, 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**.