Proofpoint Shadow

Blocca l'escalation dei privilegi e gli spostamenti laterali in tempo reale

Vantaggi principali

- Rilevamento precoce dei criminali informatici e indagini complete sulle minacce
- Riduzione dei falsi positivi nel SOC grazie ad avvisi affidabili
- Tecnologia senza agent per una facile distribuzione con un minimo coinvolgimento del team IT
- Difesa continua grazie ad adattamenti automatici in base ai cambiamenti dell'ambiente IT
- Scalabilità comprovata su reti con oltre un milione di endpoint
- Eliminazione delle lacune lasciate dal rilevamento delle minacce basato su firme e anomalie

Oltre il 90% degli attacchi informatici coinvolge identità a rischio. I criminali informatici hanno adattato le loro strategie e prendono di mira le identità con privilegi invece di cercare di violare direttamente i sistemi. Questa transizione ha portato a un aumento degli attacchi di ransomware andati a buon fine e delle violazioni dei dati. Concentrandosi sulle identità vulnerabili, i criminali informatici possono accorciare i tempi di attacco da mesi a pochi giorni o addirittura ore.

Proofpoint può aiutarti. La nostra potente soluzione Proofpoint Shadow trasforma i tuoi endpoint in una rete di esche diversive che rende quasi impossibile gli spostamenti laterali dei criminali informatici nel tuo ambiente senza essere rilevati. Parte della piattaforma Proofpoint Identity Threat Defense, Proofpoint Shadow rileva i criminali informatici in modo deterministico in funzione delle loro interazioni con percorsi di attacco apparentemente legittimi sui tuoi endpoint, ma che in realtà sono esche diversive da noi distribuite.

A differenza di altri strumenti, Proofpoint Shadow non si basa su analisi basate su firme o comportamenti. Inoltre, non utilizza agent o honeypot che possono essere sfruttati. Al contrario, l'architettura senza agent di Proofpoint Shadow permette alle esche diversive di operare nell'ombra. Proofpoint Shadow ha dimostrato la sua efficacia in oltre 160 esercitazioni di simulazioni di attacchi con alcune delle principali aziende di sicurezza nel mondo, tra cui Microsoft, Mandiant, il Dipartimento della Difesa degli Stati Uniti e Cisco.

Figura 1. I criminali informatici sono ora focalizzati sulle identità vulnerabili come principale via d'accesso tramite la catena d'attacco.

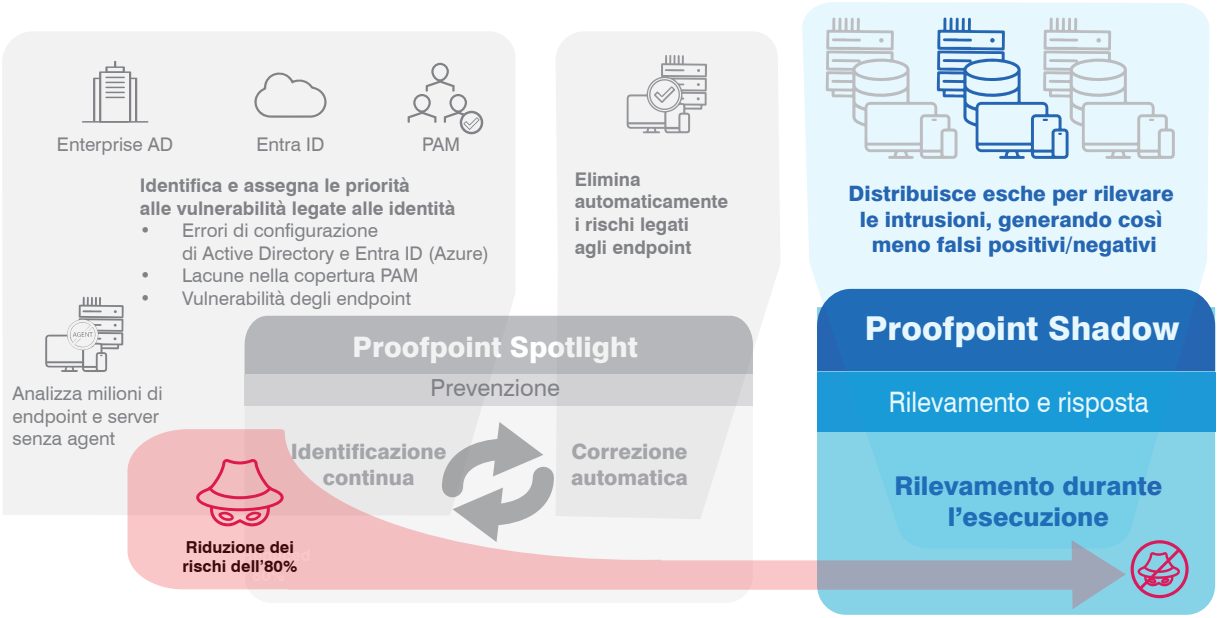

Figura 2. Parte della piattaforma Proofpoint Identity Threat Defense, Proofpoint Shadow crea una rete di esche diversive che rilevano e segnalano lo spostamento laterale di un criminale informatico nelle tue reti.

Rilevamento deterministico invece che probabilistico

Puoi rilevare e neutralizzare le minacce in diversi modi. Per esempio, puoi ricercare schemi, o firme, molto specifici. Puoi anche analizzare il comportamento di un potenziale criminale informatico. Gli strumenti convenzionali spesso non riescono a rilevare attacchi gravi, per esempio quando i criminali informatici scalano i privilegi o si spostano lateralmente nella tua rete senza essere rilevati. Questi errori di rilevamento possono permettere ai criminali informatici di prendere il controllo degli account, distribuire ransomware o rubare i dati. I team della sicurezza hanno bisogno di un approccio più avanzato e affidabile per tenere testa a questo tipo di attacchi.

Proofpoint Shadow fornisce un approccio deterministico. Utilizza esche diversive ampiamente distribuite per interagire attivamente con i criminali informatici lungo la catena di attacco e tenere traccia delle loro attività. Questi diversivi sono dissimulati accuratamente negli endpoint dell'azienda. Sembrano e si comportano come file, sessioni RDP, connessioni a database, email, script e altre risorse legittime di cui i criminali informatici vogliono impossessarsi. Quando un criminale informatico interagisce con uno di questi, Proofpoint Shadow invia un avviso in tempo reale con dati forensi al team della sicurezza. Il team può quindi utilizzare queste informazioni per compiere scelte intelligenti per bloccare l'attacco e proteggere l'azienda.

Rilevamento e protezione senza agent

L'esclusivo approccio binario senza agent di Proofpoint Shadow aiuta sia gli amministratori IT che i team della sicurezza. Basata sull'automazione intelligente, la soluzione non disturba le attività per ridurre al minimo l'impatto sull'IT. Inoltre, a differenza degli strumenti di sicurezza che si basano su agent software, i criminali informatici non possono disattivare o eludere Proofpoint Shadow.

Oltre 75 tecniche evasive

Proofpoint Shadow utilizza oltre 75 tecniche tecniche evasive attive. Crea falsi file e condivisioni di file, connessioni ai database, connessioni FTP e RDP/SSH, cronologie dei browser e URL, credenziali di accesso Windows, sessioni di rete, email, script e anche cronologie delle chat di Teams che fungono da inneschi dissimulati che sembrano essere veramente preziosi per i criminali informatici. Queste tecniche operano di concerto per cogliere i criminali informatici sul fatto, indipendentemente dal punto in cui inizia la violazione, all'interno o all'esterno dell'ambiente.

Con Proofpoint Shadow, i team della sicurezza possono automatizzare la creazione di centinaia di falsi file Word e Excel personalizzati che sembrano quelli veri. Possono anche includere il logo e l'intestazione della tua azienda. I dati fasulli incorporati nei documenti attivano allarmi inviati agli amministratori della sicurezza se un criminale informatico cerca di utilizzarli per ottenere un accesso più ampio.

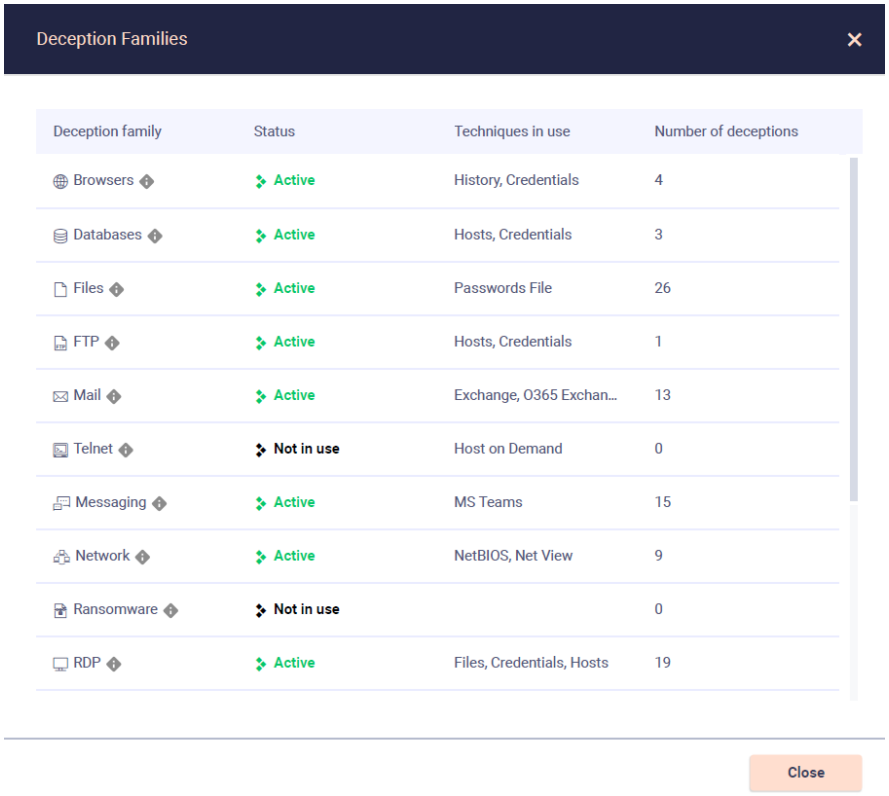

Figura 3. L'interfaccia utente di Proofpoint Shadow.

Esche diversive automatizzate e personalizzate per ogni endpoint

Il sistema di automazione intelligente di Proofpoint Shadow crea delle esche diversive realistiche e convincenti per i criminali informatici. Può facilmente evolvere e adattarsi senza sovraccaricare il team della sicurezza. Proofpoint Shadow analizza il panorama degli endpoint, crea esche diversive personalizzate per ogni macchina e le distribuisce in un solo clic. La soluzione si fa inoltre carico del processo costante di adattamento e gestione delle esche diversive nel tempo.

Punto di vista dei criminali informatici

La console di gestione di Proofpoint Shadow è ricca di dati forensi sulle attività dei criminali informatici. Fornisce ai team della sicurezza dati importanti sull'avanzamento dei criminali informatici verso le tue risorse strategiche. Può anche visualizzare una cronologia completa delle loro attività una volta che le esche diversive sono state attivate. Infine, può mostrare agli analisti della sicurezza come appaiono le esche diversive dal punto di vista dei criminali informatici.

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**.