Proofpoint Spotlight

Identifiez, hiérarchisez et corrigez automatiquement les vulnérabilités liées aux identités avant que les cybercriminels ne les exploitent

Principaux avantages

- Identification des risques liés aux identités à plusieurs étapes de la chaîne d'attaque
- Visibilité sur les identités, couvrant : Active Directory, Entra ID (anciennement Azure AD), PAM, endpoints, LAPS
- Obtention automatique d'une liste hiérarchisée des vulnérabilités liées aux identités sur les endpoints
- Correction manuelle ou automatique des vulnérabilités telles que les administrateurs fantômes
- Visibilité sur les risques de toutes les filiales et des entités récemment acquises grâce à une carte des domaines et des approbations de l'entreprise
- Génération intelligente de rapports sur les tendances de risques au fil du temps afin d'améliorer le niveau de sécurité de vos identités

Le vol et l'exploitation d'identifiants de connexion constituent une menace omniprésente et grandissante. Les cybercriminels portent désormais leur attention sur les identités plutôt que les systèmes. Ils peuvent exécuter ces attaques en quelques heures, voire en quelques minutes, et ne laisser aucune trace de compromission ou de malware.

Malgré la mise en place de la gestion des comptes à privilèges (PAM) et de l'authentification multifacteur (MFA), un endpoint d'entreprise sur six présente des identités vulnérables. Ce sont des cibles de choix pour les cybercriminels. Les ransomwares et autres menaces ciblées se concentrent sur les identités à privilèges pour parvenir à leurs fins.

Proofpoint Spotlight peut contribuer à réduire le risque que vos identités soient utilisées contre vous. La solution fait partie de la plate-forme Proofpoint Identity Threat Defense. Elle propose une identification continue et complète des vulnérabilités liées aux identités et corrige automatiquement ces menaces. Proofpoint Spotlight bloque les menaces liées aux identités avant qu'elles ne se transforment en compromissions de grande ampleur.

Des ingénieurs de la défense nationale ont développé Proofpoint Spotlight pour aider les équipes de sécurité à hiérarchiser les tâches de correction automatique des menaces. Les alertes ont pour but d'éviter tout impact sur les activités. Toutefois, le volume croissant de ces alertes a conduit à une hausse des informations parasites, que les équipes de sécurité doivent prendre le temps de trier.

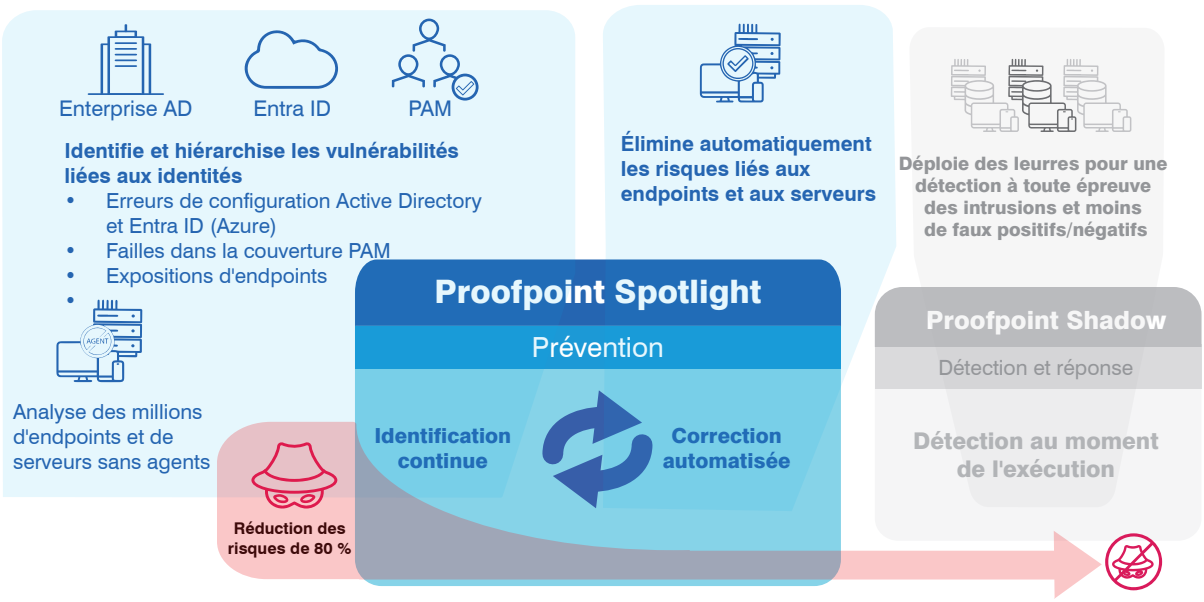

Figure 1. Composant de la plate-forme Proofpoint Identity Threat Defense, Proofpoint Spotlight propose une identification et une correction continues des vulnérabilités liées aux identités à privilèges et des violations des règles.

Comment les cybercriminels exploitent les identités à privilèges

Lorsque des cybercriminels infiltrent un hôte, il ne s'agit généralement pas de leur cible finale. Dans la plupart des attaques, les cyberpirates tentent d'élever les privilèges. Ils se déplacent ensuite latéralement dans l'environnement pour atteindre leur véritable objectif sans être détectés. Ils ont recours à des outils tels que Bloodhound, Cobalt Strike, Mimikatz et ADFind pour exploiter rapidement des identifiants de connexion à privilèges et dissimuler leur présence.

Lors de nos recherches, nous avons découvert que plus de 90 % des entreprises ont été victimes d'une compromission liée aux identités au cours de l'année écoulée. Par ailleurs, les attaques de ransomwares ont atteint des niveaux records. De nombreux facteurs expliquent cette hausse. Premièrement, les déploiements de systèmes de gestion des identités et des accès sont très complexes. En outre, les identités évoluent constamment. Les entreprises manquent également d'une visibilité complète sur les failles de leur environnement.

Les autres facteurs en cause sont notamment les suivants :

- Configuration PAM et gestion des identifiants de connexion des comptes de service, des administrateurs locaux et des domaines à privilèges insuffisantes ou incorrectes
- Création involontaire de comptes administrateur fantômes disposant de privilèges excessifs
- Fermeture incorrecte de sessions RDP
- Applications utilisateur (navigateurs, SSH, FTP, PuTTY, bases de données, etc.) mettant des identifiants de connexion et des jetons d'accès cloud en cache sur les endpoints

Exemple concret : attaque contre une compagnie d'assurance

Un cybercriminel a utilisé la technique du recyclage d'identifiants de connexion (« credential stuffing ») pour accéder à un réseau via le protocole RDP (Remote Desktop Protocol). Pour l'accès initial, le cyberpirate a eu recours à des identifiants de connexion volés.

Il a ensuite élevé les privilèges en administrateur de domaine. Les données critiques ont été chiffrées et une partie d'entre elles ont été exfiltrées. L'entreprise a payé une rançon de 40 millions de dollars pour se remettre de l'attaque.

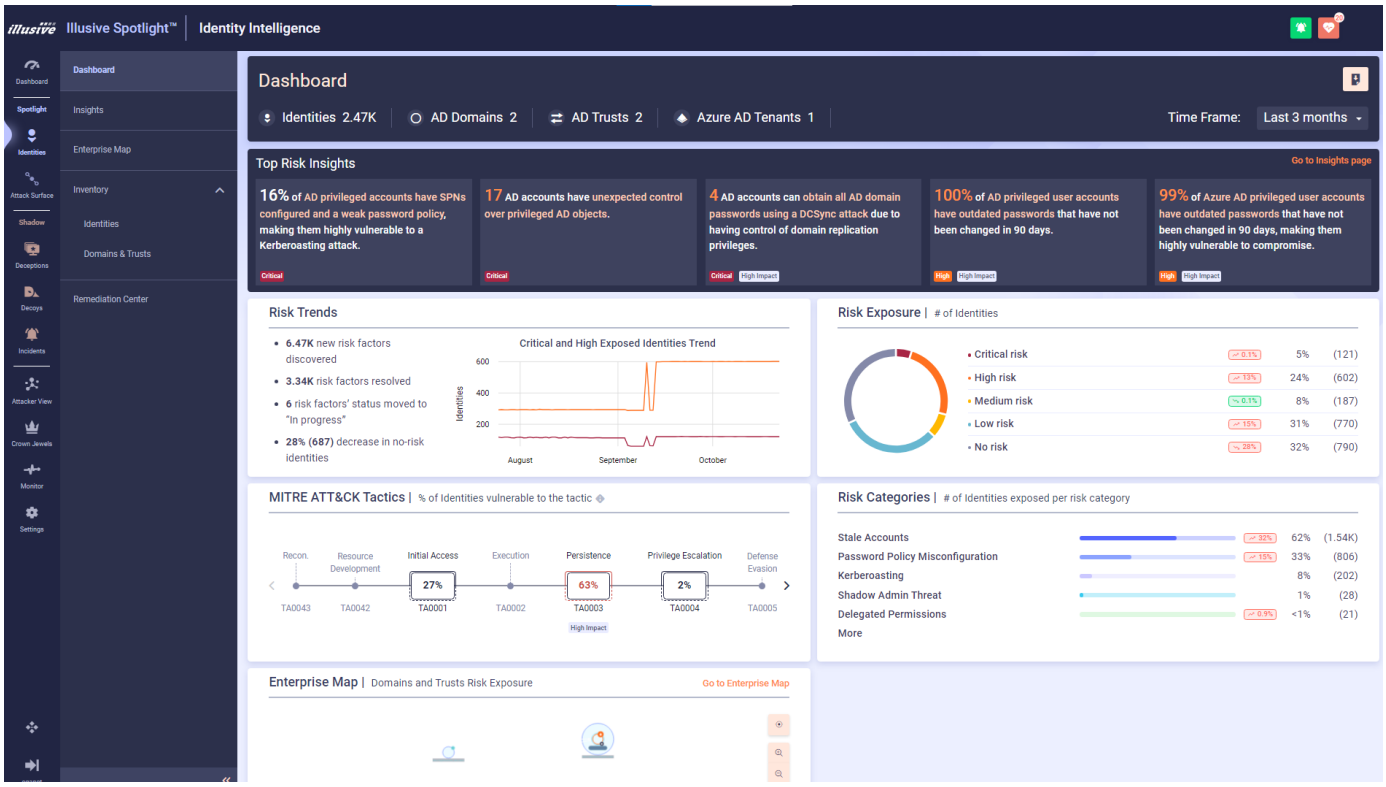

Figure 2. Tableau de bord des risques liés aux identités de Proofpoint Spotlight

Identification, hiérarchisation et correction des identités vulnérables

Proofpoint Spotlight révèle les failles entre vos règles de sécurité des identités et vos environnements réels. Il analyse les systèmes suivants pour offrir une visibilité et une hiérarchisation complètes des vulnérabilités actuelles liées aux identités :

- **Structures d'annuaire.** Active Directory et Entra ID (anciennement Azure AD).
- **Solutions PAM.** CyberArk et Delinea Centrify.
- **Endpoints.** Clients et serveurs.
- **Tâches.**

Proofpoint Spotlight permet de prévenir les attaques en éliminant les vulnérabilités liées aux identités dont les cybercriminels ont besoin pour exécuter des attaques qui peuvent aboutir à des compromissions de grande ampleur.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.