proofpoint.

Plate-forme Proofpoint Identity Threat Defense

Bloquez les élévations de privilèges et les déplacements latéraux

Solutions

- Proofpoint Shadow
- Proofpoint Spotlight

Principaux avantages

- Découverte, hiérarchisation et correction des vulnérabilités liées aux identités
- Identification des risques liés aux identités à privilèges et des voies d'attaque disponibles dans votre environnement
- Visibilité sur les vulnérabilités liées aux identités couvrant Active Directory, Entra ID, AWS Identity Center, Okta, les solutions PAM, les endpoints et LAPS
- Correction automatique des vulnérabilités liées aux identités sur les endpoints
- Détection des cybercriminels à un stade précoce et accélération des investigations sur les menaces
- Utilisation d'une technologie sans agent que les cybercriminels ne peuvent pas contourner
- Élimination des failles laissées par la détection des menaces basée sur les signatures et les comportements
- Intégration avec Proofpoint TAP, TAP ATO et NPRE
- Déploiement SaaS possible

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à réduire les quatre catégories clés de risques liés aux utilisateurs.

Les attaques sont devenues beaucoup plus sophistiquées et ciblées. Les solutions censées nous protéger sont à la traîne[1]. Les tendances suggèrent que les cybercriminels sont en train de standardiser leurs tactiques, techniques et procédures pour se concentrer sur l'identité. Les entreprises ne sont pas encore parvenues à briser la chaîne d'attaque de manière fiable. Les identités constituent un élément essentiel de la surface d'attaque, qui requiert une attention accrue.

La plate-forme Proofpoint Identity Threat Defense offre une protection de bout en bout contre les menaces liées aux identités. Elle inclut les composants Proofpoint Shadow et Proofpoint Spotlight. Elle permet la découverte et la correction des vulnérabilités liées aux identités, ainsi qu'une détection des menaces sans agent basée sur des leurres et la collecte de données d'investigation numérique. La plate-forme vous permet de découvrir, de hiérarchiser et de corriger les identités vulnérables, et vous aide à détecter et à neutraliser les menaces actives.

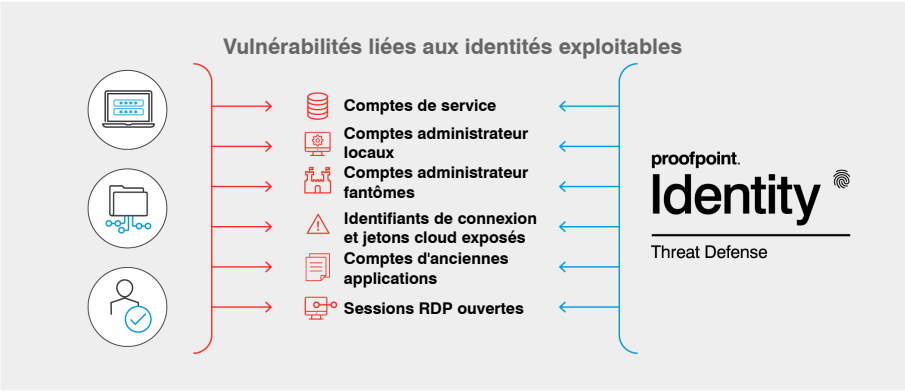

Figure 1. Proofpoint Identity Threat Defense et vulnérabilités liées aux identités exploitables

1 Certaines de ces solutions incluent la gestion des identités et des accès (IAM), l'authentification multifacteur (MFA), la détection et la réponse aux incidents pour endpoints (EDR), la gestion des événements et des informations de sécurité (SIEM) et la détection et la réponse avancées aux incidents (XDR).

Crise de l'identité

La plupart des entreprises déploient Active Directory. Malheureusement, 79 % d'entre elles ont été victimes d'une compromission liée aux identités au cours des deux dernières années. Selon le rapport d'enquête de Verizon sur les compromissions de données, 94 % des attaques réussies ont utilisé Active Directory et des identités à privilèges pour élever leurs privilèges. Les cybercriminels ont recours à un large éventail d'outils. Bloodhound, Cobalt Strike, Mimikatz et ADFind ne sont que quelques exemples. Ces outils les aident à exploiter rapidement des identités à privilèges et compliquent la détection de leurs attaques.

D'après les recherches menées par Proofpoint, un endpoint d'entreprise sur six (clients et serveurs) contient des identités vulnérables, même lorsque des solutions traditionnelles de gestion des identités et des accès (IAM) sont en place. Les cyberpirates exploitent ces vulnérabilités pour obtenir un accès à des privilèges administrateur. Lorsqu'ils infiltrent un hôte, celui-ci héberge rarement leur cible finale. Ils cherchent à se déplacer latéralement au sein du réseau pour mettre la main sur les ressources informatiques les plus critiques (de niveau 0). Une fois cet objectif atteint, ils peuvent exfiltrer des données ou lancer des attaques de ransomwares.

Figure 2. Plate-forme Proofpoint Identity Threat Defense

Bon nombre de vulnérabilités liées aux identités découlent de procédures métier et opérationnelles informatiques ordinaires, telles que les suivantes :

- **Noms d'utilisateur et mots de passe.** Les applications des utilisateurs mettent souvent ces informations en cache sur les endpoints (navigateurs, SSH, FTP, PuTTY, bases de données, etc.). Les solutions PAM ne protègent pas ces identifiants de connexion.
- **Identifiants de connexion d'administrateurs de domaine.** Ces identifiants sont parfois conservés dans la mémoire système après une session de support à distance et sont souvent mis en cache dans un compte de service non protégé.
- **Privilèges fantômes.** La configuration d'objets et de groupes d'annuaire d'identité dans Active Directory peut être très complexe. Par conséquent, certains utilisateurs peuvent se voir attribuer par inadvertance des privilèges fantômes excessifs.

Une visibilité complète sur la sécurité des identités

Les attaques réussies exploitent les failles dans la gestion et la protection. Notre plate-forme aide les responsables de la sécurité à identifier et à corriger ces failles. Voici ses atouts :

1. **Découverte.** Bénéficiez d'une visibilité continue sur les vulnérabilités liées aux identités couvrant AD, Entra ID, AWS Identity Center, Okta et les endpoints.
2. **Hiérarchisation et correction.** Obtenez une liste des vulnérabilités classées selon leur niveau de priorité. Ces risques apparaissent sur un spectre allant de « non critique » à « urgent ». Activez la correction automatisée des vulnérabilités liées aux identités directement depuis la plate-forme. Vous pouvez configurer des règles d'exception conformes à vos stratégies de sécurité.
3. **Détection et intervention.** Détectez quand des cybercriminels sont actifs dans votre environnement. Grâce aux leurres sans agent, vous pouvez détecter des activités telles que le Kerberoasting, la pulvérisation de mots de passe, l'utilisation abusive de comptes à privilèges et plus encore. Vous pouvez utiliser la collecte de données d'investigation numérique pour orienter la réponse de votre entreprise aux menaces actives.

EN SAVOIR PLUS

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

0213-003-03-04 6/24