Proofpoint Shadow

Bloquez les élévations de privilèges et les déplacements latéraux en temps réel

Principaux avantages

- Détection des cybercriminels à un stade précoce et investigations complètes sur les menaces
- Réduction des faux positifs dans le SOC grâce à des alertes fiables
- Technologie sans agent pour un déploiement aisé avec intervention limitée du service informatique
- Défense continue grâce à des ajustements automatiques au fur et à mesure de l'évolution de l'environnement informatique
- Mise à l'échelle éprouvée sur les réseaux comptant plus d'un million d'endpoints
- Élimination des failles laissées par la détection des menaces basée sur les signatures et les anomalies

Plus de 90 % des cyberattaques impliquent des identités à risque. Les cybercriminels ont adapté leurs stratégies et ciblent désormais des identités à privilèges au lieu d'essayer de compromettre directement des systèmes. Cette transition a entraîné une hausse des attaques de ransomwares réussies et des compromissions de données. En se concentrant sur les identités vulnérables, les cybercriminels peuvent réduire la durée d'implantation des attaques de plusieurs mois à quelques jours, voire quelques heures.

Proofpoint peut vous aider. Notre puissante solution Proofpoint Shadow transforme vos endpoints en réseau de leurres qui rendent presque impossible tout déplacement latéral des cybercriminels dans votre environnement sans être détectés. Composant de la plate-forme Proofpoint Identity Threat Defense, Proofpoint Shadow détecte les cybercriminels de manière déterministe en fonction de leurs interactions avec des voies d'attaque en apparence légitimes sur vos endpoints, mais qui sont en réalité des leurres que nous déployons.

Contrairement à d'autres outils, Proofpoint Shadow ne s'appuie pas sur des analyses basées sur des signatures ou des comportements. Il n'utilise pas non plus d'agents ni de honeypots susceptibles d'être exploités. À la place, l'architecture sans agent de Proofpoint Shadow permet aux leurres d'opérer dans l'ombre. Proofpoint Shadow a prouvé son efficacité dans plus de 160 exercices de simulation d'attaques avec certaines des principales entreprises de sécurité au monde, dont Microsoft, Mandiant, le ministère américain de la Défense et Cisco.

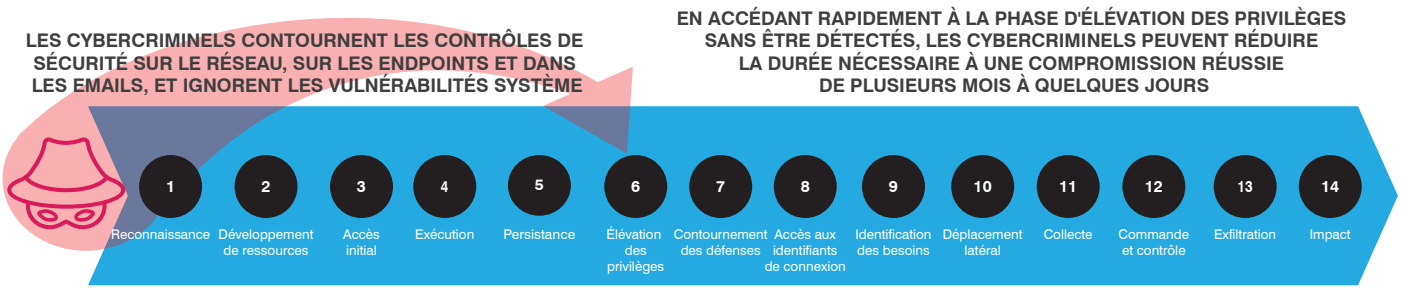

Figure 1. Les cybercriminels se concentrent désormais sur les identités vulnérables comme principale voie d'accès via la chaîne d'attaque.

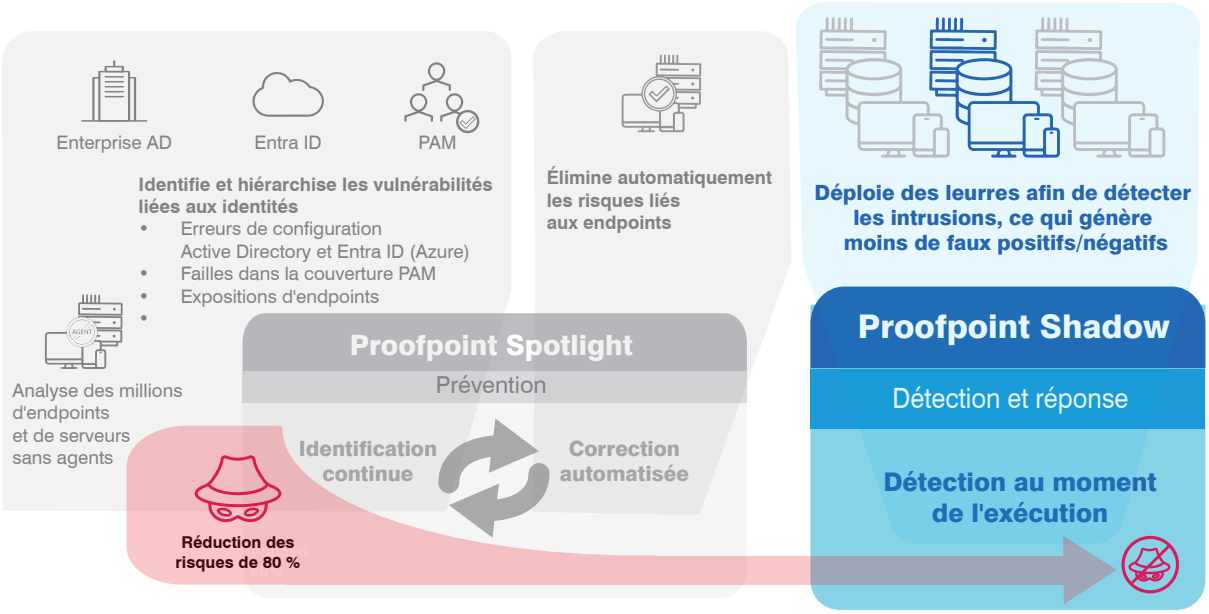

Figure 2. Composant de la plate-forme Proofpoint Identity Threat Defense, Proofpoint Shadow crée un réseau de leurres qui détectent et signalent tout déplacement latéral d'un cybercriminel sur vos réseaux.

Détection déterministe plutôt que probabiliste

Vous pouvez détecter et neutraliser les menaces de nombreuses manières. Par exemple, vous pouvez rechercher des schémas très spécifiques, ou signatures. Vous pouvez également analyser la façon dont un cybercriminel potentiel se comporte. Les outils conventionnels sont souvent incapables de détecter les attaques graves, par exemple lorsque des cybercriminels élèvent des privilèges ou se déplacent latéralement sur votre réseau sans être détectés. Ces échecs de détection peuvent permettre aux cyberpirates de prendre le contrôle de comptes, de distribuer des ransomwares ou de voler des données. Les équipes de sécurité ont besoin d'une approche plus avancée et plus fiable pour garder une longueur d'avance sur ces types d'attaques.

Proofpoint Shadow offre une approche déterministe. Il utilise des leurres largement distribués pour interagir activement avec les cybercriminels tout au long de la chaîne d'attaque et surveiller leurs activités. Ces leurres sont dissimulés en profondeur sur les endpoints de l'entreprise. Ils ressemblent à et se comportent comme des fichiers, sessions RDP, connexions de base de données, emails, scripts et autres ressources légitimes sur lesquels les cybercriminels souhaitent mettre la main. Lorsqu'un cybercriminel interagit avec l'un d'entre eux, Proofpoint Shadow envoie à l'équipe de sécurité une alerte en temps réel contenant des données d'investigation numérique. L'équipe peut alors utiliser ces informations pour faire des choix intelligents afin de bloquer l'attaque et de protéger l'entreprise.

Détection et protection sans agent

L'approche binaire, unique et sans agent de Proofpoint Shadow aide à la fois les administrateurs informatiques et les équipes de sécurité. Basée sur une automatisation intelligente, la solution ne perturbe pas les activités afin de réduire l'impact sur l'architecture informatique. Contrairement aux outils de sécurité qui s'appuient sur des agents logiciels, les cybercriminels ne peuvent pas désactiver ou contourner Proofpoint Shadow.

Plus de 75 techniques de leurre

Proofpoint Shadow emploie plus de 75 techniques de leurre actif. Il crée de faux fichiers et partages de fichiers, connexions de base de données, connexions FTP et RDP/SSH, historiques de navigateur et URL, identifiants de connexion Windows, sessions réseau, emails, scripts et même discussions Teams historiques qui servent de fils-pièges dissimulés ayant en apparence une grande valeur pour les cybercriminels. Ensemble, ces techniques permettent de prendre les cyberpirates sur le fait, peu importe où commence la compromission — à l'intérieur ou à l'extérieur de l'environnement.

Avec Proofpoint Shadow, les équipes de sécurité peuvent automatiser la création de centaines de faux fichiers Word et Excel personnalisés qui ressemblent à des vrais. Elles peuvent même inclure le logo et l'en-tête de votre entreprise. Les fausses données incorporées dans les documents déclenchent des alertes envoyées aux administrateurs de sécurité si un cybercriminel tente de les utiliser pour obtenir un accès plus étendu.

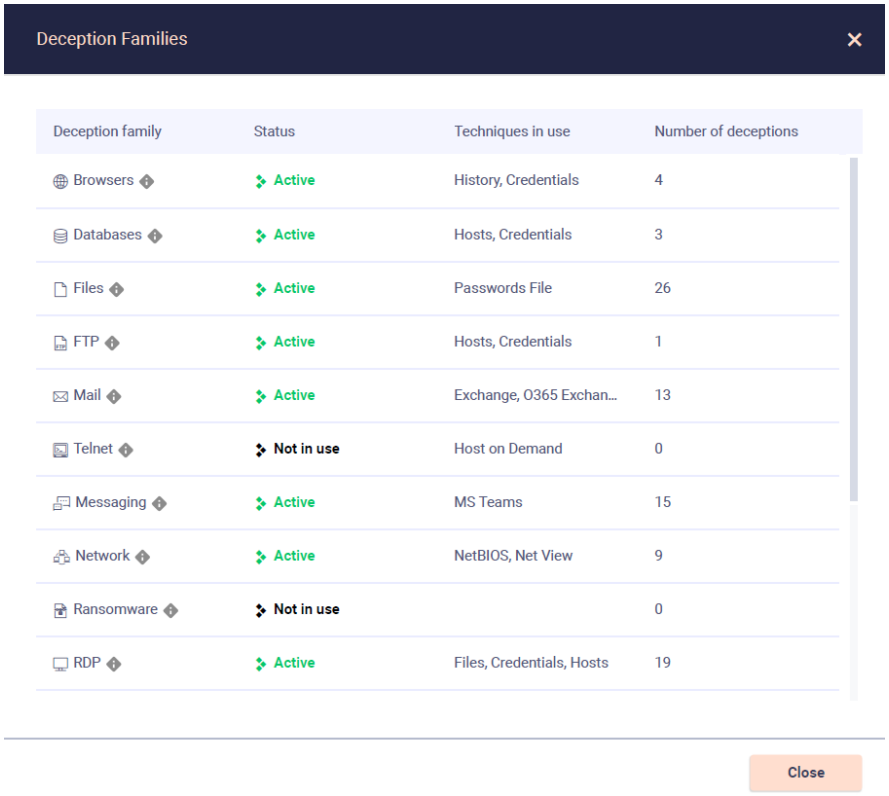

Figure 3. L'interface utilisateur de Proofpoint Shadow

Des leurres automatisés et personnalisés pour chaque endpoint

Le système d'automatisation intelligent de Proofpoint Shadow crée des leurres réalistes et convaincants pour les cybercriminels. Il peut facilement évoluer et s'adapter sans alourdir la charge de travail de l'équipe de sécurité. Proofpoint Shadow analyse le paysage des endpoints, conçoit des leurres personnalisés pour chaque machine et les déploie en un seul clic. La solution se charge également du processus continu d'ajustement et de gestion des leurres au fil du temps.

Point de vue des cybercriminels

La console de gestion de Proofpoint Shadow regorge de données d'investigation numérique sur les activités des cybercriminels. Elle fournit aux équipes de sécurité des données importantes sur la progression des cyberpirates vers vos ressources stratégiques. Elle peut également afficher une chronologie complète de leurs activités une fois que les leurres sont activés. Enfin, elle peut montrer aux analystes de sécurité à quoi ressemblent les leurres du point de vue des cybercriminels.

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**.