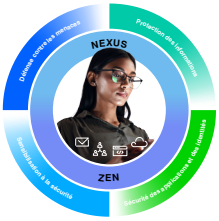
Proofpoint Account Takeover Protection

Détectez et neutralisez les prises de contrôle de comptes cloud

Principaux avantages

- Détection des comptes Microsoft 365, Google Workspace et Okta compromis
- Protection contre les prises de contrôle de comptes qui contournent la MFA
- Accélération des investigations grâce à une vue centralisée des activités postérieures à la prise de contrôle des comptes
- Réduction de la durée d'implantation des cybercriminels grâce à la suspension des comptes et à la réinitialisation forcée des mots de passe
- Annulation des modifications malveillantes apportées aux règles de la boîte email et aux paramètres MFA
- Suppression des applications tierces suspectes

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.



Proofpoint Account Takeover Protection (ATO Protection) étend les capacités de Proofpoint Targeted Attack Protection (TAP) pour détecter les comptes cloud compromis et protéger vos environnements cloud.

Proofpoint ATO Protection étend les capacités de Proofpoint Targeted Attack Protection (TAP) pour détecter et sécuriser les comptes cloud compromis. Proofpoint ATO Protection s'appuie sur l'intelligence artificielle (IA), des informations de threat intelligence mises en corrélation et l'analyse comportementale pour détecter les activités suspectes à toutes les étapes de la chaîne d'attaque. Il détecte les modifications apportées par les cybercriminels après la compromission et révoque leur accès. Il annule les modifications malveillantes apportées aux règles de la boîte email et aux paramètres de l'authentification multifacteur (MFA). Il supprime également les applications tierces suspectes, et met en quarantaine et supprime les fichiers suspects.

Proofpoint ATO Protection fournit des rapports détaillés qui répertorient les connexions suspectes, les utilisateurs attaqués et les systèmes et paramètres affectés. L'intégration avec Proofpoint Identity Threat Defense vous montre l'impact potentiel d'une prise de contrôle de comptes sur d'autres comptes et hôtes en un seul clic. Ces informations vous aident à bloquer les attaques avant qu'elles ne deviennent des compromissions plus graves susceptibles de mettre en péril votre entreprise.

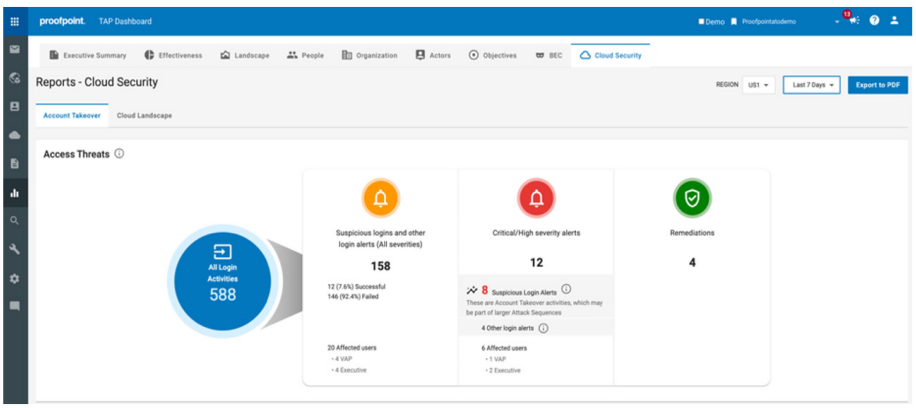


Figure 1. Proofpoint ATO Protection détecte les connexions suspectes, vous fournit des informations détaillées afin de vous aider à enquêter sur les menaces et annule les modifications malveillantes.

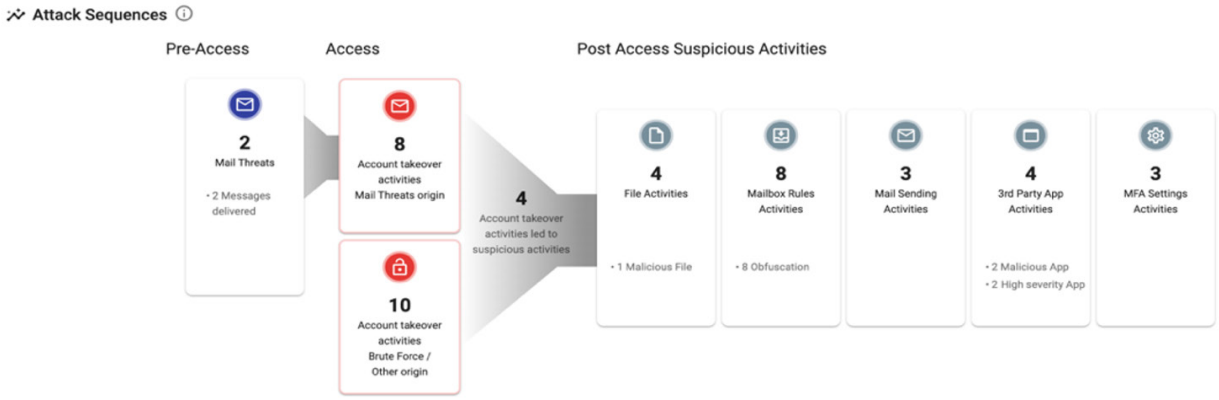


Figure 2. Le rapport Attack Sequence (Séquence d'attaque) affiche les activités de menace antérieures et postérieures à l'accès pour les comptes affectés.

Amélioration de la détection et de la visibilité

Proofpoint ATO Protection détecte les comptes compromis, les emails suspects et autres activités malveillantes dans vos environnements cloud. Il s'appuie sur la threat intelligence provenant de plus de 40 millions d'utilisateurs suivis dans des milliers d'entreprises. Il combine ces informations à l'IA et à l'analyse comportementale pour détecter toute activité inhabituelle dans votre environnement. Cette combinaison de techniques réduit les faux positifs. Vous bénéficiez d'une détection précise et d'une vue claire de toutes les activités dans vos comptes attaqués.

En cas de prise de contrôle d'un compte, Proofpoint ATO Protection ajoute des alertes au tableau de bord TAP. Une vue chronologique montre les activités de prise de contrôle de comptes, les activités au niveau des fichiers et des emails, les modifications apportées aux règles de la boîte email et aux paramètres MFA, ainsi que l'ajout d'applications tierces.

Accélération des investigations

Proofpoint ATO Protection indique à vos analystes en sécurité la cause d'une prise de contrôle de comptes et leur explique comment limiter les risques. Ces informations sont intégrées au système et au processus d'investigation TAP. Vous obtenez ainsi des informations qui complètent celles fournies par Proofpoint TAP. Une vue chronologique vous montre par ailleurs les comptes compromis et vous permet de cliquer sur chaque événement afin d'enquêter sur celui-ci.

Vous pouvez voir de quelle manière un compte a été attaqué ainsi que l'emplacement du cybercriminel. Vous pouvez également identifier les utilisateurs qui ont été victimes de menaces similaires. Des analyses avancées fournissent des vues chronologiques détaillées des activités des utilisateurs, des adresses IP, des domaines et d'autres attributs. Ces données enrichies vous aident à évaluer les risques qui pèsent sur votre entreprise.

Automatisation de la réponse

Proofpoint ATO Protection détecte et annule les modifications malveillantes apportées aux règles de la boîte email et aux paramètres MFA. Les cybercriminels modifient souvent les règles de la boîte email pour dissimuler leur présence dans votre système et le surveiller avant de lancer une attaque de phishing interne ou d'exécuter d'autres étapes de l'attaque. Proofpoint ATO Protection supprime également les applications tierces malveillantes. Toutes ces actions limitent les dégâts pour votre entreprise et réduisent le temps nécessaire pour enquêter sur les menaces et les neutraliser. Si vos investigations révèlent d'autres activités malveillantes, vous pouvez corriger les comptes compromis. Vous pouvez également supprimer les fichiers que les cybercriminels ont ajoutés au compte d'un utilisateur.

Proofpoint Account Takeover Protection était précédemment connu sous le nom de Proofpoint TAP Account Takover.

EN SAVOIR PLUS

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