Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (CAD) protège les utilisateurs de Microsoft 365 et Google Workspace contre les compromissions de comptes cloud. Proofpoint CAD vous permet de détecter les comptes compromis, de mener des investigations et de vous défendre contre les cybercriminels qui accèdent à vos données sensibles et à vos comptes approuvés. Nos puissantes fonctionnalités d'investigation numérique et nos contrôles basés sur des règles vous permettent d'assurer une surveillance continue et de neutraliser les menaces en fonction des facteurs de risque les plus importants pour vous.

PRINCIPAUX AVANTAGES

- Identification des principaux utilisateurs à risque et surveillance des incidents via des tableaux de bord détaillés
- Personnalisation et hiérarchisation des alertes en fonction des facteurs de risque les plus importants pour vous
- Mise en corrélation des menaces dans l'environnement de messagerie et le cloud pour détecter avec précision les comptes compromis
- Enquête sur les incidents de sécurité grâce à des fonctionnalités d'investigation numérique avancées et à des rapports personnalisables
- Blocage des accès non autorisés aux applications et services cloud grâce à des contrôles d'accès adaptatifs
- Automatisation des mesures de réponse aux incidents de sécurité grâce à des contrôles basés sur des règles flexibles
- Déploiement rapide dans le cloud
- Support client primé

Les identifiants de connexion des utilisateurs représentent la clé de votre royaume (votre entreprise). Si des cybercriminels parviennent à compromettre les identifiants de vos comptes Microsoft 365 ou Google Workspace, ils pourront lancer des attaques à l'intérieur et à l'extérieur de votre entreprise. Ils pourront convaincre les utilisateurs de transférer de l'argent ou des données sensibles. Ils pourront en outre accéder à vos données critiques, telles que votre capital intellectuel ou vos données clients, ce qui risque de mettre à mal votre réputation et vos finances. Par ailleurs, une fois que les attaquants ont un pied dans votre entreprise, ils installent souvent des portes dérobées (backdoors) pour maintenir l'accès en prévision de futures attaques. Bien que les cybercriminels aient le plus souvent recours au phishing pour compromettre les comptes, ils emploient également les moyens suivants :

- Attaques par force brute qui automatisent la recherche systématique d'identifiants de connexion
- Recyclage d'identifiants de connexion, également appelé « credential stuffing », qui utilise des paires de nom d'utilisateur et mot de passe volés précédemment
- Malwares, tels que les enregistreurs de frappe et les voleurs d'identifiants de connexion

Notre approche intégrée centrée sur les personnes, qui met en corrélation les activités liées aux menaces dans l'environnement de messagerie et le cloud, offre une protection efficace contre la compromission des comptes cloud. Nous associons des analyses basées sur l'accès au cloud et le comportement des utilisateurs à notre threat intelligence sur les menaces transmises par email. Vous pouvez ainsi identifier les utilisateurs à risque et détecter les comptes compromis.

Nous empêchons également tout accès non autorisé grâce à des contrôles adaptatifs de l'accès aux applications et services cloud approuvés par le département informatique. Nos règles centrées sur les personnes vous signalent les problèmes en temps réel et, si nécessaire, appliquent des contrôles basés sur le niveau de risque, tels que la mise en œuvre d'un réseau privé virtuel ou l'authentification à plusieurs facteurs.

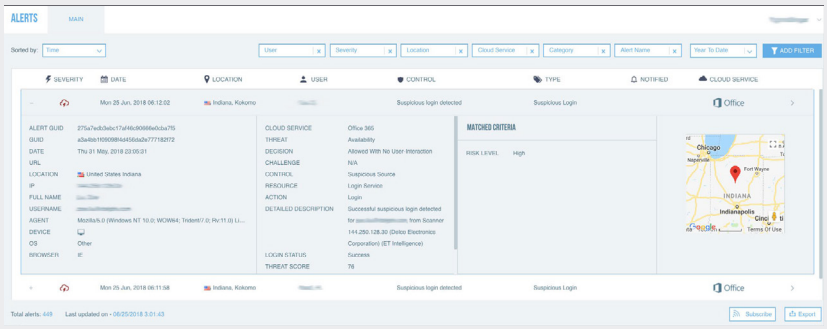
Détection des comptes compromis

Proofpoint CAD procure une visibilité sur les menaces liées au cloud et à la messagerie électronique. Nous vous aidons à différents égards :

- Identification de vos VAP (Very Attacked People™, ou personnes très attaquées) et protection de leurs comptes cloud
- Détection des compromissions grâce à des données contextuelles telles que l'emplacement des utilisateurs, le terminal utilisé, le réseau et l'heure de connexion
- Établissement de comportements de base sûrs grâce à l'analyse
- Identification des anomalies grâce à des empreintes capturées précédemment, à des seuils d'alerte et à des fonctionnalités avancées d'apprentissage automatique, et recherche d'activités suspectes telles que des tentatives de connexion excessives et inhabituelles, comme les comportements indiquant la force brute et les événements de type « too-fast-to-travel » (incohérence de localisation)

Proofpoint CAD combine également une threat intelligence multivectorielle complète, fournie par le graphique des menaces Nexus de Proofpoint, à des indicateurs de risque propres à l'utilisateur. Vous avez ainsi la possibilité de détecter les connexions à partir de sources suspectes.

Par ailleurs, nous effectuons des contrôles de réputation des adresses IP à l'aide de notre threat intelligence mondiale. Nous mettons également en corrélation les activités liées aux menaces dans l'environnement de messagerie et le cloud. Qui plus est, notre threat intelligence sur les menaces transmises par email permet d'identifier les liens entre les attaques par phishing d'identifiants de connexion et les connexions suspectes. Les cybercriminels peuvent utiliser un compte compromis pour lancer une attaque de phishing et compromettre d'autres utilisateurs au sein de votre entreprise.



Pour identifier les autres comptes compromis, nous étudions l'empreinte de l'auteur de l'attaque afin d'identifier les en-têtes User-Agent et activités inhabituels, notamment les redirections d'email.

Investigations numériques granulaires

Lorsqu'un incident se produit, vous pouvez enquêter sur les activités et alertes antérieures à l'aide de notre tableau de bord intuitif. Vous pouvez y consulter des données d'investigation numérique granulaires sur les transactions, notamment l'utilisateur, la date, l'heure, l'adresse IP, le terminal, le navigateur, l'en-tête Agent-Utilisateur, l'emplacement, la menace, le score de menace et bien d'autres. Vous pouvez également visualiser et analyser ces données à l'aide de graphiques et rapports de journaux détaillés. Vous pouvez en outre trier ou filtrer les activités et les journaux d'alerte afin de personnaliser vos rapports d'enquête. Par ailleurs, vous pouvez vous abonner à des rapports quotidiens, hebdomadaires ou mensuels. Pour une analyse plus poussée, les données d'investigation numérique peuvent être exportées manuellement ou via une intégration SIEM, prise en charge par des API REST.

Protection des comptes Microsoft 365 et Google Workspace grâce à des règles flexibles

Les informations fournies par nos données d'investigation numérique détaillées vous permettent de créer des règles de remédiation flexibles, fondées sur un large éventail de paramètres, tels que l'utilisateur, l'emplacement, le réseau, le terminal, l'activité suspecte, etc. Vous pouvez par exemple générer des alertes de connexion pour les pays figurant sur votre liste noire ou pour les terminaux qui ne respectent pas les directives de votre entreprise. Par ailleurs, lorsque vous surveillez un service à forte utilisation comme Microsoft 365 ou Google Workspace, vous devez hiérarchiser les alertes afin d'éviter une baisse de la vigilance due à un volume élevé d'alertes. Proofpoint CAD vous permet de générer des notifications d'alerte en fonction de leur gravité. Vous pouvez personnaliser chaque notification ou utiliser le modèle par défaut. Vous pouvez en outre surveiller plus étroitement les utilisateurs à risque ou les suspendre si une connexion suspecte réussit.

Les contrôles d'accès adaptatifs de Proofpoint CAD permettent la mise en place en temps réel de mesures de sécurité centrées sur les personnes, en fonction du rôle, du contexte et du niveau de risque. Les tentatives d'accès à partir de sites et de réseaux à risque ou par des cybercriminels connus sont ainsi automatiquement bloquées. Qui plus est, vous pouvez appliquer aux VAP et utilisateurs à privilèges des contrôles basés sur les risques, notamment l'authentification renforcée et la mise en œuvre de réseaux privés virtuels (VPN).

Déploiement rapide dans le cloud

Les plates-formes cloud nécessitent une protection hébergée dans le cloud. Notre architecture cloud et notre protection basée sur des API Microsoft 365 ou Google Workspace permettent un déploiement rapide et offrent une rentabilité immédiate.

Lors de l'implémentation de contrôles d'accès adaptatifs, vous pouvez rediriger vos connexions aux applications cloud vers notre passerelle d'authentification SAML (Security Assertion Markup Language). Cette passerelle applique un processus d'authentification fédérée en faisant office d'interface entre chaque fournisseur de services et le fournisseur d'identité. Proofpoint CAD prend en charge n'importe quel service cloud approuvé par le département informatique et fédéré via SAML 2.0. En outre, pour l'authentification forte, vous pouvez intégrer votre solution d'authentification à plusieurs facteurs ou utiliser notre application d'authentification mobile, Proofpoint Mobile Access, fournie avec Proofpoint CAD. Vous n'aurez pas à attendre des semaines, voire des mois, puisque quelques jours suffisent pour protéger des centaines de milliers d'utilisateurs.

En tant que leader du marché de la protection contre les menaces, nous utilisons le cloud pour mettre quotidiennement à jour notre logiciel afin de vous aider à garder une longueur d'avance sur les cybercriminels. Notre déploiement dans le cloud vous offre également la flexibilité nécessaire pour protéger les utilisateurs sur n'importe quel réseau ou terminal.

EN SAVOIR PLUS

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

À PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité 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 plus de la moitié des entreprises de l'index Fortune 1000, 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**.