proofpoint

FICHE SOLUTION

Proofpoint Supplier Threat Protection

Détectez et bloquez les menaces provenant de comptes fournisseurs compromis avant qu'elles ne causent des dommages

Principaux atouts

- **Automatisation de la découverte et de la surveillance des communications avec les fournisseurs**
- **Détection et blocage proactifs des menaces provenant de comptes fournisseurs compromis**
- **Accompagnement des utilisateurs afin qu'ils fassent des choix plus sûrs grâce à des contrôles adaptatifs**
- **Accélération de la réponse aux risques en cartographiant les compromissions de fournisseurs par rapport aux voies d'attaque sur l'ensemble des canaux**

Présentation

Alors que les entreprises adoptent les environnements de travail agentiques, les relations avec les fournisseurs s'étendent désormais au-delà de la messagerie électronique pour inclure des outils de collaboration et d'autres solutions. Cet écosystème étendu a créé de nouvelles opportunités pour les cybercriminels d'exploiter des comptes tiers et fournisseurs qui ont été piratés. Avec ces attaques, les cybercriminels profitent de la confiance des utilisateurs pour lancer des fraudes multicanales visant la chaîne logistique, voler des identifiants de connexion et exfiltrer des données. Étant donné que les messages sont envoyés à partir de comptes légitimes, ces menaces contournent souvent les défenses basées sur le domaine et l'authentification.

Proofpoint Supplier Threat Protection, inclus dans Proofpoint Collaboration Security Prime, vous offre une visibilité continue sur la compromission des comptes fournisseurs et vous défend activement contre les attaques de la chaîne logistique. Optimisé par Proofpoint Nexus™ AI et notre threat intelligence mondiale, il apprend vos schémas de communication normaux avec les fournisseurs. De ce fait, il peut signaler des changements subtils dans le comportement des utilisateurs, même lorsque les messages proviennent de domaines légitimes et authentifiés.

Les équipes de sécurité peuvent également tracer les compromissions de fournisseurs sur tous les canaux et étapes d'attaque pour trouver rapidement les menaces les plus urgentes et les contenir. Non seulement cela réduit votre exposition aux compromissions de la chaîne logistique, mais cela vous aide également à conserver des relations de confiance avec vos partenaires.

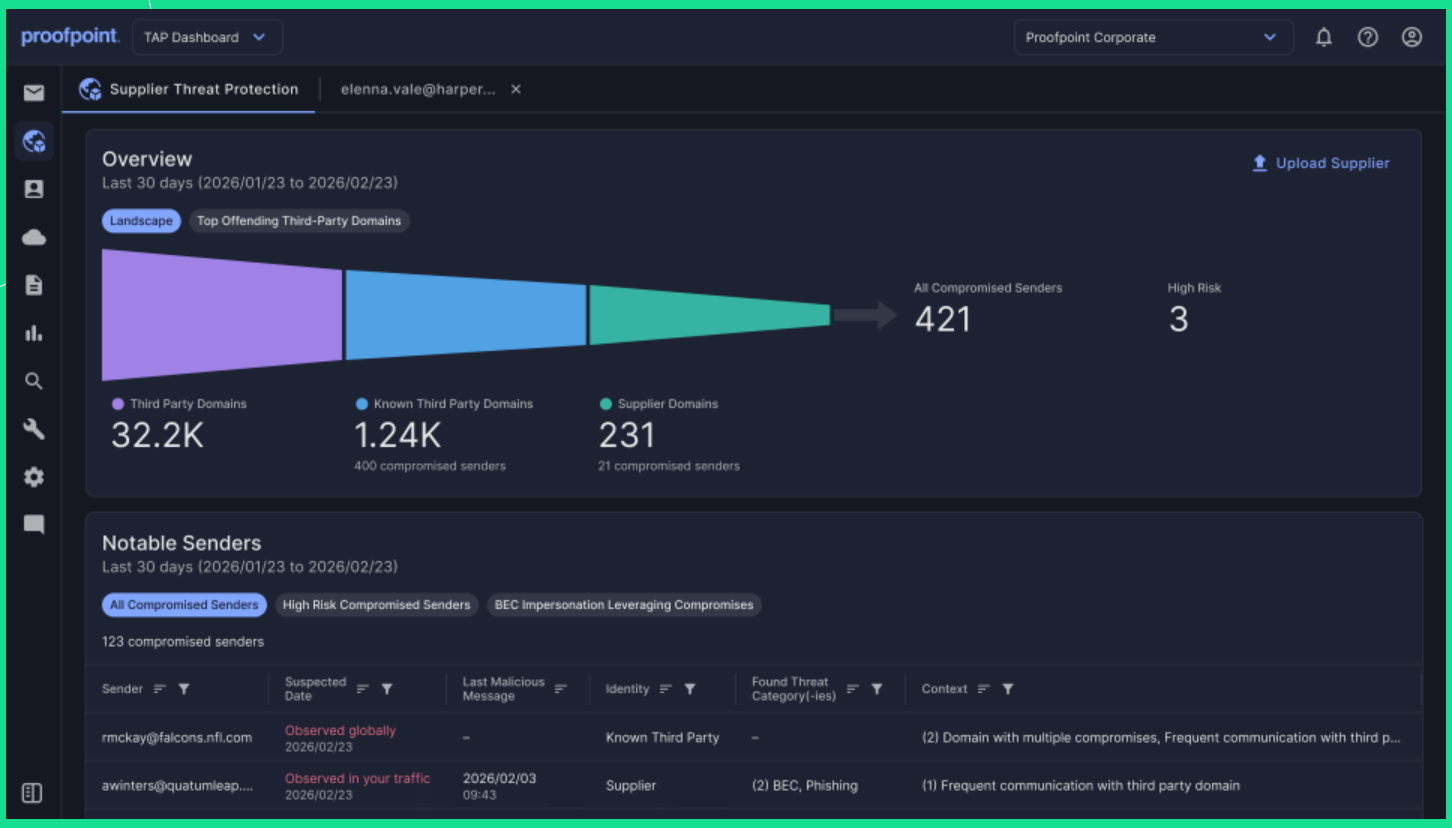

Figure 1. Proofpoint détecte les comptes fournisseurs susceptibles d'avoir été compromis et fournit des informations contextuelles pertinentes et une protection de la messagerie.

Protection complète contre les attaques provenant de fournisseurs

Proofpoint prévient les attaques provenant de fournisseurs avec une défense multicouche pilotée par l'IA. Les emails de fournisseurs malveillants sont bloqués avant qu'ils n'atteignent les utilisateurs, avec une précision de détection de 99,999 %. En parallèle, l'IA comportementale surveille les relations avec les fournisseurs de confiance pour détecter les signes subtils de compromission, même au niveau de domaines légitimes et authentifiés. Cela signifie que les cybercriminels ne peuvent pas se cacher derrière un compte de confiance pour outrepasser vos défenses.

Lorsqu'un message est suspect mais pas ouvertement malveillant, Proofpoint ajoute des mesures de protection adaptatives telles que l'affichage d'avertissements et l'isolation du navigateur. Cela permet aux utilisateurs de faire des choix plus sûrs sans perturber les messages professionnels légitimes. Les liens suspects sont automatiquement isolés ou bloqués même si quelqu'un clique dessus. En combinant le blocage avant la remise avec des protections intelligentes et instantanées des utilisateurs, Proofpoint offre une véritable défense en profondeur tout au long du cycle de vie des attaques provenant de fournisseurs.

Visibilité étende sur votre écosystème de fournisseurs

Proofpoint offre aux équipes de sécurité une visibilité approfondie et continue sur les risques liés aux fournisseurs dans l'ensemble de votre écosystème tiers. Vous pouvez ainsi gérer les risques liés à la chaîne logistique de manière proactive au lieu de gérer les incidents après qu'ils se sont produits. Vous obtenez une image claire de chaque domaine fournisseur qui communique avec votre entreprise. Cela inclut les fournisseurs actifs, les tiers nouvellement observés et les domaines précédemment associés à une compromission. Le résultat ? Une carte vivante de votre exposition aux fournisseurs.

Proofpoint va au-delà du signalement des emails malveillants. Vous obtenez également un contexte important afin de comprendre comment les fournisseurs interagissent avec votre entreprise. Vous pouvez voir les échanges financiers tels que la facturation, les destinataires inhabituels, les changements dans les schémas de communication et les thèmes suspects.

Proofpoint Nexus analyse plus de 2 100 milliards d'emails de plus de 2,8 millions de clients afin d'identifier les comptes fournisseurs compromis partout dans l'écosystème, souvent avant que ces comptes ne vous ciblent. Avec ce niveau de visibilité, vous pouvez étendre votre réseau de fournisseurs en toute confiance dans les environnements de travail agentiques modernes.

Investigations simplifiées pour une efficacité maximale

Proofpoint Supplier Threat Protection centralise la détection et la réponse aux compromissions de fournisseurs au sein de Proofpoint Collaboration Security Prime. Cela permet aux équipes de sécurité de réduire à la fois le volume d'incidents et le temps nécessaire pour mener des investigations. Les emails de fournisseurs malveillants sont bloqués avant la remise et les messages à risque élevé bénéficient de l'affichage d'avertissements et de l'isolation du navigateur. Ainsi, moins d'incidents parviennent aux analystes et moins d'événements liés aux fournisseurs nécessitent un examen manuel. Avec un tri moins routinier à gérer, les équipes de sécurité peuvent se concentrer sur les risques qui comptent le plus.

Lorsqu'un incident se produit, tout ce dont votre équipe a besoin pour mener des investigations est réuni au même endroit. L'activité des fournisseurs est automatiquement liée aux emails, au cloud et aux signaux de prise de contrôle de comptes connexes. Votre équipe peut instantanément voir si le problème est isolé ou s'il fait partie d'une attaque plus étendue en plusieurs étapes. Proofpoint Prime Threat Protection Workbench cartographie visuellement la façon dont une attaque se déplace sur différents canaux. Il est ainsi plus facile de comprendre l'impact et de prioriser la réponse en un coup d'œil.

Les équipes peuvent consulter un historique détaillé des communications et le contexte comportemental, ainsi que prendre des mesures d'application, le tout depuis une console unique. Elles n'ont donc pas besoin de jongler entre plusieurs outils, ce qui accélère le confinement. Cela signifie également que vous pouvez partager des preuves claires avec les fournisseurs concernés pour coordonner les correctifs, prévenir les incidents répétés et renforcer vos relations professionnelles.

En savoir plus

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

proofpoint.