

PROOFPOINT BROWSER ISOLATION

PROTÉGEZ LES UTILISATEURS CONTRE LES ATTAQUES AVANCÉES QUI CIBLENT LES ENVIRONNEMENTS PRIVÉS ET D'ENTREPRISE

PRINCIPAUX AVANTAGES

- Isolement des URL malveillantes dans les e-mails d'entreprise grâce à un contrôle adaptatif s'appuyant sur une analyse des risques
- Isolement du navigateur pour l'utilisation du Web à haut risque (domaines nouveaux ou inconnus)
- Prévention du « moissonnage » et du vol d'identifiants de connexion
- Déploiement simple et rapide depuis le cloud, sans matériel ni agent sur les terminaux
- Protection du personnel sans perturber l'expérience de navigation
- Simplification de la conformité au RGPD de l'Union européenne

Protéger vos collaborateurs contre les attaques de phishing ciblées et le vol d'identifiants de connexion exige des efforts constants. De plus, les cybercriminels gagnent du terrain en utilisant des URL malveillantes dans le cadre de campagnes à grande échelle. Comment se protéger contre ces menaces qui prolifèrent ? Avec Proofpoint Browser Isolation, vos collaborateurs peuvent accéder à Internet en toute sécurité, tout en bénéficiant d'une protection efficace contre les malwares et les fuites de données.

DESCRIPTION DU PRODUIT

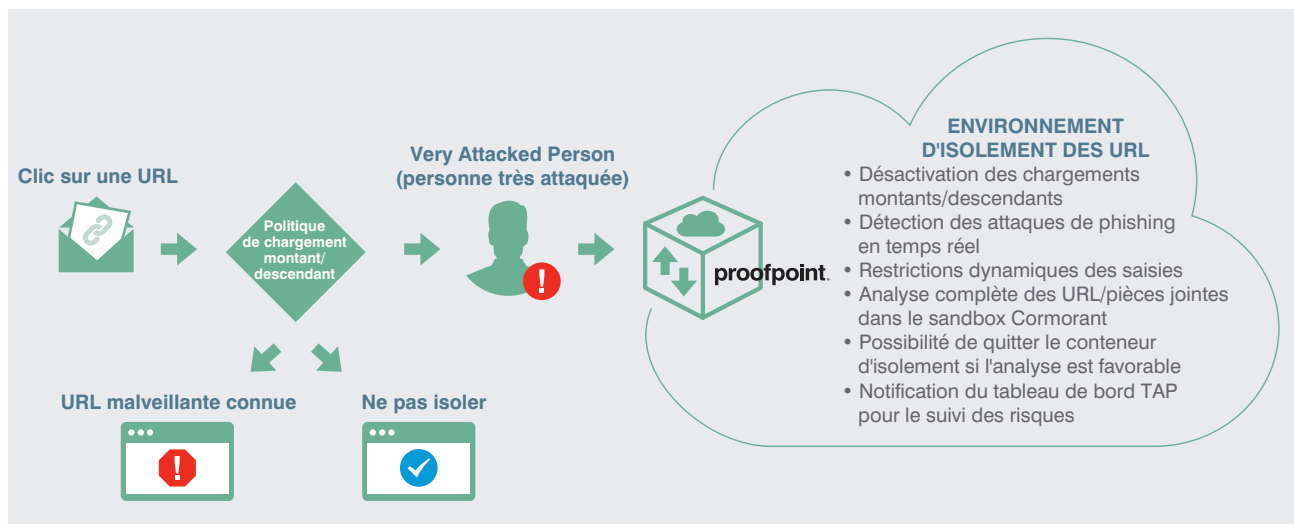
Proofpoint Browser Isolation permet à vos utilisateurs d'accéder en toute sécurité à des sites Web, ainsi qu'à leur messagerie personnelle et d'entreprise. Pour ce faire, il isole les sessions de navigateur dans un conteneur sécurisé. Cette solution unique vous protège contre les malwares et le contenu malveillant. Elle désactive les téléchargements montants et descendants, et empêche les vols ou les fuites de données sensibles. Proofpoint Browser Isolation contribue à résoudre les problèmes de sécurité, de productivité et de confidentialité, liés aux attaques de phishing et à l'accès aux sites Web à haut risque. Qui plus est, son déploiement, son administration et sa prise en charge sont d'une grande simplicité.

FONCTIONNALITÉS ET AVANTAGES

Adaptation de la sécurité aux URL à haut risque et aux utilisateurs fréquemment ciblés

De nos jours, les cybercriminels ciblent des individus précis de votre entreprise à l'aide d'e-mails de phishing. Vous avez donc besoin de contrôles adaptatifs supplémentaires pour protéger vos collaborateurs les plus exposés. Proofpoint Browser Isolation protège vos utilisateurs contre le contenu Web malveillant présent dans les e-mails d'entreprise. Il isole les sessions de navigateur selon les règles définies afin de bloquer les URL à haut risque, notamment les URL inconnues, les réseaux sociaux et les applications cloud.

L'intégration avec Proofpoint Targeted Attack Protection (TAP) permet aux clients TAP d'utiliser Browser Isolation pour protéger la messagerie d'entreprise. Combinés à TAP, les contrôles centrés sur les personnes constituent un moyen très efficace de réduire les risques. Ainsi, vous pouvez choisir les utilisateurs auxquels s'appliquera l'environnement d'isolement en fonction des facteurs de risque liés à la messagerie d'entreprise. L'intégration à TAP assure la détection et l'analyse en temps réel des tentatives de phishing. Les sessions de navigateur isolées sont signalées et incorporées au tableau de bord TAP, afin que vous puissiez disposer d'une visibilité optimale et surveiller le niveau de risque.



Réduction de la surface d'exposition aux attaques

Comme de nombreuses entreprises, vous autorisez vos collaborateurs à consulter Internet ou leur messagerie Web personnelle sur le lieu de travail. Les cybercriminels le savent et en tirent profit pour lancer des attaques sophistiquées. De fait, des études révèlent que jusqu'à 60 % des attaques ont pour origine l'utilisation du Web ou de la messagerie privée sur des appareils d'entreprise. Comment réduire le risque tout en accordant à vos collaborateurs la liberté de naviguer sur Internet et d'accéder à leurs e-mails personnels ?

Grâce à Proofpoint Browser Isolation, vous pouvez choisir d'isoler certains sites Web ou applications cloud. Vos collaborateurs peuvent ainsi naviguer sur Internet ou accéder à leur messagerie Web personnelle en toute sécurité, tandis que vous renforcez la sécurité de votre entreprise. Ces actions n'entraînent aucun risque pour les ressources d'entreprise. L'inspection des fichiers et le suivi du comportement des utilisateurs sont inutiles. En outre, les fichiers ou les pièces jointes contenant des virus ou des macros malveillantes ne sont jamais téléchargés. La solution isole même le contenu de sites approuvés qui ont été compromis. Cette approche vous protège contre les attaques de type « watering hole » et les liens dans les e-mails conduisant à des applications cloud rendues dangereuses, telles que Microsoft SharePoint, Dropbox, etc. Grâce aux restrictions dynamiques de saisie, le vol d'identifiants de connexion recourant aux navigateurs est lui aussi limité. De plus, Proofpoint Browser Isolation empêche les téléchargements à l'insu de l'utilisateur et empêche vos terminaux d'accéder à bien d'autres contenus Web malveillants.

Réduction de la charge de travail de l'équipe informatique

Autoriser vos collaborateurs à accéder à des URL inconnues ou non catégorisées et à leurs e-mails personnels vous pose un réel souci. Vous savez à quel point les risques sont grands. Cependant, vos collaborateurs ont souvent d'excellentes raisons de consulter ces sites. Avec la plupart des solutions, les équipes informatiques doivent décider si elles bloquent ou autorisent ces sites. Or, si tous ces domaines sont bloqués, elles seront inondées de demandes d'exception pour l'accès à des sites précis.

Proofpoint Browser Isolation offre une solution plus efficace. Il résout les problèmes de sécurité, de productivité et de confidentialité liés à l'utilisation du Web par les collaborateurs. Il isole les sessions de navigation dans un conteneur sécurisé grâce auquel vos collaborateurs peuvent accéder librement à leur messagerie Web personnelle et à d'autres sites. L'équipe informatique en tire également avantage, puisqu'elle n'a plus à consacrer un temps précieux à définir des exceptions au cas par cas. Qui plus est, le déploiement, l'administration et la prise en charge de la solution sont d'une grande simplicité. L'amélioration de la productivité de l'équipe informatique qui en résulte est synonyme d'économies. En outre, une telle initiative contribue à instaurer un climat de confiance avec vos collaborateurs. Vous évitez par ailleurs les infractions à la conformité en conservant la messagerie Web dans la sphère privée. Proofpoint Browser Isolation est facile à déployer dans la mesure où il repose entièrement sur le cloud. Vous pouvez également l'intégrer à vos propres filtre Web, proxy, passerelle et pare-feu.

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 à Proofpoint pour diminuer leurs risques les plus critiques en matière de sécurité et de conformité via les e-mails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.