

FICHE SOLUTION

Microsoft et Proofpoint – unis pour protéger l'espace de travail moderne

Deux leaders de la cybersécurité. Une solution unique centrée sur les personnes et l'IA.



Principaux atouts

- Réduisez le risque de compromission des données
- Protégez les utilisateurs grâce à une sécurité multi-couche
- Unifiez la protection des données dans les applications Microsoft et tierces
- Améliorez la conformité et le contrôle des règles

Cette solution 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.

Introduction

Les cyberattaques se multiplient de manière exponentielle. Les avancées en matière d'IA permettent désormais aux cybercriminels de mener un nombre bien plus important de campagnes sans ressources supplémentaires. De plus, ces attaques peuvent être lancées presque sans effort à l'échelle mondiale.

En tant que plate-forme de productivité par défaut pour des entreprises de toutes tailles, Microsoft 365 est devenu une cible de choix pour ces attaques. Et même si Microsoft offre de solides défenses, même la cybersécurité la plus performante ne peut qu'être mise à rude épreuve face à ces assauts incessants. D'où l'importance d'évaluer les risques associés à un point de défaillance unique sur les canaux critiques, comme la messagerie électronique.

En combinant les défenses de Microsoft 365 et la plate-forme optimisée par Proofpoint Nexus™ AI, vous bénéficiez d'une protection résiliente contre les menaces à côté desquelles les solutions traditionnelles passent souvent. Ensemble, ces solutions protègent votre environnement contre le phishing, l'ingénierie sociale, les fuites de données et bien plus encore. Elles responsabilisent également vos collaborateurs et laissent plus de temps à vos équipes, qui peuvent ainsi se concentrer sur la croissance.

« Les acheteurs doivent envisager des solutions de protection de la messagerie électronique complémentaires ou supplémentaires pour respecter les bonnes pratiques en matière de lutte contre les menaces modernes véhiculées par email. »

GARTNER | [MAGIC QUADRANT POUR LA PROTECTION DE LA MESSAGERIE, T4 2025](#)

Les défis de sécurité de l'espace de travail moderne

L'email demeure le principal vecteur de menace initial pour les cyberattaques d'aujourd'hui. Ces dernières années, la surface d'attaque s'est toutefois élargie. Aujourd'hui, les collaborateurs travaillent dans Microsoft Teams, Slack, des applications cloud, des plates-formes de réseaux sociaux, des services de partage de fichiers et plus encore. Sans surprise, les cybercriminels développent de nouvelles tactiques pour exploiter ces canaux numériques.

De plus en plus, les cybercriminels utilisent les outils de collaboration pour contourner les contrôles de protection de la messagerie d'ancienne génération. Ils peuvent ainsi distribuer des liens malveillants, voler des identifiants de connexion et obtenir un accès non autorisé. Dans le même temps, ils utilisent les emails pour lancer des exploits tels que le phishing et le piratage de la messagerie en entreprise (BEC, Business Email Compromise). Ces tactiques continuent d'être à l'origine de la plupart des compromissions des données.

Face à la multiplication des menaces multicanales et en plusieurs phases, même les outils de sécurité les plus avancés peuvent avoir du mal à suivre le rythme. Il est en outre plus difficile que jamais pour les équipes d'obtenir une visibilité sur les attaques et de prendre le contrôle.

Les menaces ciblant les personnes dominant le paysage des menaces. Plus de 90 % des compromissions de données qui aboutissent débutent par la réception d'un email.

1. Internet Crime Complaint Center du FBI, *Internet Crime Report (IC3)*, 2024.

Comment Microsoft sécurise l'espace de travail

Microsoft 365 fournit une base de sécurité solide pilotée par l'IA à travers Defender et Purview. Ces deux solutions sont au cœur de son architecture de sécurité.

Defender

Defender propose une détection avancée optimisée par l'IA pour bloquer les menaces véhiculées par email. Il analyse les billions de signaux que Microsoft collecte quotidiennement – y compris le contenu des emails, le comportement des expéditeurs et les indicateurs contextuels – afin d'identifier les intentions malveillantes. Dans le cas de menaces BEC, Defender procède à une analyse des intentions et à une détection des anomalies comportementales. Les menaces basées sur des images, telles que le texte caché et les codes QR, sont détectées grâce à des capacités avancées d'analyse des images.

Purview

Purview offre une prévention des fuites de données (DLP) de haut niveau. Il contribue ainsi à réduire le risque de compromission de données et à garantir la conformité aux réglementations. La classification et l'étiquetage permettent aux entreprises d'appliquer des règles de sécurité des données de manière cohérente au niveau de la messagerie électronique, des endpoints et des applications cloud.

L'approche centrée sur les personnes de Proofpoint

Proofpoint propose une plate-forme complète et centrée sur les personnes, alimentée par ses moteurs Nexus AI. Vous bénéficiez ainsi de défenses résilientes qui se déploient en quelques minutes grâce à une simple intégration avec l'API Microsoft Graph.

Les modèles d'IA de Proofpoint sont entraînés avec l'un des ensembles de données les plus vastes et les plus diversifiés du secteur de la cybersécurité.

Proofpoint Collaboration Security Prime

Proofpoint Collaboration Security Prime offre une protection contre les menaces multicanales et en plusieurs phases, qui bloque les attaques centrées sur les personnes et les agents d'IA au niveau des emails, de la messagerie instantanée, des outils de collaboration, des applications cloud et des services de partage de fichiers. Il étend la sécurité de pointe de Proofpoint au-delà des emails pour sécuriser les interactions de confiance et intégrer la résilience humaine directement dans la plate-forme.

Grâce à des workflows automatisés et à une protection complète, Proofpoint Prime rationalise les opérations et renforce les défenses au sein des environnements de collaboration.

Prévention des fuites de données

Les solutions Proofpoint Data Loss Prevention (DLP) offrent une protection omnicanale centrée sur les personnes et conçue pour identifier et atténuer les risques de fuite de données par email, dans le cloud et via les endpoints. Proofpoint Enterprise DLP unifie les données télémétriques tirées des contenus, des comportements et des menaces pour traiter tout le spectre des scénarios de fuite de données centrés sur les personnes et empêcher la transmission non autorisée d'informations sensibles. Basée sur une architecture moderne et évolutive, la solution offre visibilité et contrôle sur les exfiltrations de données sans perturber les workflows des utilisateurs.

Plus de 2 millions d'entreprises de premier plan du monde entier sont protégées par Proofpoint.

Une alliance pour plus de sécurité : Proofpoint et Microsoft

La pile de sécurité intégrée de Microsoft, combinée à Proofpoint Collaboration Security Prime et à Proofpoint DLP, vous offre une protection contre les menaces multicanales et en plusieurs phases, ainsi qu'une protection des données centrée sur les personnes et omnicanale.

Ensemble, ces solutions unifient les données télémétriques des contenus, des comportements et des menaces provenant des emails, des outils de collaboration, des applications cloud et des endpoints. Ainsi, les équipes de sécurité bénéficient d'une visibilité et d'un contrôle sur l'espace de travail moderne sans perturber les workflows des utilisateurs.

Proofpoint Collaboration Security Prime ajoute une couche de protection supplémentaire à la détection des attaques BEC, du phishing, des malwares et des compromissions des fournisseurs par Microsoft Defender. Notre threat intelligence aide à détecter des attaques qui pourraient autrement passer inaperçues. De plus, Proofpoint offre une visibilité sur les VAP (Very Attacked People™, ou personnes très attaquées). Les utilisateurs les plus ciblés bénéficient ainsi d'une sécurité renforcée, une fonctionnalité qui n'est pas disponible de manière native dans Microsoft 365.

Proofpoint DLP fonctionne en tandem avec Microsoft Purview pour renforcer la protection des données au sein de l'espace de travail moderne. Purview propose une classification performante et des contrôles robustes des règles au sein de Microsoft 365, tandis que Proofpoint étend la visibilité unifiée aux emails, aux outils de collaboration, aux applications cloud et aux endpoints. En combinant la prise en compte du contenu et le contexte utilisateur, les entreprises bénéficient d'une gouvernance cohérente sur tous les canaux et d'une protection renforcée des informations sensibles.

Lorsque vous utilisez les solutions de sécurité de la collaboration et des données de Proofpoint, vous bénéficiez de deux couches supplémentaires de protection de classe mondiale.



Figure 1. Les couches de sécurité centrées sur les personnes de Proofpoint pour renforcer Microsoft 365

Des résultats concrets et une valeur ajoutée pour les clients

Les entreprises utilisent souvent les protections de Microsoft au niveau de la passerelle, et celles de Proofpoint pour la boîte email.

Les entreprises qui utilisent Proofpoint pour renforcer leur environnement Microsoft 365 constatent des améliorations mesurables de leur sécurité.

- Elles bloquent 27 % de menaces en plus.
- Le risque de subir une compromission majeure de données est réduit de 75 %.

Ces résultats ont un impact financier majeur. Ils se traduisent par une réduction des coûts de l'ordre de plusieurs millions, car les équipes consacrent moins de temps à la réponse aux incidents, la productivité des collaborateurs est préservée et l'entreprise évite des sanctions réglementaires coûteuses.

Exploitez le plein potentiel de la sécurité Microsoft 365. Découvrez comment Proofpoint étend et renforce votre protection.

www.proofpoint.com/fr/compare/proofpoint-and-microsoft

proofpoint®

À propos de Proofpoint, Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr.

Suivez-nous : LinkedIn _____

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques déposées contenues dans les présentes sont la propriété de leurs détenteurs respectifs.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →