proofpoint®

EBOOK

Proofpoint et Microsoft : une alliance pour plus de sécurité

Renforcez la sécurité de Microsoft 365 grâce à la détection avancée des menaces et au filtrage du spam et du graymail

Renforcement de la protection de votre environnement Microsoft 365

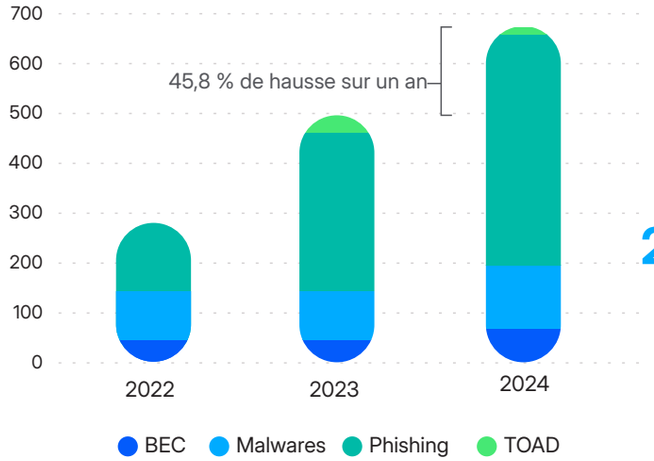
Peu importe si vous disposez de fonctionnalités de base de sécurité de la messagerie de Microsoft ou si vous avez effectué la mise à niveau vers Microsoft Defender for Office 365. Face à l'adoption massive de Microsoft 365 comme plate-forme professionnelle, les attaques vont se multiplier. L'email étant aujourd'hui le point de départ d'un grand nombre de cyberattaques, le renforcement de la sécurité de votre messagerie Microsoft doit être une priorité absolue.

Si ces tendances sont aussi alarmantes, c'est parce que les attaques véhiculées par email continuent de représenter une menace pour de nombreuses entreprises, même celles qui utilisent les défenses intégrées de Microsoft. Les évaluations de la sécurité de la messagerie réalisées par Proofpoint montrent que Microsoft peine encore à détecter les menaces avancées. Les entreprises restent donc exposées à des menaces telles que les suivantes :

- Phishing avancé
- Malwares
- Piratage de la messagerie en entreprise (BEC, Business Email Compromise)
- Codes QR
- URL malveillantes
- Attaques par téléphone (TOAD)

Protection ininterrompue contre les menaces en plein essor

Menaces avancées détectées par Proofpoint lors d'évaluations des menaces



3,88 % Pourcentage de menaces TOAD

63,19 % Pourcentage de menaces de phishing

23,88 % Pourcentage de menaces de malwares

9,05 % Pourcentage de menaces BEC

proofpoint.

Protection avancée contre les cyberattaques furtives

Phishing, URL malveillantes et malwares

Les cybercriminels continuent d'envoyer une avalanche de pièces jointes et de liens malveillants par email, que seules des fonctions avancées de protection de la messagerie sont à même de bloquer.

Proofpoint s'appuie sur un sandboxing prédictif, l'extraction des URL, la détection des contournements, l'isolation du navigateur et un large éventail d'autres techniques avancées pour offrir la défense la plus efficace possible contre ces charges virales malveillantes.

Protection contre les attaques BEC

Les attaques d'usurpation d'identité sans charge virale, telles que les attaques BEC, font partie des menaces plus difficiles à détecter, car ces emails ont souvent l'air légitimes.

Les moteurs Proofpoint NexusAI analysent les relations et le langage des utilisateurs tout en recherchant d'autres indicateurs de menaces potentielles. Les discordances au niveau des attributs d'en-tête, les boucles de rétroaction DMARC et le comportement de l'expéditeur fournissent des informations précieuses dont nous nous servons pour stopper net les menaces BEC.

Protection contre les attaques TOAD

Lors des attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery), également appelées phishing de rappel, les cybercriminels envoient des emails qui tentent de convaincre les destinataires d'appeler un faux centre d'appels.

Ces menaces peuvent être difficiles à détecter, car elles comportent rarement des charges virales malveillantes. Les moteurs Proofpoint NexusAI s'appuient sur l'apprentissage automatique et la vision par ordinateur pour rechercher des indicateurs de menaces connus afin de bloquer ces menaces (numéros de téléphone et codes QR malveillants, usurpations d'identité basées sur des images, etc.).

Une majorité écrasante des clients Microsoft qui souhaitent renforcer la sécurité de leur messagerie se tournent vers Proofpoint. 85 % des entreprises du classement Fortune 100 — et plus de 1,88 million de clients à travers le monde — nous ont choisis comme partenaire de sécurité privilégié.

Proofpoint est salué pour ses performances dans des rapports d'analyse tels que le Magic Quadrant de Gartner. Dans le dernier *rapport de Gartner sur les fonctionnalités essentielles des plates-formes de protection de la messagerie*, Proofpoint a obtenu la note la plus élevée dans quatre des cinq cas d'utilisation[1].

Proofpoint Core Email Protection bloque 99,99 % des menaces véhiculées par email, du spam et du graymail. Notre pile de détection multicouche Proofpoint Nexus combine graphiques relationnels, apprentissage automatique, vision par ordinateur et analyse sémantique. Elle est optimisée par des données sur les menaces issues de plus de 3 billions d'emails analysés chaque année. Elle peut donc prévenir la plupart des menaces avancées actuelles, dont les suivantes :

- Attaques BEC
- Prise de contrôle de comptes
- Codes QR malveillants
- Usurpation d'identité
- Phishing latéral

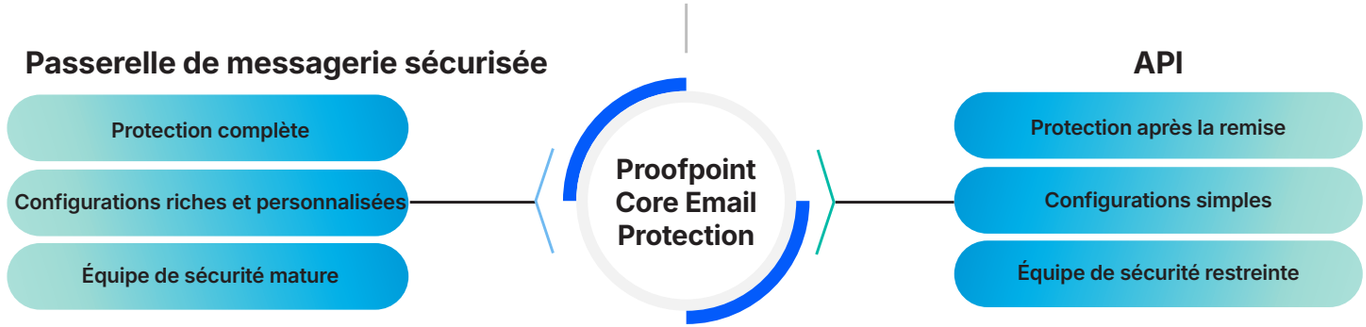
Proofpoint Core Email Protection ne se contente pas de bloquer les menaces. Il aide également les équipes de sécurité, qui bénéficient de workflows rationalisés basés sur des alertes et d'une recherche intégrée. Qui plus est, les emails signalés par les utilisateurs sont automatiquement corrigés, et les utilisateurs sont formés en temps réel à chaque fois qu'ils signalent un email suspect.

« La plate-forme [Proofpoint] offre une protection de la messagerie inégalée grâce à ses fonctionnalités robustes et optimisées par l'IA de détection des menaces, d'analyse multicouche du contenu et de sandboxing avancé. »[2]

GARTNER

1. Gartner, *Critical Capabilities for Email Security Platforms Report* (Rapport sur les fonctionnalités essentielles des plates-formes de protection de la messagerie), janvier 2025.
2. Ibid.

Passerelle de messagerie sécurisée ou API ? Proofpoint vous laisse le choix



Critère n° 1 : délai de rentabilisation

Quand choisir un déploiement basé sur API

Les déploiements basés sur API de Proofpoint ne prennent que quelques jours. Vous bénéficiez d'une protection automatisée dans un délai de 48 heures une fois que l'entraînement du système avec une année de données utilisateur est terminé. Notre solution basée sur API est plus adaptée aux équipes qui souhaitent bénéficier d'une protection de la messagerie puissante mais quasi automatique.

Quand choisir un déploiement basé sur SEG

Les déploiements Proofpoint via une passerelle de messagerie sécurisée (SEG) peuvent prendre quelques semaines. Cet investissement de temps permet toutefois d'éliminer la plupart des risques en offrant une protection avant la remise, après la remise et au moment du clic. Notre solution basée sur une passerelle de messagerie sécurisée offre davantage de possibilités de configuration et de personnalisation de votre déploiement. Elle est plus adaptée aux équipes qui souhaitent renforcer la protection de leur architecture.

Critère n° 2 : orientation Microsoft

Quand choisir un déploiement basé sur API

Si vous souhaitez renforcer la passerelle de messagerie sécurisée de Microsoft avec la protection après la remise de Proofpoint, utilisez notre intégration avec l'API Microsoft Graph. La solution Proofpoint basée sur API offre une expérience utilisateur Outlook native pour les menaces véhiculées par email, le spam et le graymail.

Quand choisir un déploiement basé sur SEG

Si vous souhaitez remplacer la passerelle de messagerie sécurisée de Microsoft, utilisez Proofpoint. Notre solution basée sur une passerelle de messagerie sécurisée offre une protection avant la remise, après la remise et au moment du clic grâce à Proofpoint Browser Isolation.

Critère n° 3 : sophistication de l'infrastructure de messagerie

Quand choisir un déploiement basé sur API

Si vous souhaitez utiliser la passerelle de messagerie sécurisée Microsoft de votre entreprise pour le routage des emails, choisissez la solution Proofpoint basée sur API. En général, les clients qui optent pour l'API ont des exigences simples en matière d'infrastructure de messagerie.

Quand choisir un déploiement basé sur SEG

Si votre entreprise dispose d'une infrastructure de messagerie sophistiquée, choisissez une passerelle de messagerie sécurisée. En général, les clients qui optent pour la passerelle de messagerie sécurisée souhaitent appliquer des règles qui contrôlent le flux d'emails et qui reposent sur des conditions telles que le domaine de l'expéditeur et l'authentification.

Pourquoi choisir Proofpoint ?

À propos de Proofpoint

Protection des personnes

3,4 Bios
d'emails analysés chaque année

> 1,4 Bio
de SMS/MMS analysés chaque année

124 Mios
d'attaques BEC bloquées chaque mois

> 183 Mios
de simulations d'attaques de phishing chaque année

0,8 Bio
de pièces jointes analysées chaque année

21 Bios
d'URL analysées chaque année

177 Mios
d'attaques TOAD bloquées chaque année

Adoption par le marché

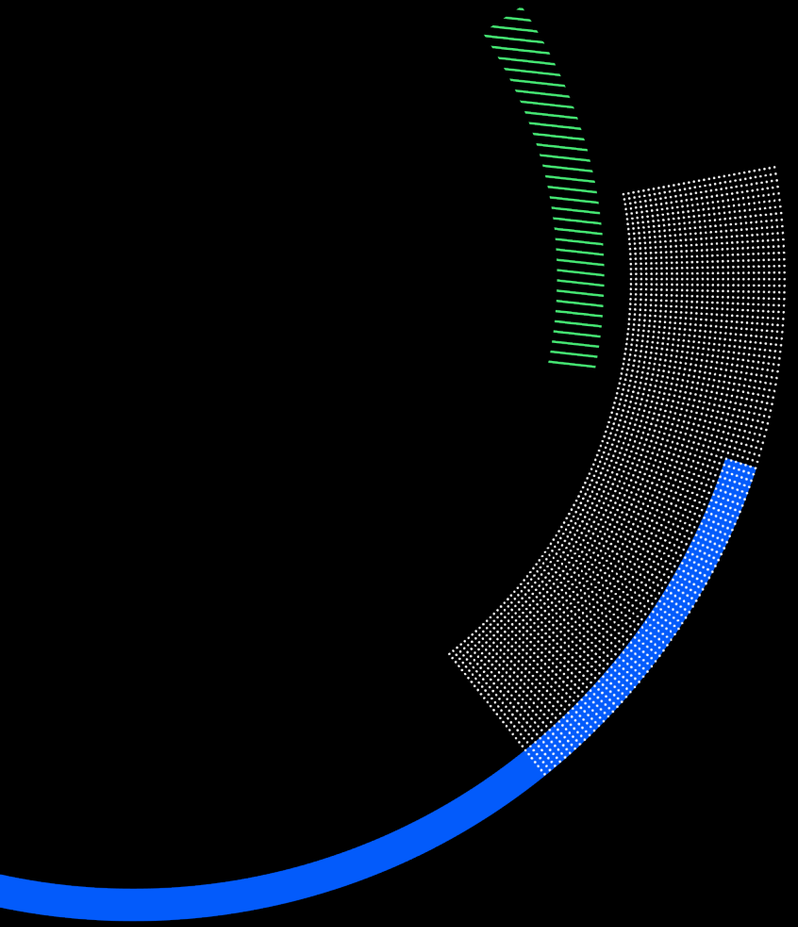
> 1,88 Mio
de clients

> 150
FAI et opérateurs mobiles partout dans le monde

85 %
du F100 protégés par Proofpoint

50 %
du F100 utilisent la DLP Proofpoint

> 60 %
du F1000 protégés par Proofpoint



proofpoint®

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risque 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 85 % des entreprises du classement Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via la messagerie, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.

Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →