proofpoint®

EBOOK

Une protection plus rapide et intelligente de la messagerie

Cinq raisons de choisir Proofpoint pour renforcer la sécurité de la messagerie Microsoft 365 via une API

Introduction

L'email est depuis longtemps le principal vecteur de menaces. Qui plus est, les attaques avancées telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise), les risques liés à la chaîne logistique, les ransomwares et les compromissions de comptes sont en hausse.

C'est donc sans surprise que des experts comme Gartner et Forrester recommandent de renforcer la sécurité de Microsoft 365[1, 2].

Des solutions intégrées de sécurité des emails dans le cloud (ICES) basées sur API ont vu le jour pour assurer une protection complète de la messagerie, du cloud et des données. Ces solutions peuvent être déployées rapidement pour bloquer ces attaques avancées.

La plupart des clients Microsoft qui cherchent à renforcer leur sécurité dans les plus brefs délais se tournent vers Proofpoint. 85 % des entreprises du classement Fortune 100 — et plus de 1,8 million de clients à travers le monde — nous ont choisis comme partenaire de sécurité. Proofpoint est le leader du secteur de la protection de la messagerie et du cloud.

L'API Proofpoint Core Email Protection établit une nouvelle norme pour les solutions ICES. Non seulement elle offre un niveau supérieur de détection des menaces avec un taux d'efficacité de 99,99 %, mais elle met également des outils de gestion fluides à la disposition des équipes. Il s'agit d'une plate-forme évolutive optimisée par les technologies d'IA révolutionnaires offertes par Proofpoint Nexus et notre threat intelligence mondiale inégalée. Avec Proofpoint, vous pourrez :

- Bloquer un large éventail de menaces grâce à la solution basée sur l'IA la plus performante au monde
- Optimiser l'efficacité de votre centre d'opérations de sécurité (SOC)
- Pérenniser votre architecture de sécurité afin de la préparer au paysage des menaces de demain

Mais les avantages ne s'arrêtent pas là. Voici une liste complète des raisons de choisir l'API Proofpoint Core Email Protection pour renforcer la sécurité de Microsoft 365.

1. Mark Harris, Peter Firstbrook, et al. (Gartner), « Market Guide for Email Security » (Guide du marché de la protection de la messagerie), octobre 2021.
2. Jess Burn, Joseph Blankenship, et al. (Forrester), « Best Practices: Phishing Prevention » (Bonnes pratiques en matière de prévention du phishing), novembre 2021.

Raison n° 1

Blocage d'un large éventail de menaces

La threat intelligence est une composante essentielle de la détection et de la neutralisation des menaces. Plus le volume de données auquel les algorithmes ont accès est important, mieux ils sont à même d'identifier les anomalies.

Proofpoint s'appuie sur une combinaison unique de données de threat intelligence. Notre pile de détection multicouche, Nexus AI, est entraînée par des billions de points de données mondiaux qui ont été collectés pendant plus de 20 ans auprès de milliers de clients. Nous combinons ces informations aux renseignements de notre équipe de recherche sur les cybermenaces pour optimiser la protection contre les menaces de nos clients.

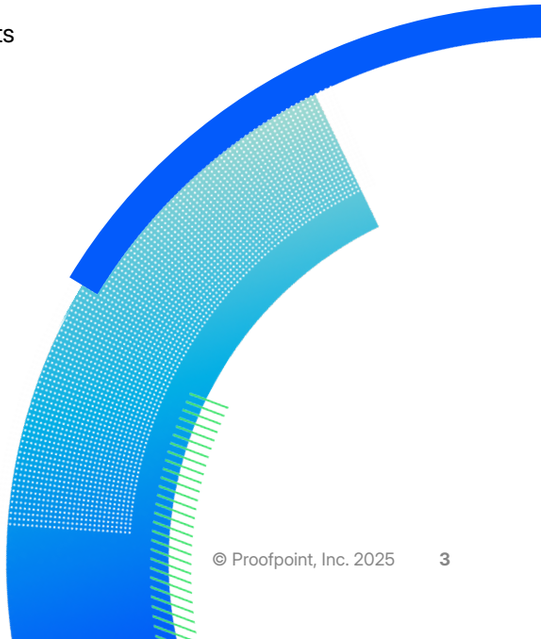
Soyez plus précis

La plupart des solutions basées sur API n'ont recours qu'à une seule technique de détection, par exemple la détection des anomalies. Par conséquent, elles passent souvent à côté de menaces réelles ou empêchent la remise de messages légitimes. Proofpoint, quant à lui, associe techniques d'IA et d'apprentissage automatique, threat intelligence et sandboxing pour accroître la précision de ses moteurs de détection. Nos ensembles de données étant complets, nous pouvons identifier plus de menaces et générer moins de faux positifs.

Protégez votre entreprise sous tous ses angles

Proofpoint Nexus AI intègre six cœurs performants lui permettant de bloquer un large éventail de menaces basées sur l'IA.

- **Nexus Language Model (LM)** reconnaît des structures linguistiques récurrentes subtiles et des indices comportementaux, ce qui lui permet d'identifier les attaques BEC avant qu'elles ne puissent causer des dommages.
- **Nexus Generative AI** analyse les données au niveau de la messagerie, du cloud et des endpoints afin d'identifier les tentatives de phishing et d'exfiltration de données.
- **Nexus Threat Intelligence (TI)** enrichit les modèles de détection des menaces en proposant des mises à jour en temps réel sur les tactiques, techniques et vulnérabilités des cybercriminels.
- **Nexus Relationship Graph (RG)** surveille les comportements des utilisateurs sur l'ensemble des systèmes, en recherchant les anomalies qui peuvent être le signe de menaces internes ou de compromissions de comptes.
- **Nexus Machine Learning (ML)** propose une détection prédictive des menaces.
- **Nexus Computer Vision (CV)** identifie et neutralise les menaces dissimulées dans des éléments visuels, comme les sites de phishing, les codes QR, les pièces jointes malveillantes et les emails falsifiés.



Raison n° 2

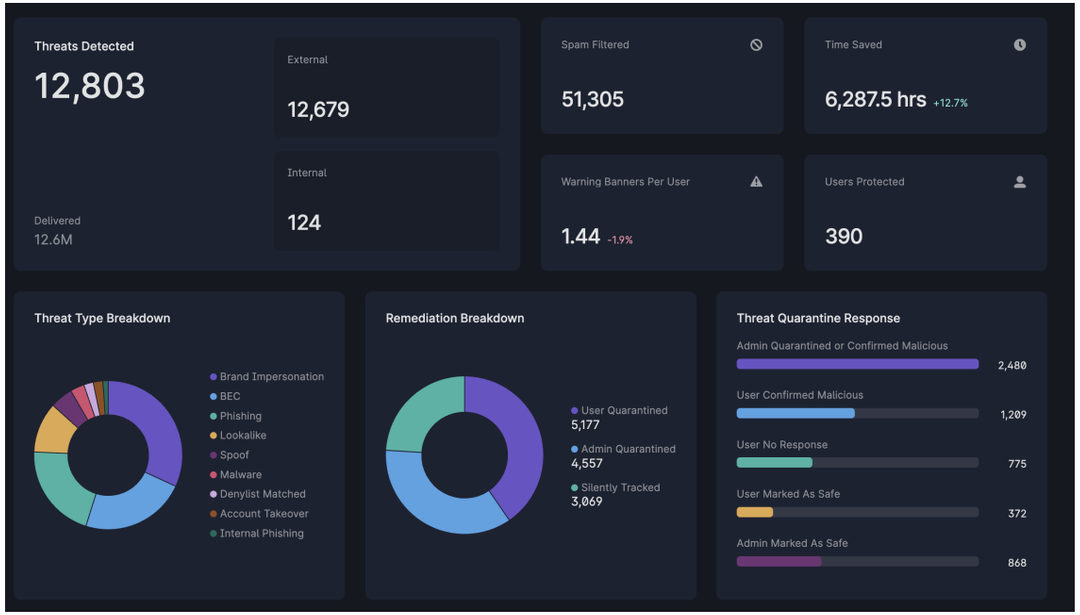
Optimisation de l'efficacité de votre SOC

Plus une menace reste présente longtemps dans votre environnement Microsoft 365, plus elle peut faire de dégâts. C'est pourquoi une réponse efficace et rapide aux incidents est essentielle pour préserver la sécurité de votre entreprise.

L'API Proofpoint Core Email Protection automatise la protection de la messagerie et offre des workflows très efficaces aux équipes SOC, qui peuvent ainsi se concentrer sur les tâches les plus importantes.

Voici comment Proofpoint rationalise le SOC :

- **Automatisation de la détection, de la neutralisation et de la réponse aux menaces email.** Le volume de menaces email que les équipes doivent analyser est considérablement réduit.
- **Affichage de bannières d'avertissement contextuelles et de messages de formation en temps réel.** Les messages d'avertissement et de formation aident les utilisateurs à prendre des décisions éclairées en matière de sécurité. Les administrateurs ont donc moins d'événements potentiels à analyser et à corriger.
- **Génération de brefs résumés sur les menaces.** Les équipes ont accès à un résumé intuitif, créé par l'IA générative, des points les plus importants pour chaque menace.
- **Accélération de la traque et de la correction des menaces.** La recherche intégrée et les workflows basés sur des alertes aident les équipes à identifier rapidement les véritables menaces et à les corriger avant qu'elles ne puissent causer des dommages.
- **Déploiement rapide.** Notre solution est intégrée à l'API Microsoft Graph et dispose d'une période d'apprentissage automatisé de moins de 48 heures.



Avec Proofpoint

99,99 % des menaces email sont bloquées avant qu'elles ne deviennent des compromissions

30 % de menaces email en moins doivent être gérées par le SOC

Raison n° 3

Protection contre les menaces actuelles les plus furtives

Les menaces email évoluent constamment et sont difficiles à bloquer. C'est pourquoi la protection des collaborateurs est une tâche ardue, même pour les entreprises les plus sophistiquées. Heureusement, Proofpoint peut vous aider.

Grâce à l'API Proofpoint Core Email Protection, vous pouvez détecter et bloquer les menaces connues et inconnues dans toute votre entreprise. Les menaces avancées sont ainsi neutralisées non pas après leur distribution, mais avant. Il s'agit notamment des menaces suivantes :

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.

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 Nexus AI 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.

Menaces TOAD

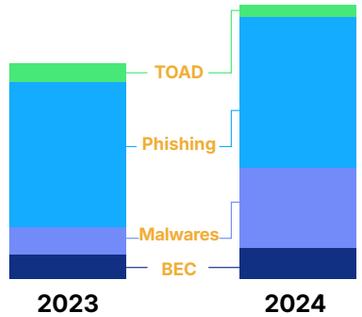
Lors des attaques par téléphone (TOAD, Telephone-Oriented Attack Delivery), également appelées phishing de rappel, les cybercriminels envoient des emails qui tentent de convaincre les destinataires d'appeler un faux centre d'appels. Ces menaces peuvent être difficiles à détecter, car elles comportent rarement des charges virales malveillantes.

Les moteurs Proofpoint Nexus AI 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.).

+ 45,8 %

d'augmentation du nombre de menaces* distribuées aux utilisateurs sur un an

* Messages malveillants détectés par Proofpoint



124 Mios

Nombre d'attaques BEC bloquées chaque mois par Proofpoint

45 %

Hausse annuelle des menaces email distribuées aux utilisateurs finaux

9 Mios

Nombre d'attaques TOAD bloquées chaque mois par Proofpoint

Raison n° 4

Expérience utilisateur optimale

En matière de protection de la messagerie, la meilleure expérience que vous puissiez offrir aux utilisateurs est une expérience invisible. Notre taux de détection de 99,99 % vous rapproche de cet objectif. Proofpoint réduit les distractions pour les utilisateurs en bloquant les menaces, le spam et le graymail.

Avec l'API Proofpoint Core Email Protection, vous pouvez offrir aux utilisateurs :

- Une expérience Outlook native pour le spam et le graymail
- Moins de distractions grâce à une détection extrêmement efficace et à une correction rapide
- Des avertissements contextuels leur permettant de se former en temps réel

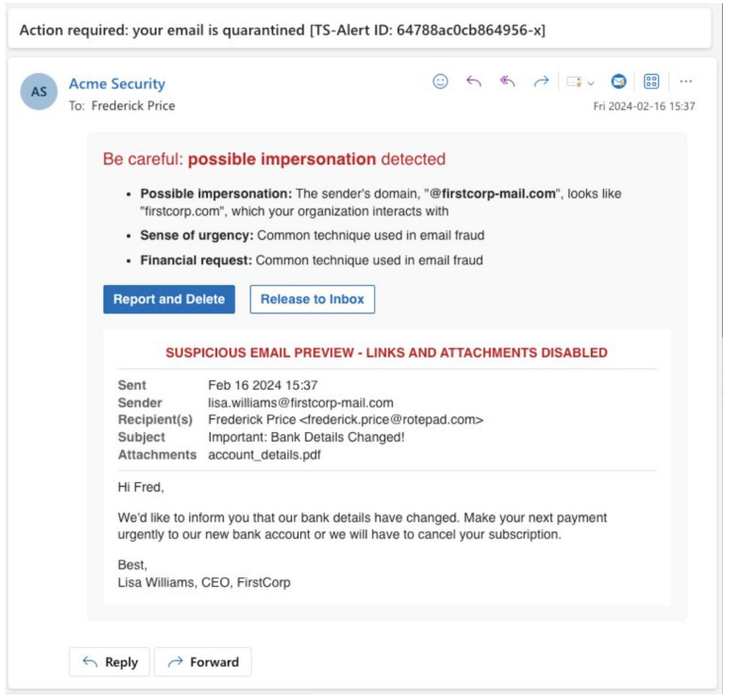
Proposez des expériences utilisateur Outlook natives

De nos jours, les utilisateurs sont submergés par le volume d'emails qu'ils reçoivent quotidiennement. Proofpoint réduit les informations parasites en déplaçant automatiquement le spam et le graymail de la boîte de réception vers le dossier Courrier indésirable par défaut de Microsoft.

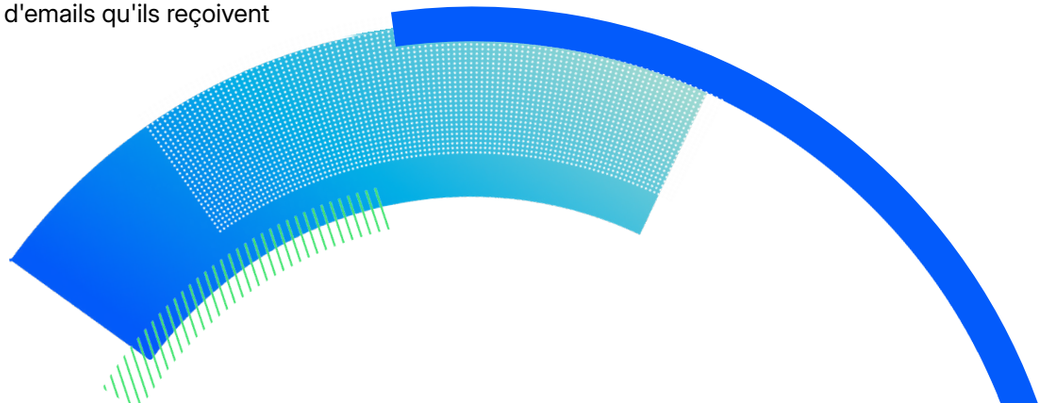
Les utilisateurs peuvent retransférer les messages de leur choix dans leur boîte de réception, ce qui évite que les emails provenant de ces expéditeurs soient marqués comme spam ou graymail à l'avenir.

Préservez la productivité des utilisateurs et des équipes de sécurité

L'API Proofpoint Core Email Protection aide les collaborateurs à rester productifs en distribuant en toute sécurité les emails présentant un risque faible à modéré. Ces messages incluent une formation en temps réel qui aide les utilisateurs à prendre des décisions éclairées en matière de sécurité et à apprendre de leurs erreurs. Les administrateurs ont donc moins d'événements potentiels à analyser et à corriger.



Formation en temps réel des utilisateurs en cas d'emails suspects



Raison n° 5

Pérennisation de votre architecture de sécurité

Proofpoint vous aide à réduire les risques au niveau de tous les points d'interaction des collaborateurs, aujourd'hui et à l'avenir.
Nous protégeons votre entreprise contre les cybercriminels qui usurpent l'identité de vos collaborateurs, partenaires et fournisseurs, et prévenons les fuites de données accidentelles et intentionnelles.

Par ailleurs, nos solutions s'intègrent à un large éventail d'outils pour vous aider à automatiser et à consolider votre pile de sécurité.

Notre plateforme s'intègre aux solutions de sécurité d'éditeurs de solutions de premier plan, tels que Palo Alto Networks, Okta, CrowdStrike et bien d'autres encore.

Consolidez vos éditeurs de solutions pour améliorer votre retour sur investissement

Lorsque vous choisissez Proofpoint pour renforcer la sécurité de Microsoft 365, vous obtenez également un accès à nos solutions complètes, qui vont au-delà de la protection de votre entreprise contre les attaques par email. Vous pouvez ainsi fournir à votre équipe des outils de pointe pour rationaliser leurs workflows.

Avec Proofpoint, vous bénéficiez d'une sécurité qui couvre vos collaborateurs, vos données et toute votre entreprise.

Bloquez les menaces ciblant les utilisateurs

- Protégez la messagerie contre les malwares, le phishing et les attaques BEC.
- Prévenez les usurpations d'identité et les compromissions de fournisseurs.
- Protégez les outils de collaboration contre le vol d'identifiants de connexion et les attaques de malwares.

Protégez vos données et vos communications numériques

- Empêchez vos utilisateurs de mettre les données en péril par erreur.
- Détectez les activités internes malveillantes et recevez des alertes en temps réel.
- Gouvernez toutes vos communications numériques.

Apprenez à vos collaborateurs à prendre des décisions de sécurité plus avisées

- Proposez des formations personnalisées basées sur le niveau de risque.
- Simulez des attaques pour évaluer la résilience de vos utilisateurs.
- Encouragez les bons comportements grâce à des suggestions d'actions en temps réel par email et sur le Web.

Neutralisez les attaques visant les applications SaaS et les identités

- Détectez et neutralisez les prises de contrôle de comptes.
- Suivez et comprenez de façon proactive les voies d'attaque via Active Directory.
- Détectez les comptes SaaS (Software-as-a-Service) et prévenez la dérive du niveau de sécurité.

Collaborez avec un leader du secteur

Avec Proofpoint, vous n'avez pas à choisir entre une technologie de pointe et une solution entièrement intégrée. Nous sommes un leader reconnu du secteur dans les domaines de la cybersécurité, de la protection contre les fuites de données (DLP) et de la conformité.

Proofpoint Core Email Protection salué par les analystes du secteur

Gartner	Leader Magic Quadrant 2024 pour les plates-formes de protection de la messagerie	En tête dans quatre des cinq cas d'utilisation Dans le Magic Quadrant 2024 pour les plates-formes de protection de la messagerie : - Protection de la messagerie de base - Plates-formes de sécurité - Protection des emails sortants - Utilisateurs avancés
FORRESTER®	Forrester Wave™ : Enterprise Email Security, Q2 2023 | Leader	
FROST & SULLIVAN	Frost Radar™ : Email Security, 2023 – Leader dans les catégories Marché de la protection de la messagerie et Index de croissance du rapport Frost Radar™ pour la 9e année consécutive	Frost & Sullivan 2024 Prix Company of the Year Award | Global Email Security Industry et Excellence in Best Practices Frost & Sullivan 2025 Prix Company of the Year Award | Australian Email Security Industry Excellence in Best Practices
GIGAOM	Rapport GigaOm Radar 2023 consacré à la lutte contre le phishing : Leader et Fast Mover	Rapport GigaOm Radar 2024 consacré à la détection et à la neutralisation des menaces liées aux identités : Leader et Fast Mover Rapport GigaOm Radar 2024 consacré aux technologies de tromperie : Leader et Fast Mover
kuppingercole ANALYSTS	Rapport Leadership Compass 2023 pour la protection de la messagerie : Leader dans les quatre catégories : générale, produits, innovation et marché	
OMDIA	Rapport Omdia Universe 2024 pour la protection de la messagerie : Leader	
	Market Quadrant 2024 de Radicati pour la protection de la messagerie : Top Player	

proofpoint.

Passez à l'étape supérieure

La meilleure cyberdéfense est celle qui est capable de neutraliser les menaces « à la source ». C'est la raison pour laquelle plus de 1,8 million de clients à travers le monde nous ont choisis comme partenaire de sécurité.

L'API Proofpoint Core Email Protection bloque 99,99 % des menaces 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.

L'API Proofpoint Core Email Protection ne se contente pas de bloquer les menaces. Elle 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 ces derniers sont formés en temps réel chaque fois qu'ils signalent un email suspect.

Découvrez comment Proofpoint peut vous aider à renforcer la sécurité de votre messagerie et de votre cloud Microsoft 365.

proofpoint.com/fr/products/threat-defense

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

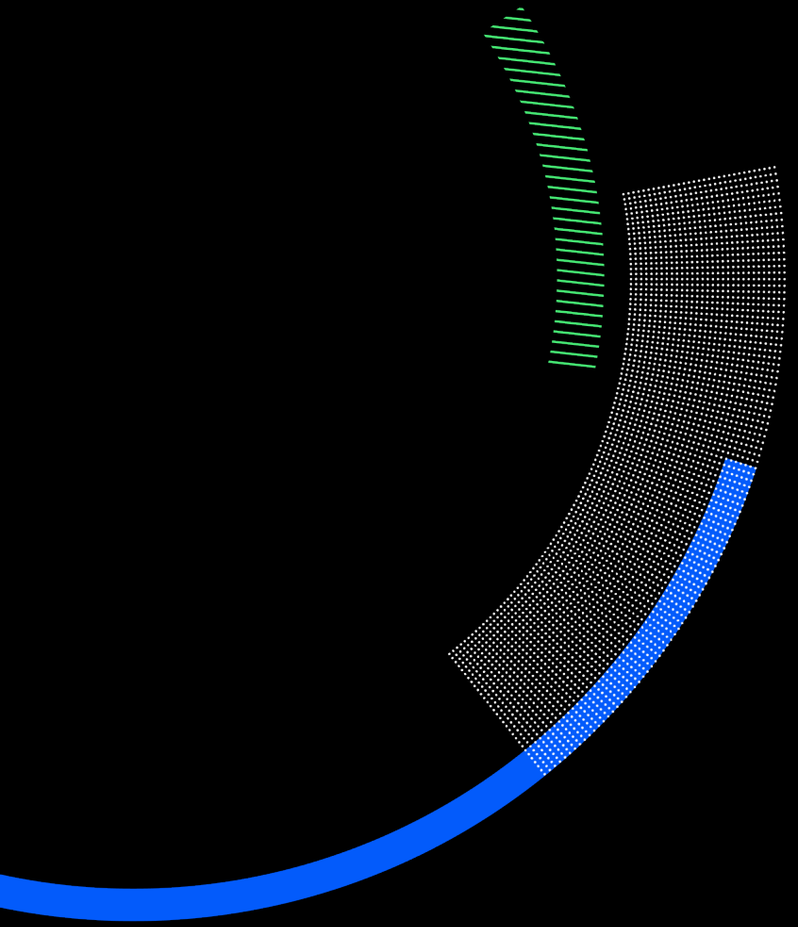
> 1,88 Mio
de clients

> 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 →