

Comment choisir la meilleure solution de protection de la messagerie électronique pour votre entreprise



Principales fonctionnalités

Voici les principales fonctionnalités à prendre en considération lorsque vous envisagez de vous procurer une solution de protection de la messagerie électronique moderne :

1. Protection contre le plus large éventail de menaces
2. Détection et neutralisation automatisées des menaces
3. Options de déploiement flexibles
4. Expérience utilisateur de qualité
5. Protection contre les menaces au-delà des emails

Présentation

L'email reste l'un des principaux vecteurs de cyberattaques. Ces dernières années, cependant, la surface d'attaque s'est étendue au-delà de la messagerie électronique, les utilisateurs employant désormais de multiples canaux numériques pour communiquer et collaborer. Il n'est donc pas étonnant que les cybercriminels leur emboîtent le pas et tirent profit de cette tendance. De fait, ils distribuent avec grand succès une large variété de menaces centrées sur les personnes à travers tous les canaux numériques.

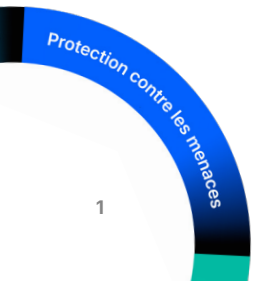
En réaction, les entreprises assemblent un patchwork disparate de produits isolés de pointe pour contrer ces menaces.

Malheureusement, cette stratégie laisse des failles dans la défense et néglige de nombreux risques. Qui plus est, gérer et intégrer des outils de sécurité différents est à la fois compliqué et coûteux. Pour éviter ces écueils, les entreprises ont besoin d'une solution complète de protection de la messagerie électronique, capable de les défendre contre les menaces actuelles et émergentes centrées sur les personnes, sous la forme d'une plate-forme unique.

Dans ce guide, nous mettons en évidence les fonctionnalités clés indispensables d'une solution de protection de la messagerie électronique performante, ainsi que les raisons de leur importance.



Figure 1. Répartition des types de menaces distribuées par email



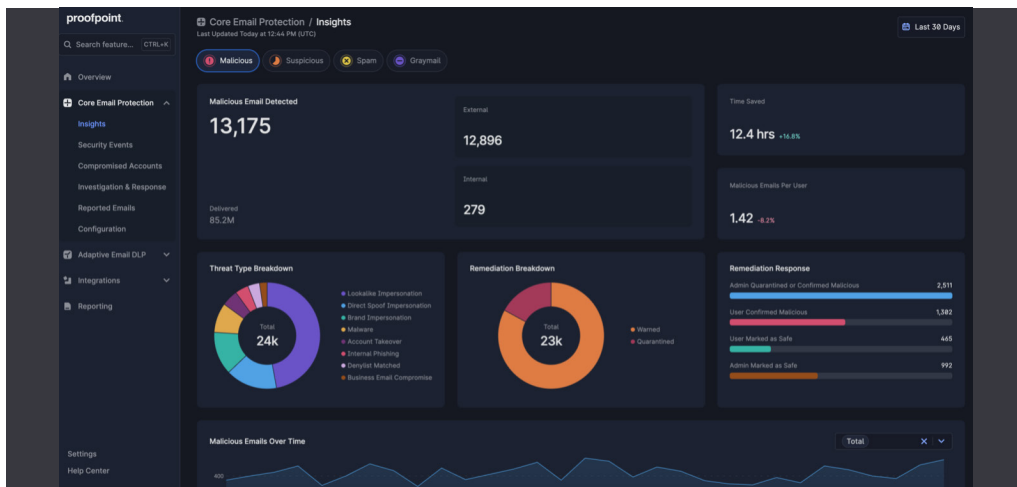


Figure 2. Vue complète des menaces par email bloquées par Proofpoint Core Email Protection

55 Mrds \$

Pertes dues aux attaques BEC entre 2013 et 2023 dans le monde²

60 secondes

Temps moyen qu'il faut à un utilisateur pour tomber dans le piège d'un email de phishing³

1. Protection contre le plus large éventail de menaces

Le coût moyen d'une compromission de données causée par une attaque de phishing ou de piratage de la messagerie en entreprise (BEC, Business Email Compromise) s'élève à 4,88 millions de dollars¹. Il s'agit du deuxième coût de compromission le plus élevé, après celui des attaques dues à des utilisateurs internes malveillants. Et chaque menace qui passe entre les mailles du filet peut coûter cher en termes de pertes financières et d'atteinte à l'image de marque.

Les équipes de sécurité mettent tout en œuvre pour réduire autant que possible l'exposition aux risques de l'entreprise. La seule manière d'atteindre cet objectif est de bloquer le plus large éventail de menaces.

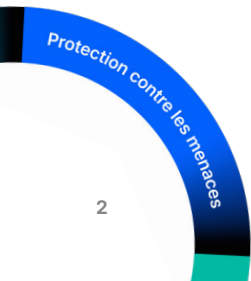
Voici les critères que doit réunir une solution de protection de la messagerie électronique à cet égard :

- **Utilisation d'une threat intelligence en temps réel.** Une threat intelligence constamment actualisée facilite l'identification des menaces émergentes. Cela étant, la threat intelligence ne se résume pas aux données, elle doit également impliquer des équipes de recherche sur les cybermenaces hautement qualifiées. Lorsqu'une solution dispose de ces deux atouts, elle est capable d'analyser les tendances à grande échelle plus rapidement et efficacement. Elle peut par exemple détecter et suivre des cybercriminels et acteurs étatiques sophistiqués, de même qu'identifier les évolutions du paysage des menaces.

- **Exploitation de l'IA pour la détection des menaces.** Pour bloquer les attaques par email qui reposent sur la manipulation associée à des charges virales, une pile de détection multicouche optimisée par l'IA est essentielle. Les grands modèles de langage (LLM), les graphiques relationnels et comportementaux, l'apprentissage automatique et la capacité d'analyse d'images sont autant de fonctionnalités fondamentales, car elles garantissent le blocage des menaces à grande échelle.
- **Surveillance continue des menaces.** La capacité à analyser les URL et les pièces jointes en environnement sandbox est importante. Le moment auquel vous effectuez ce sandboxing l'est tout autant. Pour identifier les attaques ayant éludé les défenses ou les menaces à activation différée, il convient d'adopter une solution qui détecte et bloque les menaces tout au long de leur cycle de vie – avant la remise, après la remise et au moment du clic.
- **Visibilité sur les utilisateurs ciblés.** Vous devez identifier les personnes ciblées et les méthodes d'attaque utilisées, ainsi qu'établir si les utilisateurs visés sont tombés dans le piège. De même, il est important de savoir de quelle manière ces utilisateurs sont ciblés, à quelles données ils ont accès et s'ils ont tendance à être la cible d'attaques. Fort de ces informations, vous pourrez mettre en place les mesures de protection adéquates au moment opportun.

Plus les menaces sont détectées tôt, plus votre entreprise est en sécurité. En outre, vos équipes informatiques et de sécurité ne devront plus consacrer leur temps précieux à la réponse aux incidents et à la correction.

1. IBM, *Rapport sur le coût d'une violation de données*, 2024.
 2. FBI, « Business Email Compromise: The \$55 Billion Scam » (Piratage de la messagerie en entreprise : des arnaques chiffrées à 55 milliards de dollars), septembre 2024.
 3. Verizon, *Data Breach Investigations Report* (Rapport d'enquête sur les compromissions de données), 2024.



2. Détection et neutralisation automatisées des menaces

Les messages malveillants qui atteignent les boîtes de réception ou sont signalés par les utilisateurs peuvent monopoliser les équipes de sécurité et nuire à leur productivité. L'analyse et la suppression manuelles de ces menaces sont très chronophages. Il est essentiel de détecter et de neutraliser ces menaces rapidement. Une intervention rapide peut faire toute la différence entre un incident mineur et une compromission à grande échelle.

Voici les critères que doit réunir une solution de protection de la messagerie électronique à cet égard :

- Boîte email de signalement d'abus optimisée par l'IA.** Les messages signalés par les utilisateurs doivent être traités aussi vite que possible. Lorsqu'ils sont automatiquement dirigés vers une boîte de réception surveillée par une machine, ils peuvent être analysés par l'IA et neutralisés sans intervention de votre équipe informatique ou de sécurité. Un système de réponse automatisée doit aussi informer les utilisateurs que leurs signalements ont été reçus. Ce feedback ferme la boucle de rétroaction et renforce les comportements positifs.
- Orchestration et correction automatisées.** Les emails malveillants ne doivent en aucun cas rester dans les boîtes de réception des utilisateurs. Au contraire, ils doivent être supprimés automatiquement des boîtes de réception à l'échelle de l'entreprise. Assurez-vous également que la solution s'intègre facilement avec vos outils SIEM/SOAR existants. Vous disposerez ainsi d'une vue plus unifiée de votre écosystème de sécurité.
- Workflows simplifiés.** Les outils de sécurité doivent faciliter le travail des analystes. Par exemple, des workflows intuitifs et des résumés de menaces clairs générés par l'IA constituent des atouts pour leur productivité. Des fonctionnalités telles que la recherche intégrée et des alertes priorisées peuvent les aider à traquer rapidement les menaces. Il en va de même pour les outils qui accélèrent les mesures de correction qui restent à prendre après les actions automatisées.

Lorsque l'efficacité de votre équipe de sécurité s'améliore, vos défenses se renforcent. De plus, vous exploitez au mieux le potentiel de vos ressources et investissements de sécurité existants.

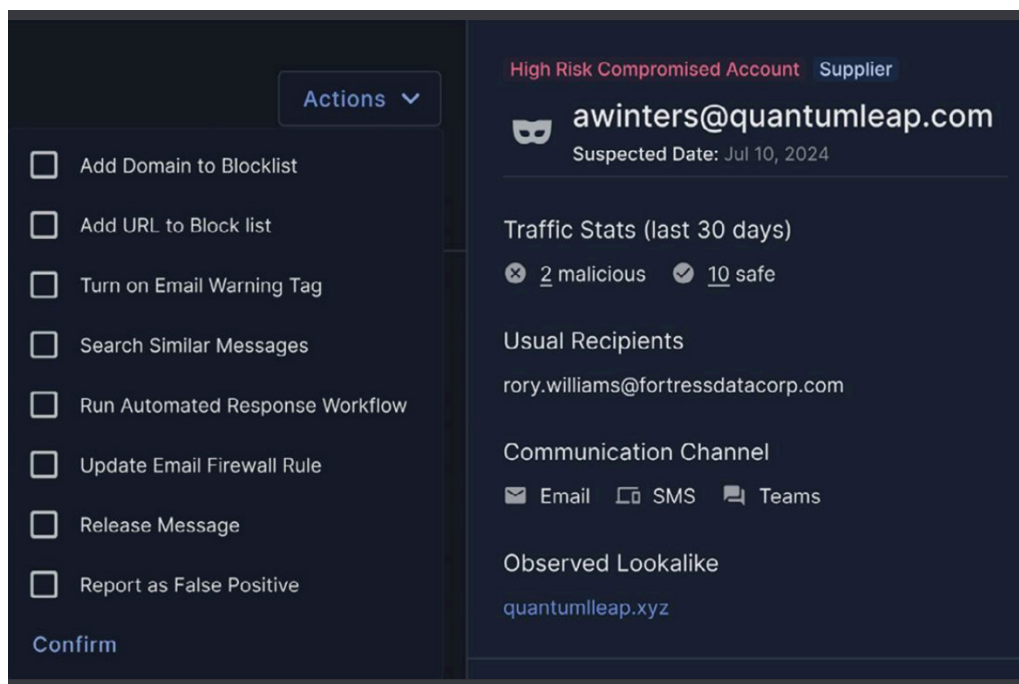
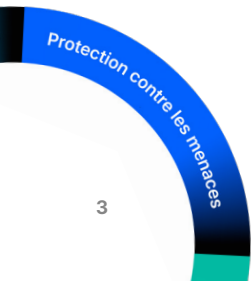


Figure 3. Exemples de workflows automatisés de détection et de réponse de Proofpoint Core Email Protection



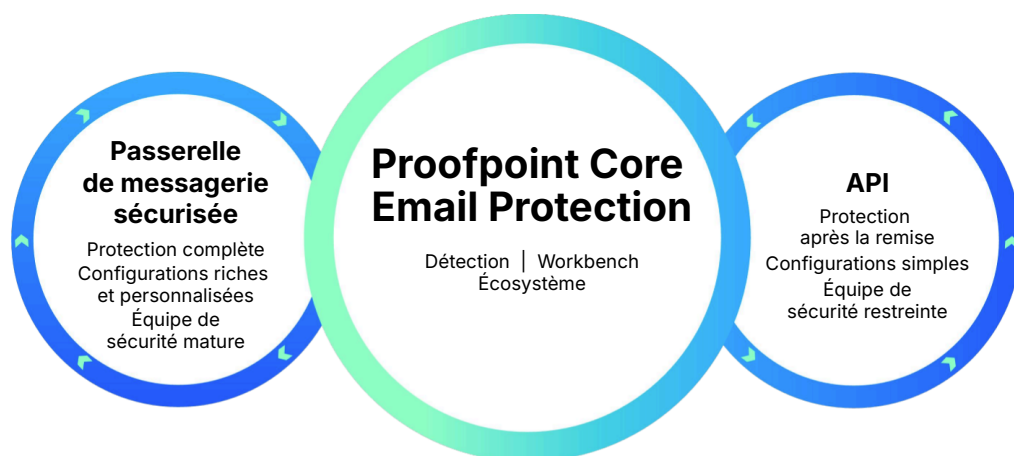


Figure 4. Avantage du déploiement par API et par passerelle de messagerie sécurisée de Proofpoint Core Email Protection

3. Options de déploiement flexibles

Votre architecture, vos priorités de sécurité et vos exigences en matière de conformité sont en évolution constante. Une solution de protection de la messagerie électronique doit pouvoir évoluer et monter en charge en parallèle. Même si un déploiement par API constitue la meilleure approche aujourd'hui, il est possible que cela ne soit plus le cas à l'avenir. En ne vous cantonnant pas à une seule approche de déploiement, vous avez la garantie de pouvoir optimiser votre couverture en fonction des risques en présence.

En outre, lorsque vous disposez d'un choix, vos équipes informatiques et de sécurité peuvent faire évoluer et renforcer vos défenses pour qu'elles restent efficaces à long terme. Et votre entreprise peut conserver une protection robuste au fur et à mesure de sa croissance.

Voici les fonctionnalités à envisager :

- **Déploiement par passerelle de messagerie sécurisée.** Les passerelles de messagerie sécurisées assurent une protection complète pour de nombreux types d'environnements. C'est l'option à privilégier si vous souhaitez bénéficier d'une protection de la messagerie hautement personnalisable. Ces passerelles vous permettent de maximiser votre niveau de sécurité de bout en bout grâce à une protection avant la remise, après la remise et au moment du clic. Elles offrent des options de configuration flexibles, ainsi qu'une visibilité sur les risques liés aux personnes.
- **Déploiement basé sur API.** Cette option offre un onboarding simple à exécuter et des contrôles prédéfinis au sein de plates-formes cloud telles que Microsoft 365. Le déploiement peut être réalisé en quelques minutes. Ce choix s'impose si vous souhaitez une protection de la messagerie puissante mais exigeant peu de travail de configuration, associée à une expérience d'administration fortement automatisée, avec des informations sur les menaces faciles à comprendre et des actions de correction automatiques.

En optant pour un éditeur de solutions offrant des options de déploiement flexibles, vous disposez du type de détection qui vous convient, tout en assurant la pérennité de votre dispositif de sécurité.

74 %

Pourcentage de RSSI considérant le facteur humain comme la plus grande vulnérabilité de leur entreprise⁴

40 %

La sensibilisation à la sécurité peut réduire le nombre de clics sur des menaces réelles de plus de 40 % en moins de six mois⁵

4. Expérience utilisateur de qualité

Un adage dit que votre plus grand risque et votre meilleure arme de détection occupent le même espace : celui entre la chaise et le clavier. Pour que les messages malveillants soient bloqués, les utilisateurs ont besoin des bons outils.

S'ils sont débordés, ils seront davantage susceptibles d'ignorer les vraies menaces ou de commettre des erreurs. Le spam, le graymail et les fausses alertes incessantes augmentent ce risque. Les collaborateurs ont besoin d'avertissements clairs et exploitables, d'outils de génération de rapports intuitifs et de simulations de phishing bien conçues afin de renforcer les comportements de sécurité positifs.

Voici les critères que doit réunir une solution de protection de la messagerie électronique à cet égard :

- Détection du spam et du graymail.** Le spam et les emails envoyés en masse encombrant les boîtes de réception et distraient les utilisateurs. Même le graymail, tel que les emails commerciaux non sollicités, peut affecter la productivité. La protection de la messagerie électronique préserve l'intégrité des boîtes de réception et les désencombre, ce qui améliore l'expérience utilisateur et aide les collaborateurs à rester concentrés.
- Avertissements aux utilisateurs en cas de messages suspects.** Les emails suspects peuvent être de nature malveillante ou légitime, et seul un utilisateur peut faire la différence. Les notifications contextuelles

préliminaires informent les utilisateurs des signaux de menaces identifiés dans les messages. En même temps, elles neutralisent automatiquement les pièces jointes ou URL malveillantes associées avec le message suspect, imposant à l'utilisateur d'interagir avec la notification avant de pouvoir le faire avec l'email lui-même.

- Protection au moment du clic.** Même les collaborateurs bien intentionnés peuvent commettre une erreur et cliquer sur une menace lorsqu'ils sont submergés de travail. Les protections au moment du clic telles que les bannières d'avertissement permettent aux utilisateurs de marquer une pause et de réfléchir avant d'agir. De plus, les fenêtres de navigation virtuelle ajoutent une couche de protection supplémentaire en prévenant le vol d'identifiants de connexion et le téléchargement de malwares.
- Sensibilisation à la sécurité personnalisée.** Souvent, les simulations de phishing et les formations de sensibilisation constituent les principales méthodes d'interaction entre les collaborateurs et les solutions de protection de la messagerie électronique. Les outils de formation les plus efficaces proposent un apprentissage en temps réel lorsque les utilisateurs cliquent sur un message de phishing. Ils offrent en outre de courts modules interactifs, adaptés au niveau de connaissances de chaque utilisateur. Cette approche personnalisée favorise la sensibilisation et les bons comportements à long terme.

Une expérience utilisateur cohérente aide vos utilisateurs à rester vigilants tout en étant concentrés sur leurs tâches.

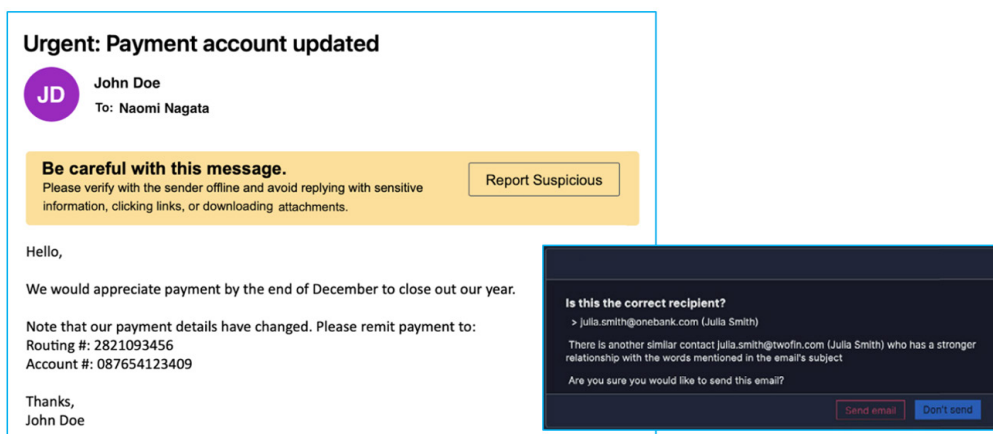
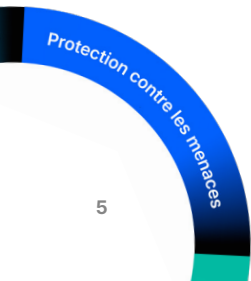


Figure 5. Exemple de message d'alerte signalant une erreur de destinataire potentielle et bannière d'avertissement correspondante s'affichant dans l'email

4. Proofpoint, *Voice of the CISO*, 2024.
 5. Étude Proofpoint ZenGuide.



2 524 %

Hausse du nombre d'URL malveillantes diffusées dans le cadre d'attaques de phishing par SMS au cours des trois dernières années⁶

5. Protection contre les menaces au-delà des emails

Avec l'élargissement des espaces de travail numériques, il est important de disposer d'une plate-forme adaptable. Celle-ci doit être capable de protéger non seulement la messagerie électronique, mais aussi les nouveaux canaux de communication numériques. Les cybercriminels ne limitent plus leurs attaques à l'email. Ils ont suivi les utilisateurs sur des plates-formes telles que Microsoft Teams, Slack, Zoom, LinkedIn et WhatsApp, qui sont autant de nouveaux vecteurs d'attaque.

Pour qu'une solution soit pérenne, elle doit inclure des protections avancées supplémentaires, telles que l'authentification des emails DMARC, la détection fiable des comptes cloud compromis et une visibilité sur les menaces email provenant des fournisseurs.

Voici les autres points à prendre en compte :

- **Authentification rationalisée des emails.** L'authentification des emails tant à l'entrée qu'en sortie est l'un des moyens les plus efficaces pour lutter contre les emails frauduleux. Pour protéger votre image de marque, optez pour un éditeur de solutions qui propose des services managés ou hébergés afin de rationaliser le déploiement de l'authentification. Les conseils d'experts peuvent s'avérer précieux dès lors qu'il est question du protocole DMARC.

- **Détection des comptes compromis.** Associer visibilité sur les menaces par email (comme les clics effectifs sur les messages de phishing) et alertes CASB (Cloud Access Security Broker) garantit une détection plus précise des comptes compromis. Une telle approche limite le nombre de faux positifs et permet d'appliquer des réponses automatisées, comme forcer la réinitialisation de mots de passe ou supprimer le partage de fichiers sensibles.
- **Protection contre le phishing au-delà des emails.** Les URL malveillantes sont désormais le vecteur d'attaque le plus courant, en partie parce qu'elles peuvent être envoyées par tous les canaux, notamment les applications de messagerie instantanée, les outils de collaboration et les réseaux sociaux. Optez pour une solution capable d'analyser les URL en temps réel, de façon à ce que les liens malveillants soient bloqués partout et chaque fois que les utilisateurs tentent d'y accéder.
- **Limitation des risques liés aux fournisseurs.** Il peut être difficile d'identifier les menaces au sein de votre chaîne logistique sans une visibilité suffisante. Les solutions de protection de la messagerie électronique dotées de fonctionnalités intégrées d'identification des risques liés aux fournisseurs peuvent attribuer des scores de risques et détecter les comptes fournisseurs compromis, ce qui contribue à limiter les fraudes. Associée à l'authentification, cette approche proactive peut renforcer la protection contre l'un des vecteurs d'attaque les plus difficiles à identifier.

Grâce à ces fonctionnalités, vos équipes peuvent gérer efficacement les menaces nouvelles et émergentes, quelle que soit leur origine.

6. Étude de Proofpoint.

Conclusion

Plus de 94 % des menaces qui ciblent vos collaborateurs sont transmises par email⁷, raison pour laquelle une protection robuste de ce vecteur prévalent est essentielle.

Pour optimiser votre défense contre les menaces, optez pour une solution de protection de la messagerie complète, comprenant à la fois des fonctionnalités de base et avancées. Une telle solution doit pouvoir détecter et neutraliser les menaces automatiquement, ainsi qu'offrir une expérience utilisateur optimale. Dans l'idéal, elle doit également proposer des options de déploiement flexibles pour s'adapter à l'évolution de vos besoins. Enfin, elle doit sécuriser d'autres canaux numériques que l'email, comme les outils de collaboration, les plates-formes de messagerie instantanée et les applications cloud.

Dépendez-vous d'un assemblage de solutions spécialisées et cloisonnées ? Si c'est le cas, vous avez toute latitude pour améliorer la protection de votre messagerie électronique. Le moment est venu d'évaluer l'efficacité de votre dispositif de sécurité contre les menaces centrées sur les personnes, qu'elles soient diffusées par email ou par d'autres vecteurs.

Proofpoint offre une sécurité centrée sur les personnes

Proofpoint Core Email Protection permet à votre entreprise de réduire les risques au niveau de tous les points d'interaction des utilisateurs, aujourd'hui et à l'avenir.

Proofpoint Core Email Protection bloque 99,99 % des menaces véhiculées par email avant qu'elles ne deviennent des compromissions. Optimisé par Proofpoint Nexus, notre pile de détection de pointe assistée par l'IA, Proofpoint Core Email Protection identifie et neutralise les menaces email avancées, y compris le phishing, le piratage de la messagerie en entreprise (BEC), les malwares, les ransomwares, la prise de contrôle de comptes, l'usurpation d'identités, l'ingénierie sociale, etc. Grâce à la console moderne et intuitive qui offre une visibilité complète sur les menaces et des workflows de correction automatisés, les analystes en sécurité gagnent en efficacité. L'architecture pérenne de la solution la prépare au paysage des menaces de demain, grâce à des options de déploiement flexibles de type API ou passerelle de messagerie sécurisée.

Voilà pourquoi plus de deux millions de clients, dont 85 des entreprises du classement Fortune 100, font confiance aux solutions de sécurité centrée sur les personnes de Proofpoint pour protéger leurs utilisateurs et leurs activités.

Pour en savoir plus, contactez notre équipe commerciale à l'adresse sales@proofpoint.com.

7. Étude de 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](#)

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 citées dans ce document sont la propriété de leurs détenteurs respectifs. ©Proofpoint, Inc. 2025

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →