

**FICHE SOLUTION**

# Proofpoint Prime Threat Protection – Édition entreprise

**Principaux avantages**

- Bloque un large éventail de menaces avec une précision de 99,99 %
- Étend la protection des utilisateurs sur toutes les plates-formes, pas seulement la messagerie électronique
- Renforce la résilience des utilisateurs grâce à des informations et à des conseils basés sur les risques
- Réduit les délais de réponse en cas de compromission de comptes de collaborateurs et de fournisseurs
- Simplifie les opérations grâce à une détection extrêmement efficace et à un workflow automatisé
- Accélère la rentabilisation grâce à la consolidation et à l'intégration préconfigurée

## Présentation

La messagerie électronique reste l'un des principaux vecteurs de cybermenaces. Toutefois, ces dernières années, la surface d'attaque s'est élargie. Les cybercriminels ciblent désormais des personnes par email et via d'autres canaux numériques tels que les plates-formes de messagerie, les outils de collaboration, les applications cloud et les services de partage de fichiers.

En réponse, un grand nombre d'entreprises adoptent une approche fragmentée de la sécurité, basée sur des produits isolés. Cette stratégie engendre toutefois des failles supplémentaires dans leurs défenses et néglige de nombreux risques. Par ailleurs, la gestion et l'intégration de tous ces outils s'avèrent complexes.

Pour vous défendre contre ces menaces centrées sur les personnes en constante évolution, vous devez adopter une approche globale. Proofpoint Prime Threat Protection (Prime) peut vous aider.

Proofpoint Prime vous permet de vous défendre contre les attaques multicanales en plusieurs phases et de sécuriser vos communications d'entreprise. Il fournit également des conseils basés sur les risques à l'intention de vos collaborateurs et rationalise vos opérations de sécurité à tous les niveaux.

## Proofpoint Prime Threat Protection – Édition entreprise

### PROOFPOINT USER PROTECTION

- Sensibilisation à la cybersécurité et modification des comportements
- Protection contre la prise de contrôle de comptes
- Protection des outils de collaboration et de messagerie

### PROOFPOINT IMPERSONATION PROTECTION

- Protection contre l'usurpation de domaines
- Relais de messagerie sécurisé
- Protection contre les menaces ciblant les fournisseurs
- Services de mise hors service des domaines malveillants

### PROOFPOINT CORE EMAIL PROTECTION

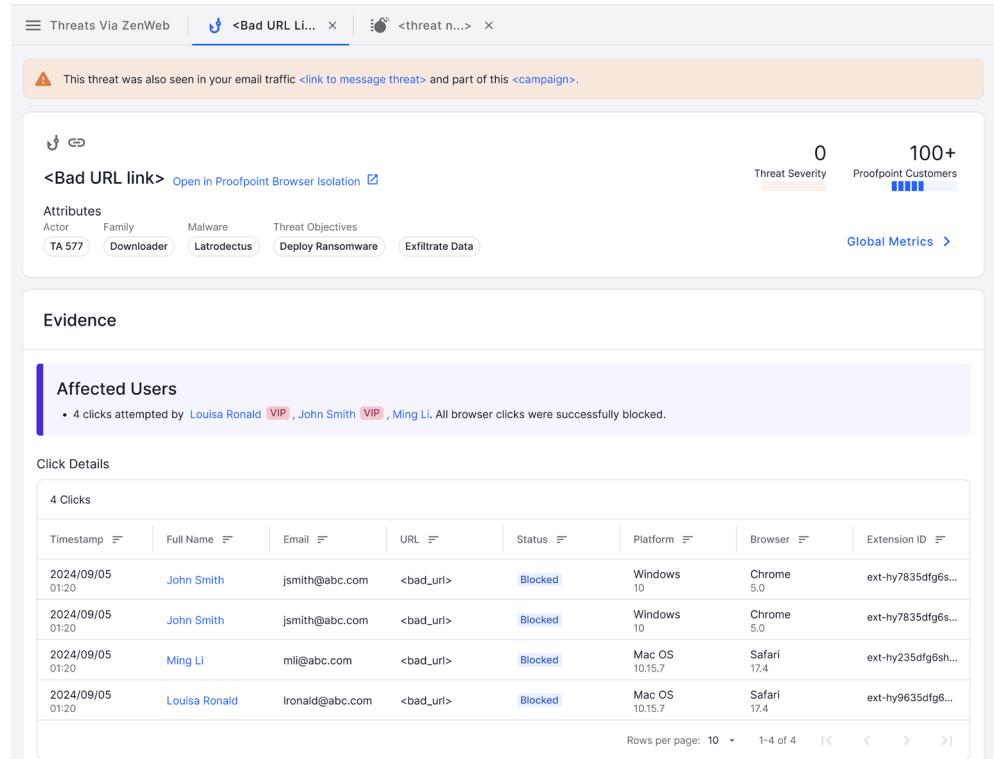
## Blocage des menaces ciblant la messagerie électronique et d'autres canaux numériques

Les collaborateurs n'ont jamais communiqué et collaboré aussi efficacement qu'aujourd'hui. Ils travaillent dans Microsoft Teams, Slack, des applications cloud, des services de partage de fichiers et plus encore. Si ces outils boostent la productivité des collaborateurs, ils élargissent également la surface d'attaque. Les cyberattaques centrées sur les personnes ne sont plus confinées à la messagerie électronique — et vos défenses ne devraient plus l'être non plus.

Proofpoint Prime protège votre espace de travail numérique tout entier. Que les menaces soient véhiculées par email, via des messages instantanés, sur les réseaux sociaux ou par le biais d'applications de collaboration, Proofpoint Prime offre une protection en temps réel contre un large éventail de menaces — piratage de la messagerie en entreprise (BEC, Business Email Compromise), ransomwares, spear phishing, etc.

Optimisé par la technologie Proofpoint Nexus® AI, Proofpoint Prime offre une protection inégalée contre les menaces avec une efficacité de 99,99 %. Il allie threat intelligence riche, modèles de langage avancés, graphiques relationnels, apprentissage automatique, analyse comportementale et vision par ordinateur. Toutes ces technologies fonctionnent de concert pour détecter et bloquer les menaces avant qu'elles ne provoquent des dégâts.

Grâce à sa vaste portée et à ses puissantes fonctionnalités d'IA, Proofpoint Prime protège vos collaborateurs — quels que soient leur lieu et leurs méthodes de travail.



The screenshot shows a threat detail page for a 'Bad URL link'. The top navigation bar includes 'Threats Via ZenWeb', '<Bad URL Li...>', and '<threat n...>'. A warning message states: '⚠ This threat was also seen in your email traffic <link to message threat> and part of this <campaign>.' The threat card displays the following details:

- Threat Type:** Bad URL link
- Open in Proofpoint Browser Isolation**
- Threat Severity:** 0 (0/100+)
- Proofpoint Customers:** 100+
- Global Metrics:** (button)

The 'Attributes' section shows:
 

- Actor: TA 577
- Family: Downloader
- Malware: Latroductus
- Threat Objectives: Deploy Ransomware, Exfiltrate Data

The 'Evidence' section includes a 'Affected Users' table with 4 rows, showing users Louisa Ronald, John Smith, Ming Li, and Ming Li. The 'Click Details' table shows 4 Clicks with the following data:

Timestamp	Full Name	Email	URL	Status	Platform	Browser	Extension ID
2024/09/05 01:20	John Smith	jsmith@abc.com	<bad_url>	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6s...
2024/09/05 01:20	John Smith	jsmith@abc.com	<bad_url>	Blocked	Windows 10	Chrome 5.0	ext-hy7835dfg6s...
2024/09/05 01:20	Ming Li	mli@abc.com	<bad_url>	Blocked	Mac OS 10.15.7	Safari 17.4	ext-hy235dfg6sh...
2024/09/05 01:20	Louisa Ronald	lronald@abc.com	<bad_url>	Blocked	Mac OS 10.15.7	Safari 17.4	ext-hy9635dfg6...

Page navigation: Rows per page: 10 | 1-4 of 4 | < > >>

**Figure 1.** Proofpoint étend la protection contre le phishing au-delà des emails. Il bloque également les URL malveillantes partagées via des plates-formes de messagerie, de collaboration et de communication.

## Défense contre les attaques en plusieurs phases

Les cybercriminels prennent le contrôle de comptes d'utilisateurs légitimes à l'aide d'une myriade de tactiques : phishing, attaques par force brute, piratage de session, ingénierie sociale, etc. Une fois qu'un compte est piraté, les cybercriminels élèvent souvent les priviléges, accèdent à vos données et s'implantent durablement. Même si vous avez mis en place une authentification multifacteur (MFA), vous n'êtes pas à l'abri des prises de contrôle de comptes (ATO).

Proofpoint Prime prévient les attaques ATO qui contournent la MFA. Il permet aux équipes de sécurité de détecter, d'analyser et de neutraliser rapidement les comptes compromis sur les plates-formes les plus populaires, comme Microsoft 365, Google Workspace et Okta.

Non seulement il offre une vue centralisée sur les activités des cyberpirates après la compromission, mais il prend également en charge diverses réponses automatisées. Les équipes ont la possibilité de suspendre automatiquement les comptes compromis, de forcer les réinitialisations de mots de passe, d'annuler des modifications non autorisées et de supprimer les applications tierces suspectes.

La solution vous protège également contre les attaques en plusieurs phases lancées par des cybercriminels utilisant des comptes de fournisseurs compromis. Proofpoint Prime détecte les comptes tiers potentiellement compromis dans l'ensemble de l'écosystème Proofpoint et avertit votre équipe de sécurité. Il permet également à votre équipe d'appliquer des contrôles de sécurité adaptatifs, tels que l'isolation des URL et l'affichage d'avertissements en cas d'emails suspects, sans bloquer les messages légitimes.

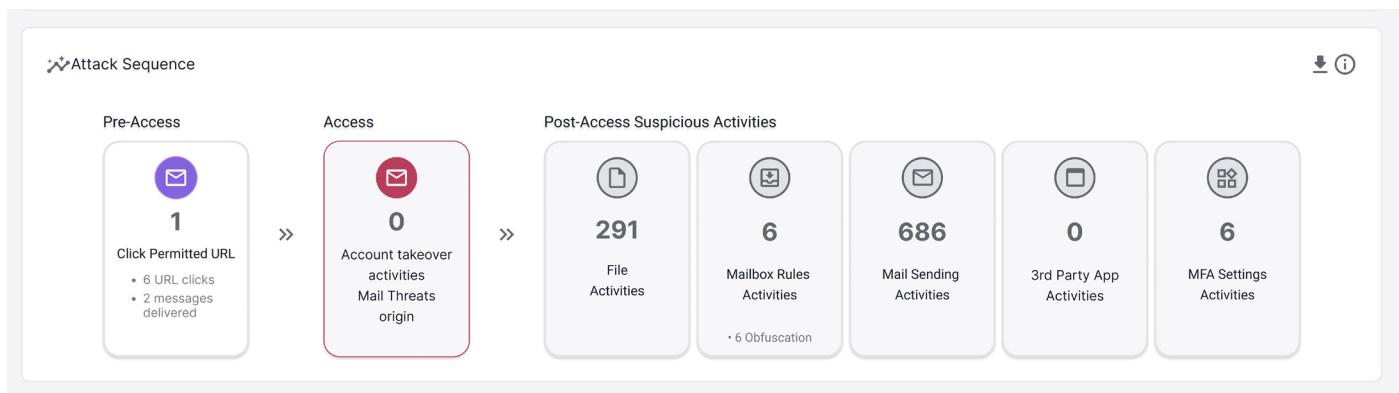


Figure 2. Proofpoint Prime affiche les activités malveillantes antérieures et postérieures à l'accès pour les comptes affectés.

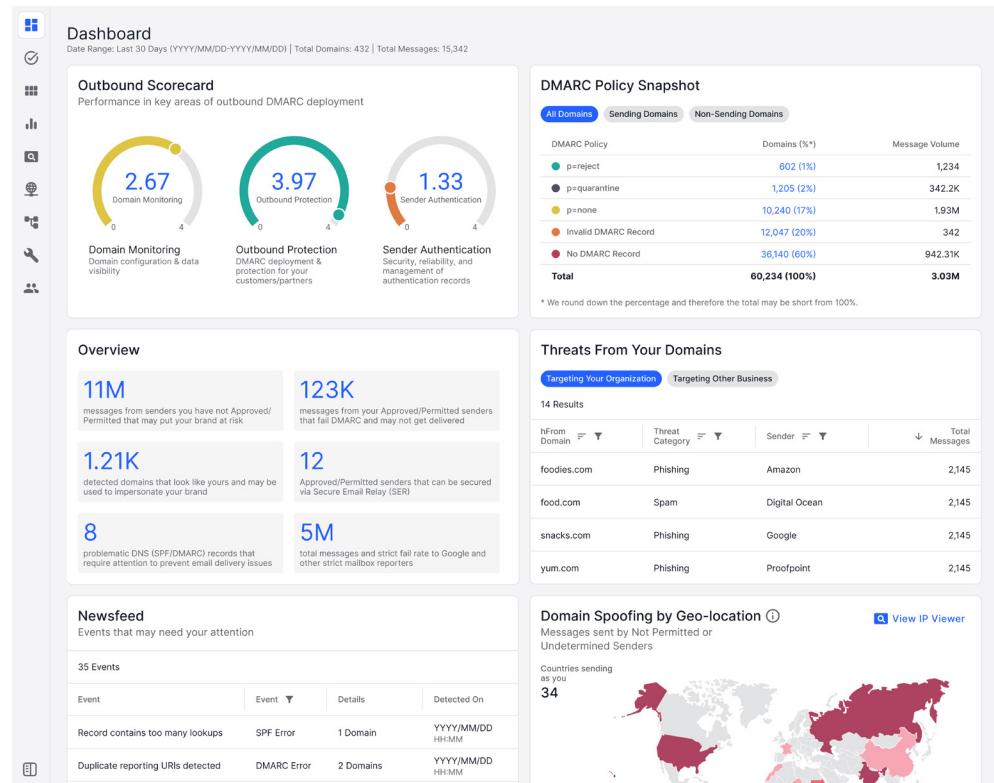
## Protection de vos communications d'entreprise de confiance

Les cyberpirates emploient souvent des tactiques d'usurpation d'identité pour s'immiscer dans des communications d'entreprise de confiance. L'usurpation de l'identité de votre entreprise — que ce soit par le biais de l'usurpation directe de domaines ou de l'enregistrement de domaines imitant les vôtres — met en danger vos collaborateurs, clients et partenaires et peut être très dommageable pour votre marque.

Proofpoint Prime peut vous aider à réduire ces risques d'usurpation d'identité de façon proactive. Il vous offre une visibilité complète sur tous les emails sortants envoyés depuis vos domaines de confiance, y compris par des tiers. Vous avez accès à des outils puissants ainsi qu'à des consultants experts qui vous guideront à chaque étape de votre déploiement de l'authentification des emails.

Vous pourrez ainsi assurer votre conformité DMARC et empêcher les cybercriminels d'usurper vos domaines. Notre protection s'étend au-delà des emails générés par les utilisateurs de sorte à inclure un environnement dédié sécurisé pour relayer les messages générés par les applications et les emails envoyés par des fournisseurs SaaS tiers en votre nom.

Proofpoint Prime propose également des fonctionnalités avancées de détection de domaines similaires. Il surveille Internet de façon dynamique à la recherche de domaines qui ressemblent beaucoup aux vôtres et fournit des informations détaillées sur leur enregistrement et leur potentielle utilisation inappropriée. Et nous ne nous arrêtons pas à la détection — nous pouvons mettre hors service les URL et domaines malveillants en votre nom grâce aux relations étroites que nous entretenons avec des bureaux d'enregistrement, des hébergeurs et des fournisseurs de domaines de premier niveau. Nos professionnels gèrent le processus de bout en bout, afin que vos équipes puissent se concentrer sur votre cœur de métier.



**Figure 3.** Proofpoint Prime vous offre une visibilité sur les menaces d'usurpation de domaines, les domaines malveillants imitant les vôtres et les emails envoyés à l'aide de vos domaines de confiance.

## Renforcement de la résilience grâce à des informations et à des conseils basés sur les risques

Les cybercriminels ciblent les personnes. Malheureusement, une formation annuelle en cybersécurité ne suffit pas à améliorer votre niveau global de sécurité contre leurs tactiques en constante évolution.

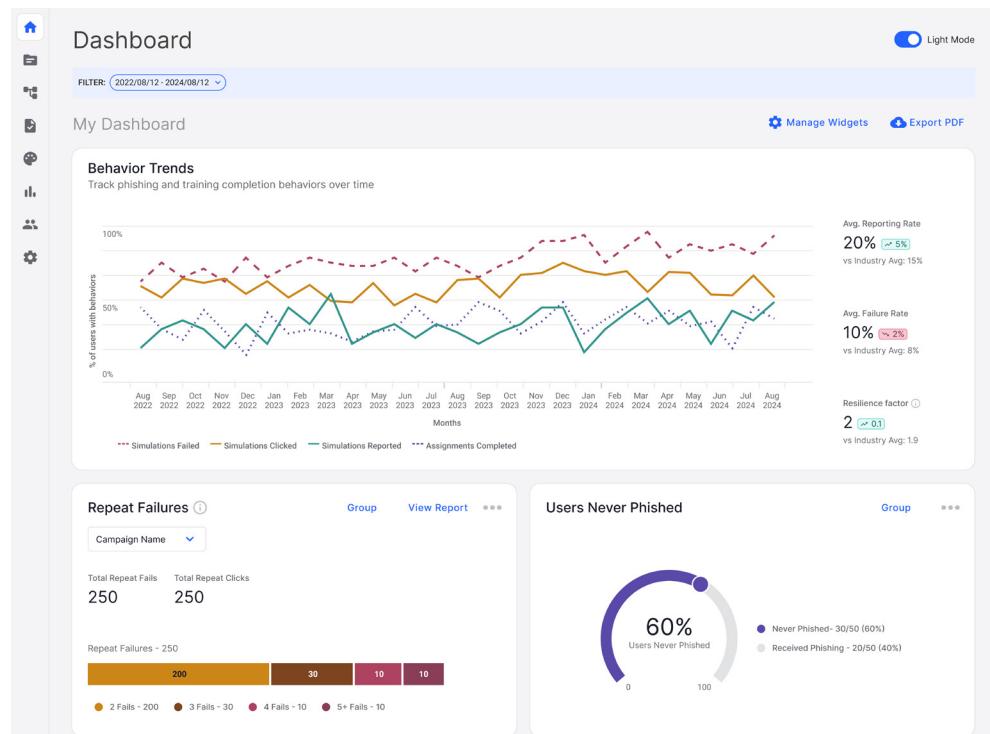
Proofpoint Prime fournit des conseils et des informations sur les risques liés aux utilisateurs qui favorisent un changement significatif des comportements et une résilience humaine durable. Il s'appuie sur un apprentissage adaptatif basé sur les risques qui va plus loin que les approches traditionnelles, ce qui le rend bien plus efficace que les méthodes universelles.

Proofpoint Prime aide les entreprises à mesurer les risques liés aux utilisateurs et à identifier les collaborateurs à haut risque en agrégeant des informations issues de l'ensemble de l'écosystème Proofpoint. Grâce à la fonctionnalité de parcours d'apprentissage adaptatif, Proofpoint permet aux équipes d'attribuer automatiquement des expériences d'apprentissage personnalisées

aux utilisateurs à risque en fonction de leur comportement, de leur exposition aux menaces, de leur rôle, de leurs compétences en sécurité et de leurs priviléges métier.

Par exemple, un VAP (Very Attacked Person, ou personne très attaquée) peut se voir attribuer automatiquement des activités ciblées — comme des formations, des notifications et des simulations d'attaques de phishing — en fonction des types de menaces spécifiques qui le ciblent. Les équipes de sécurité peuvent ainsi proposer des contenus axés sur les menaces plus pertinents, favoriser un engagement significatif et adapter les efforts de changement des comportements plus efficacement au sein de l'entreprise.

À mesure que vos collaborateurs deviennent plus résilients face aux menaces en perpétuelle mutation, vous réduisez votre exposition globale aux risques et votre personnel devient une ligne de défense essentielle. Avec Proofpoint Prime, vous pouvez mesurer l'impact de votre programme de renforcement de la résilience humaine et évaluer précisément la réduction des risques liés aux utilisateurs. Vous pouvez ainsi démontrer l'efficacité de votre programme, ce qui vous permet d'obtenir plus facilement le soutien de votre direction et des parties prenantes.

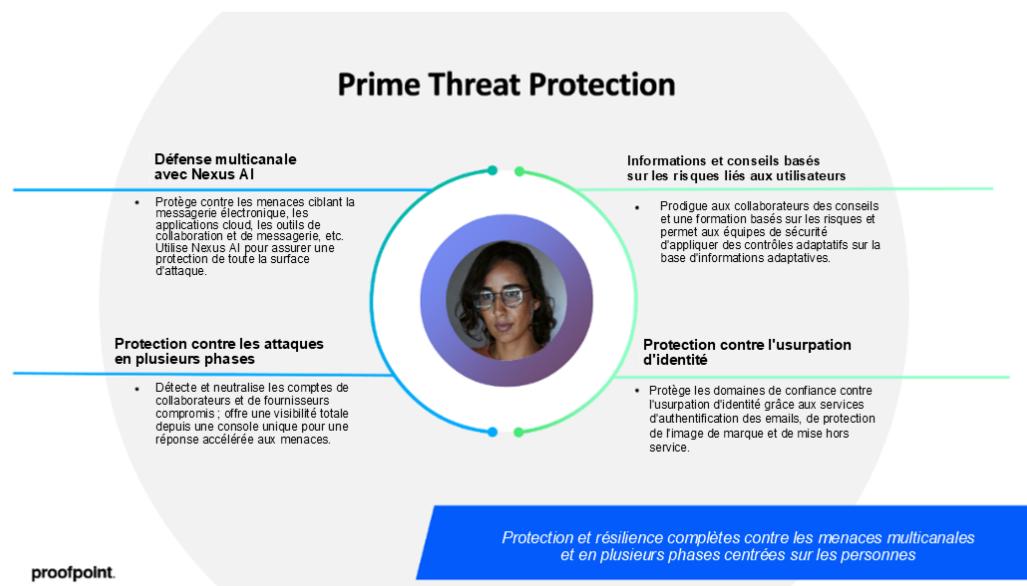


**Figure 4.** Nourri par la threat intelligence mondiale de Proofpoint, Proofpoint Prime vous fournit des informations sur le paysage des menaces en perpétuelle mutation. Vous pouvez guider et former vos utilisateurs aux nouvelles menaces tout en capturant les tendances comportementales au fil du temps.

## Exploitation des avantages d'une protection intégrée

Il est de plus en plus difficile de protéger les environnements de travail numériques contre les cybermenaces. Une combinaison de produits isolés et cloisonnés ne suffit pas et néglige de nombreux risques. Cela entraîne des problèmes d'intégration, une gestion complexe, des dépenses excessives et des coûts opérationnels élevés.

Proofpoint Prime résout ces problèmes grâce à une approche complète de la défense contre les menaces, qui élimine les failles de sécurité et réduit la complexité associée à des solutions fragmentées et isolées. Notre protection intégrée contre les menaces permet à votre équipe d'intervenir plus rapidement et plus efficacement grâce à des workflows automatisés, à une threat intelligence partagée et à des intégrations préconfigurées. Qui plus est, Proofpoint Prime réduit les coûts de licence, ce qui vous permet de diminuer vos frais opérationnels et d'améliorer votre retour sur investissement. Cerise sur le gâteau, vous bénéficiez d'un partenaire de confiance à la pointe du secteur.



# 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](http://www.proofpoint.com/fr).

Suivez-nous : [X](#) | [LinkedIn](#) | [Facebook](#) | [YouTube](#)

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 →**