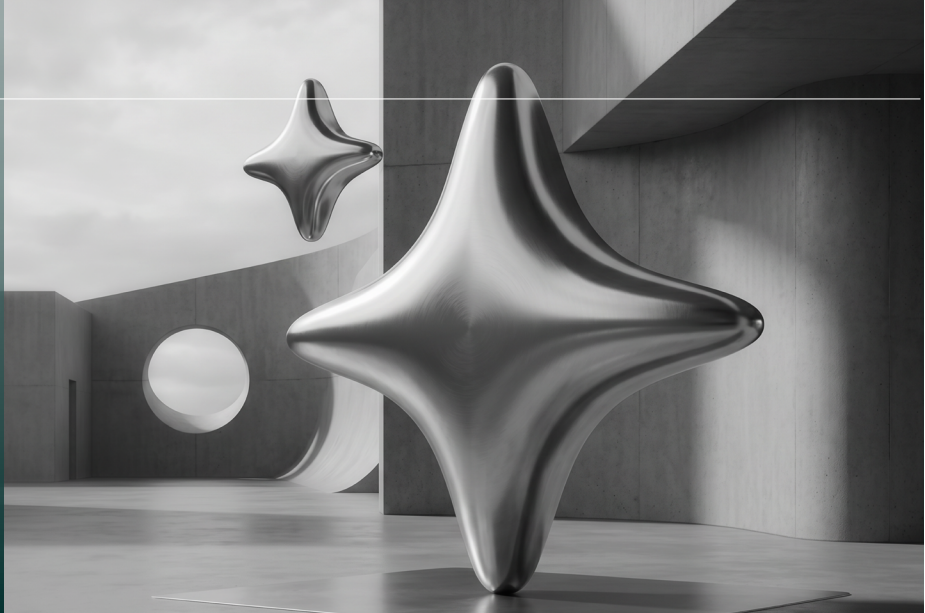


L'IA chez Proofpoint



L'IA offre des solutions nouvelles et innovantes pour aider les collaborateurs à accomplir leur travail. Mais dans le même temps, elle aide également les cybercriminels à accroître leur propre productivité. Les tactiques, techniques et procédures (TTP) de ces derniers sont désormais renforcées par l'IA, ce qui leur permet de mener des attaques en plusieurs phases et sur plusieurs canaux à l'échelle mondiale. Ces menaces contournent souvent les dispositifs de sécurité traditionnels et sont plus difficiles à détecter par les utilisateurs.

Cependant, les risques ne sont pas uniquement le fruit d'attaques externes. Les expositions de données trouvent de plus en plus leur origine dans le comportement quotidien des utilisateurs au

sein même de l'entreprise. L'IA peut aider à surveiller le flux de données et à identifier les comportements à risque en contexte. Cela peut réduire considérablement le fardeau qui pèse sur les équipes des centres d'opérations de sécurité (SOC).

Alors que les répercussions de l'IA sur le monde du travail ne cessent d'évoluer, Proofpoint se positionne à l'avant-garde du secteur en matière d'utilisation de l'IA pour protéger ses clients. En combinant innovation continue fondée sur l'IA et threat intelligence inégalée, nos solutions prennent le pas sur les cybercriminels, protègent les données sensibles et aident les entreprises à rester en sécurité dans un monde de plus en plus axé sur l'IA.

Comment les cybercriminels utilisent l'IA pour intensifier leurs attaques

Proofpoint a pu observer de ses propres yeux les conséquences de l'IA lorsqu'elle est utilisée par les cybercriminels. En 2025, Proofpoint a observé une hausse de 94 % du nombre de menaces par email ciblant les clients par rapport à l'année précédente. Cela conduit à un paysage des menaces plus sophistiqué qui inclut l'injection de requêtes d'IA, l'envoi en masse d'emails et les attaques par détournement de services légitimes.

Les cybercriminels exploitent l'IA pour gagner du terrain de plusieurs façons :

- **Multiplicateur de force.** L'IA permet aux cybercriminels de mener des attaques plus sophistiquées sur une surface plus large. Cette année, nous avons recensé des milliers d'emails visant à amener des agents d'IA à agir pour le compte du cybercriminel.
- **Barrière à l'entrée réduite.** L'IA permet d'automatiser 80 à 90 % de la chaîne d'attaque. Les cybercriminels ont ainsi plus de temps pour se consacrer à des attaques

plus complexes. Nous avons observé une hausse des attaques en plusieurs étapes et sur plusieurs canaux, impliquant des milliers de messages indésirables.

- **Ciblage avancé.** Avant l'avènement de l'IA, les cybercriminels s'appuyaient sur des modèles génériques et prévisibles pour mener leurs attaques. Avec l'IA, ils peuvent créer des attaques personnalisées pour chaque victime.

Cette année, nous avons observé une augmentation des attaques personnalisées détournant des services légitimes.

Toutes ces évolutions ont compliqué l'identification précise des menaces par email.

L'analyse sémantique et d'autres méthodes basées sur les grands modèles de langage peuvent s'avérer utiles.

En 2025, Proofpoint a observé une hausse de

94%

du nombre de menaces par email ciblant les clients par rapport à l'année précédente.

Proofpoint Nexus AI pour sécuriser la collaboration

Les solutions Proofpoint Collaboration Security Prime s'appuient sur notre plate-forme Nexus™ AI, qui utilise une approche multicouche de la détection des menaces.

Comment les cybercriminels utilisent l'IA pour intensifier leurs attaques

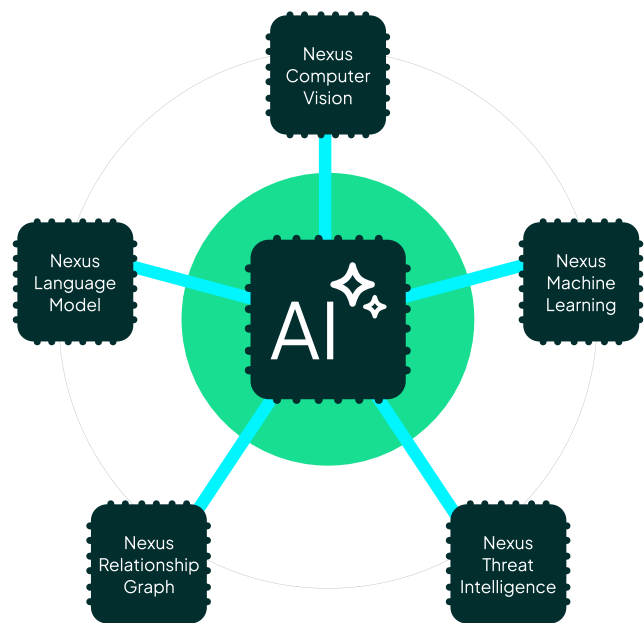
Proofpoint Nexus consiste en un ensemble de moteurs optimisés par l'IA qui fonctionnent de concert pour offrir une efficacité de détection de 99,999 %. Il combine apprentissage automatique, vision par ordinateur, graphiques des relations, threat intelligence et modèles de langage pour détecter et bloquer les attaques avec précision.

Les modèles Proofpoint Nexus AI traitent **2,1 billions d'emails** par an, avec le soutien d'une équipe de threat intelligence qui suit plus de **100 groupes cybercriminels uniques** et plus de **8 900 campagnes de menaces**.

Nexus LM™ (Language Model) détecte les attaques BEC et les menaces de phishing sophistiquées, en s'appuyant sur une analyse avancée du langage (notamment le langage transactionnel, le sentiment d'urgence, le contexte et l'intention) pour mettre au jour les menaces dissimulées et les risques inconnus pesant sur les données.

Nexus RG™ (Relationship Graph) identifie les changements subtils de comportement dans les communications de vos utilisateurs, en détectant les écarts par rapport au comportement habituel, les variations de volume et le partage de données d'entreprise sensibles afin de réduire les risques de fuite de données, et vous protège contre les cyberrisques liés au comportement.

Nexus TI™ (Threat Intelligence) analyse les tactiques des cybercriminels et protège de manière proactive contre les nouvelles cybermenaces en exploitant des données en temps réel pour identifier les nouvelles tactiques des cyberpirates et les vulnérabilités système, ainsi que déclencher une émulation en sandbox pour les URL et les pièces jointes suspectes.



Nexus CV™ (Computer Vision) identifie et neutralise les menaces basées sur la vision. Grâce à une technologie de vision par ordinateur avancée, Nexus CV détecte les menaces cachées dans des éléments visuels, comme les sites de phishing, les codes QR, les pièces jointes malveillantes et les emails falsifiés.

Nexus ML™ (Machine Learning) utilise des techniques d'apprentissage dynamiques et adaptatives, telles que l'apprentissage supervisé, l'apprentissage non supervisé et les méthodes d'ensemble. Il combine ces techniques avec des capacités de détection prédictive des menaces permettant de cartographier les comportements d'attaque connus, ainsi qu'avec des techniques non supervisées pour détecter les anomalies inconnues.

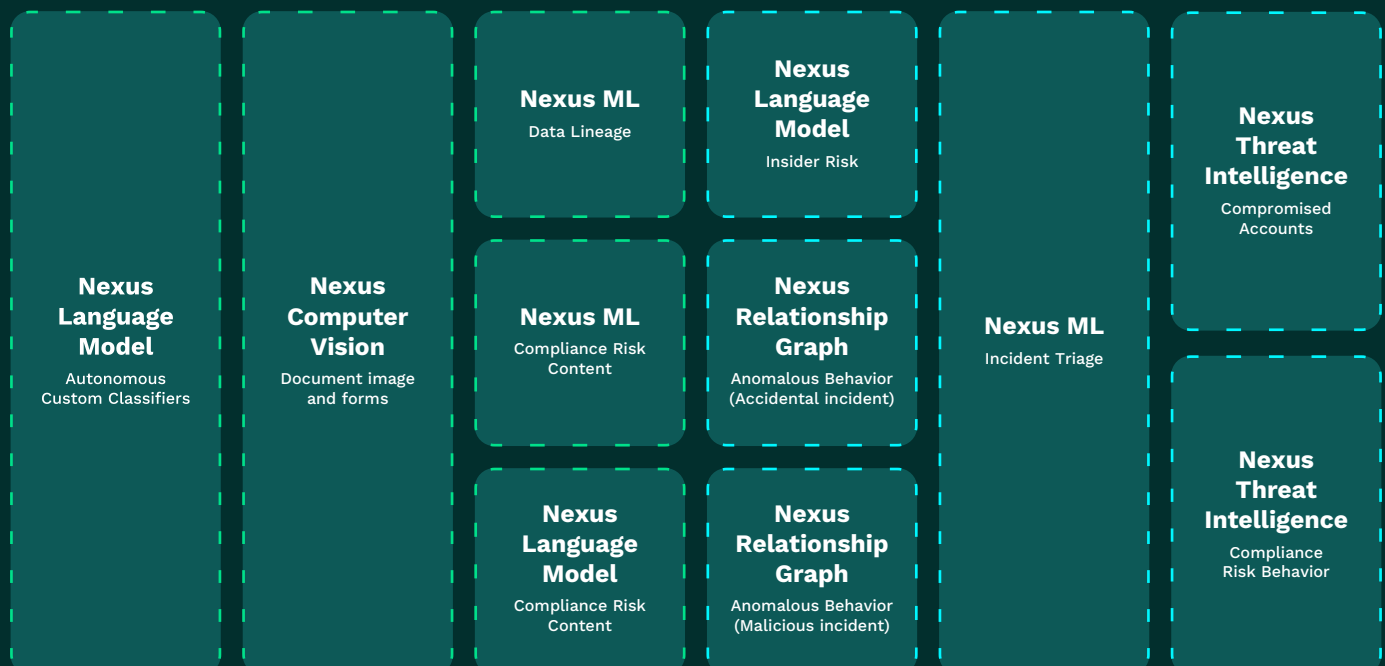
Proofpoint Nexus AI pour la sécurité et la gouvernance des données

Proofpoint utilise les mêmes moteurs Nexus performants et à la pointe du marché pour optimiser ses solutions de sécurité et gouvernance des données.

L'IA pour prévenir les fuites de données

Proofpoint Nexus classe et suit le parcours des données ainsi que leur flux. Peu importe que les destinataires fassent partie de l'entreprise ou soient à l'extérieur.

- **Nexus LM™ (Language Model)** apprend à identifier les types de documents professionnels utilisés au sein de votre entreprise, tels que les documents de négociation, les prévisions ou les conceptions produits. Il transforme ces classes apprises en un contexte de règles exploitables permettant de détecter, de prioriser et de protéger rapidement les données sensibles sans intervention manuelle.
- **Nexus RG™ (Relationship Graph)** analyse les relations entre les données afin de prévenir les fuites de données accidentelles ou intentionnelles résultant d'emails adressés au mauvais destinataire ou de scénarios d'exfiltration de données.
- **Nexus TI™ (Threat Intelligence)** protège contre les comptes compromis qui envoient des emails de phishing, tant en interne qu'en externe.
- **Nexus CV™ (Computer Vision)** détecte les contenus sensibles présents dans les images intégrées aux emails et aux documents.
- **Nexus ML™ (Machine Learning)** offre une visibilité de bout en bout sur la manière dont les fichiers sont créés, copiés, renommés, partagés et déplacés entre les référentiels et les destinations. Il relie cette activité à un historique traçable qui permet



L'IA agentique chez Proofpoint

L'IA CHEZ PROOFPOINT | FICHE SOLUTION

En matière d'environnement de travail basé sur l'IA agentique, Proofpoint investit dans deux domaines clés.

1. Proofpoint Satori™ Agents

Nous développons des agents d'IA destinés à être intégrés aux solutions Proofpoint existantes. Les Proofpoint Satori Agents automatisent les tâches et réduisent la charge de travail manuelle de vos équipes SOC.

- **Abuse Mailbox Agent** automatise la vérification manuelle des messages signalés. Il allège ainsi la charge de travail des SOC chargés de distinguer les menaces réelles des emails inoffensifs.



- **DLP Triage Agent** gère les alertes et la surveillance des activités de votre solution de prévention des fuites de données (DLP).
- **Phishing Simulation Agent** utilise l'automatisation basée sur l'IA pour mettre en œuvre vos programmes de sensibilisation à la sécurité informatique et renforcer la résilience humaine.

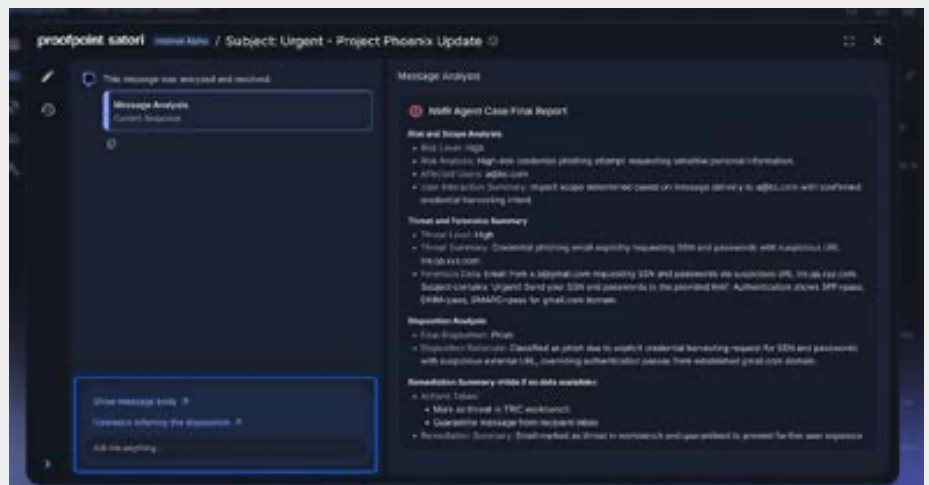


Figure 2. Proofpoint Satori Abuse Mailbox Agent en action

2. Proofpoint AI Security

Nous sommes conscients des risques pour la sécurité introduits par l'adoption rapide de l'IA par les utilisateurs, les agents et les systèmes d'entreprise. C'est pourquoi nous avons élargi notre plate-forme Human-Centric Security pour qu'elle assure la gouvernance et la sécurité de l'intégralité de l'espace de travail agentique.

Proofpoint AI Security unifie la visibilité, le contrôle et la protection de toutes les interactions avec l'IA – garantissant ainsi une utilisation sécurisée et conforme des technologies d'IA.

- **Sécurise les interactions des utilisateurs, des agents et des systèmes avec l'IA** à l'échelle de l'entreprise
- **Offre une visibilité et une gouvernance de bout en bout** sur l'utilisation de l'IA, les agents et les interactions avec les modèles
- **Prévient les fuites de données, l'utilisation abusive d'outils et les autorisations d'accès excessives** dans les workflows d'IA

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 en toute confiance. Pour en savoir plus, consultez le site 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.