proofpoint.

L'IA chez Proofpoint

L'IA offre des solutions nouvelles et innovantes pour aider les gens dans le cadre de 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. C'est là que l'IA peut s'avérer utile. Elle permet de surveiller les flux de données et d'identifier les comportements à risque en contexte, ce qui allège considérablement la charge de travail des équipes des centres des 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.

94 %

Proofpoint a constaté une augmentation de 94 % des menaces par email ciblant ses clients en 2025.

Comment les cybercriminels utilisent l'IA pour

Proofpoint a pu observer de ses propres yeux les conséquences de l'IA lorsqu'elle est utilisée par les cybercriminels. En 2025, Proofpoint a constaté une augmentation de 94 % du nombre de menaces par email ciblant ses clients par rapport à l'année précédente. Cela se traduit par un paysage des menaces plus sophistiqué, avec notamment l'injection d'invites, l'envoi d'emails en masse et des 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. Grâce à l'IA, ils peuvent désormais personnaliser leurs attaques en fonction de chaque victime. Cette année, nous avons constaté une recrudescence des attaques personnalisées qui exploitent 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.

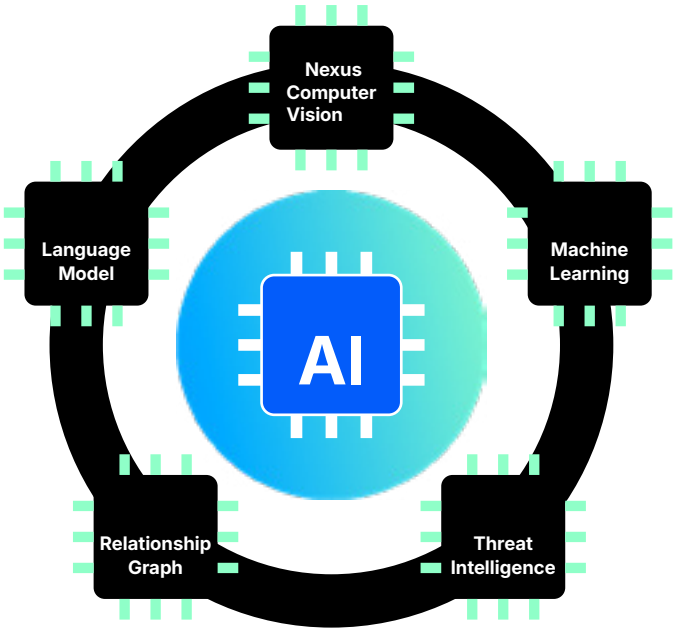
Proofpoint Nexus AI pour sécuriser la collaboration

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

L'IA pour détecter et bloquer les menaces

Proofpoint Nexus est 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 2,3 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 8 400 campagnes de menaces actives.



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 comportementaux subtils 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 le risque d' attaques basées sur le 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

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 d'accélérer les enquêtes, de mettre en place des contrôles basés sur l'origine et de fournir des preuves prêtes à être présentées lors d'audits pour les programmes de protection des données.

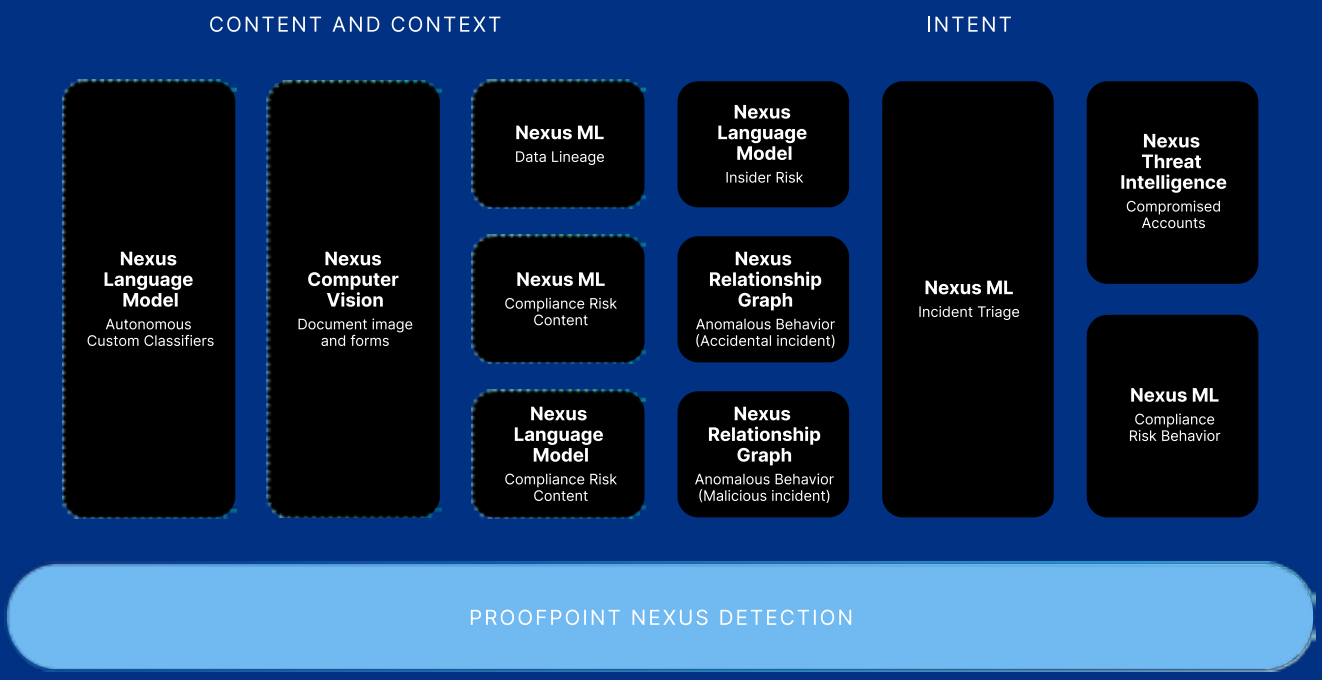


Figure 1. Nexus optimise les solutions de sécurité et de gouvernance des données.

L'IA agentique chez Proofpoint

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.

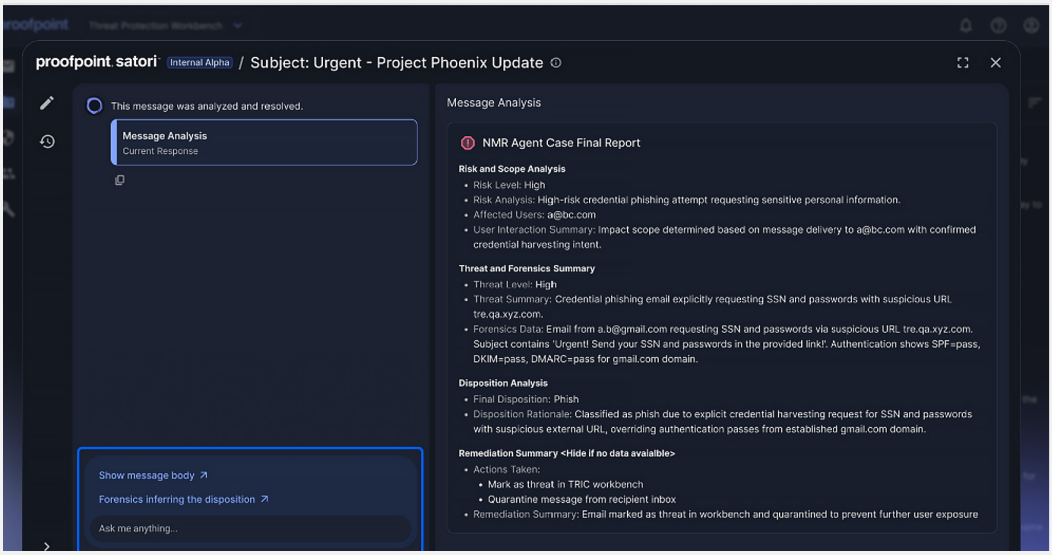


Figure 2. Proofpoint Satori Abuse Mailbox Agent en action

2. Proofpoint Secure Agent Gateway

Nous sommes conscients des failles de sécurité inhérentes à la mise en œuvre de workflows d'IA agentique au sein de votre entreprise. C'est pourquoi nous étendons notre plate-forme Human-Centric Security afin de protéger également tous vos agents.

Proofpoint Secure Agent Gateway sécurise les workflows agentiques existants et unifie les contrôles agentiques de l'ensemble des agents de votre environnement.

- **Sécurise les flux d'informations sensibles** entrant et sortant de chaque workflow agentique
- **Est optimisé par notre technologie MCP (Model Context Protocol)**
- **Contrôle l'accès aux données sensibles** utilisées par les agents