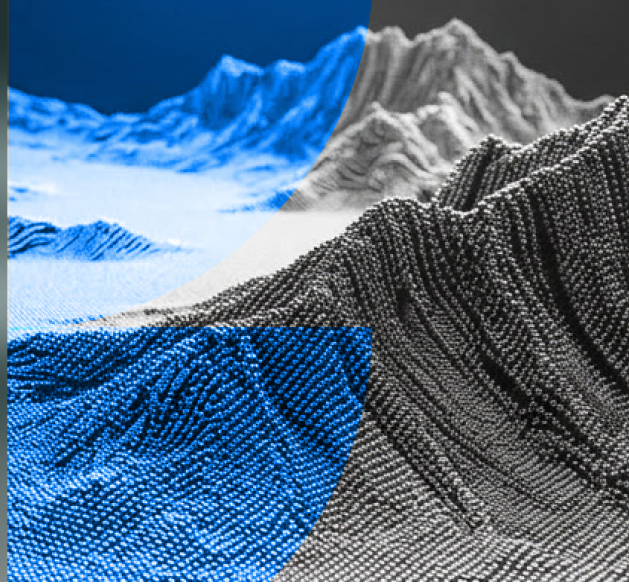
proofpoint

FICHE SOLUTION

Proofpoint Core Email Protection

Bloquez les menaces par email optimisées par l'IA grâce à une protection complète et continue tout au long du cycle de vie des emails



Principaux avantages

- **Blocage des menaces par email optimisées par l'IA avant la remise**
- **Détection des menaces avec un taux d'efficacité de 99,999 %**
- **Déploiement en 24 heures via une API ou une passerelle de messagerie sécurisée (SEG)**
- **Couverture complète avant la remise, après la remise et au moment du clic**
- **Threat Protection Workbench unifié permettant d'accélérer les investigations**
- **Intégrations avec des écosystèmes de premier ordre**

Le défi : les menaces par email optimisées par l'IA

Les cybercriminels lancent des attaques à la vitesse des machines. L'IA de pointe a supprimé les contraintes qui limitaient autrefois la vitesse avec laquelle les cybercriminels pouvaient élaborer des leurres de phishing, des attaques BEC (Business Email Compromise) et des campagnes d'ingénierie sociale. Une seule campagne génère désormais une infinité de variantes hautement ciblées et personnalisées pour chaque destinataire.

Ces menaces générées par l'IA arrivent via la messagerie électronique et les canaux de collaboration sans fautes de frappe, sans modèles réutilisés et sans empreintes familières. Les défenses traditionnelles basées sur des listes de réputation et des signatures statiques ne peuvent pas suivre le rythme. Dans le même temps, 94 % des cyberattaques ciblant les personnes commencent toujours par un email[1].

Ces attaques exploitent des failles de sécurité : protections avant la remise manquantes, angles morts dans la détection des compromissions de fournisseurs, environnements cloud et de collaboration cloisonnés et absence de contrôles visant à empêcher les prises de contrôle de comptes.

L'IA en tant que multiplicateur de force

Des tâches qui prenaient autrefois 16 heures à un cybercriminel ne lui demandent plus que 5 minutes. Le phishing généré par l'IA produit des leurres parfaits et personnalisés, sans erreurs révélatrices.

Infinité de variantes
Tous les leurres sont différents

Vitesse des machines
Création de campagnes en quelques minutes

Multicanal
Email, voix et vidéos

[1] Source : recherches sur les menaces menées par Proofpoint

La solution : Proofpoint Core Email Protection

Proofpoint Core Email Protection bloque un large éventail de menaces par email optimisées par l'IA grâce à une protection complète et continue couvrant l'intégralité du cycle de vie des emails. Il se déploie via une passerelle de messagerie sécurisée ou une API pour vous offrir une efficacité de détection des menaces sans égal au sein du secteur, de 99,999 %.

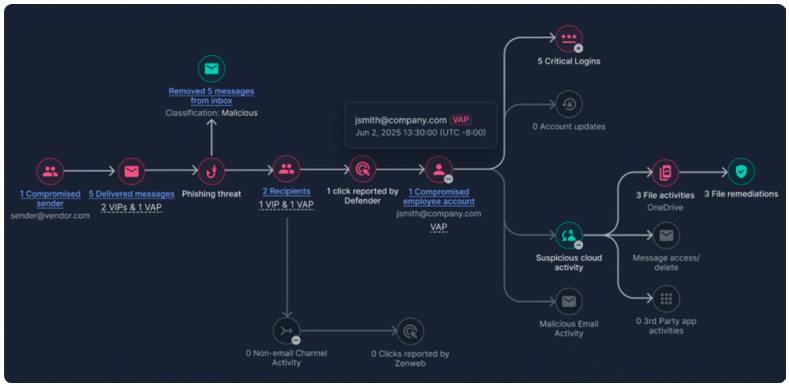


Figure 1. Threat Protection Workbench cartographie les menaces de bout en bout.

Fonctions essentielles :

Détection optimisée par Proofpoint Nexus AI

Proofpoint Nexus utilise des modèles de langage, des graphiques relationnels, l'apprentissage automatique, la threat intelligence et la vision par ordinateur pour détecter un large éventail de menaces par email avancées grâce à des détections basées sur l'intention de l'IA.

Proofpoint Nexus AI

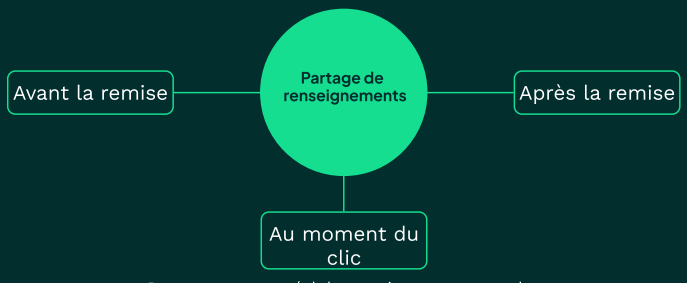
- **LM** — Language Model
- **RG** — Relationship Graph
- **ML** — Machine Learning
- **TI** — Threat Intelligence
- **CV** — Computer Vision

Données inégalées sur les menaces

2,1 Bio	20,4 Bio	8 900	>100
d'emails	d'URL	campagnes	acteurs

Protection complète et continue

Proofpoint Core Email Protection propose une défense coordonnée avant la remise, après la remise et au moment du clic. Les renseignements sont partagés en temps réel entre les contrôles, de sorte qu'une menace détectée après la remise permet d'affiner la décision suivante prise avant la remise.



Partage en temps réel de renseignements entre les contrôles

Modules complémentaires :

- Prise de contrôle de comptes
- Messagerie
- Fournisseur
- Heure de connexion

Déploiement unifié basé sur SEG et API

Proofpoint unifie ses déploiements de pointe basés sur des SEG et des API au sein d'une architecture unique et intégrée. Notre SEG aide à bloquer les menaces entrantes et sortantes au niveau de la passerelle de messagerie, tandis que notre protection basée sur API étend la visibilité et la réponse aux menaces par email internes et après la remise.

Une console, un workflow d'investigation et un ensemble de règles uniques remplacent la fragmentation opérationnelle associée à la gestion d'outils distincts. Les entreprises qui optent pour le déploiement via une API peuvent effectuer celui-ci en seulement 24 heures. Elles peuvent aussi choisir de combiner SEG et API pour une couverture maximale.

Une sécurité opérationnelle efficace

Avec 99,999 % des menaces bloquées automatiquement, les équipes de sécurité peuvent se concentrer sur les investigations prioritaires. Threat Protection Workbench propose une reconstitution visuelle, de bout en bout, de la chaîne d'attaque, en reliant les messages, les utilisateurs, les clics et les mesures correctives dans une vue unique. Les workflows automatisés, la recherche intégrée et le tri basé sur les alertes réduisent le temps moyen de correction.

Impact opérationnel

Voici ce à quoi vous pouvez vous attendre avec Proofpoint

Efficacité de la détection sans précédent

Efficacité en matière de détection des menaces de 99,999 %, avec seulement un faux positif pour 19,7 millions de messages et un faux négatif pour 5,3 millions de messages.

Réduction du délai de rentabilisation

Les déploiements via une API sont opérationnels en 24 heures. Les déploiements combinant SEG et API assurent une défense en profondeur.

Réduction de la charge de travail du SOC

Les workflows automatisés et les investigations visuelles de la chaîne d'attaque réduisent le temps que les analystes consacrent à la corrélation manuelle.

Couverture étendue des menaces

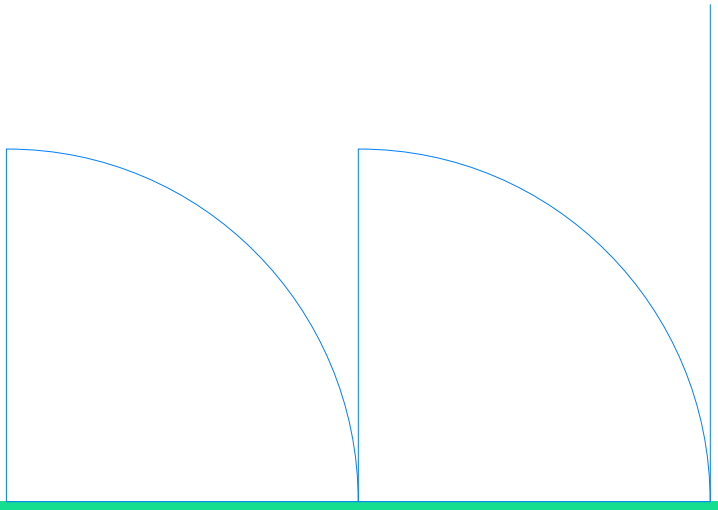
Bénéficiez d'une protection contre les menaces externes, les compromissions après la remise, le phishing interne et les envois directs.

Architecture pérenne

Une plate-forme intégrée offre une protection automatique contre les nouvelles menaces détectées et les cybercriminels émergents.

Intégrations de premier plan

Intégrations avec les écosystèmes CrowdStrike, Okta, Palo Alto Networks, Microsoft Defender, Splunk et Sentinel.



Visitez le site **proofpoint.com/fr** pour en savoir plus

proofpoint.