HORNETSECURITY
BY proofpoint

IA & CYBERSÉCURITÉ

LES HACKERS ONT-ILS PRIS L'AVANTAGE ?

RAPPORT 2026

Basé sur l'étude OpinionWay pour Hornetsecurity by Proofpoint



HORNETSECURITY
BY proofpoint.

INTRODUCTION

L'étude **« Cybersécurité & IA » menée par OpinionWay pour Hornetsecurity by Proofpoint** révèle une évolution majeure du paysage cyber français : l'IA renforce les capacités des cybercriminels et accroît la crédibilité des attaques.

Aujourd'hui, **38 % des décideurs cyber estiment que l'IA favorise avant tout les attaquants**, tandis que seuls 17 % considèrent qu'elle améliore la sécurité des entreprises.

Face à cette accélération des menaces, les entreprises réagissent : **85 % intègrent déjà l'IA dans leur cybersécurité** et **68 % prévoient d'en faire une priorité d'investissement dans les 12 à 24 prochains mois**.

Le défi est désormais clair : **renforcer les défenses, sensibiliser les équipes** et **investir dans les bons outils pour garder une longueur d'avance**.



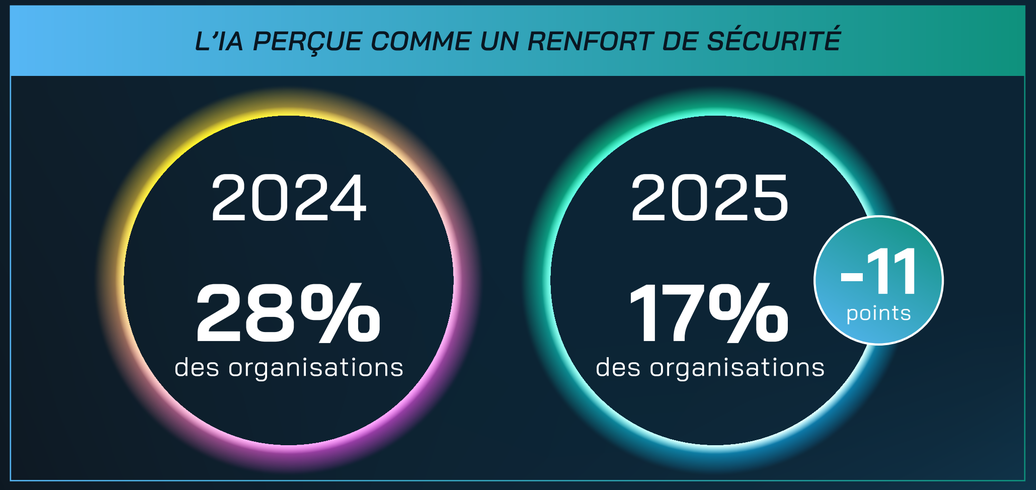
HORNETSECURITY
BY proofpoint.

CONSTATS CLÉS **À RETENIR**

1. LE RAPPORT DE FORCE BASCULE EN FAVEUR DES ATTAQUANTS

L'IA est de plus en plus perçue comme un avantage pour les cybercriminels.





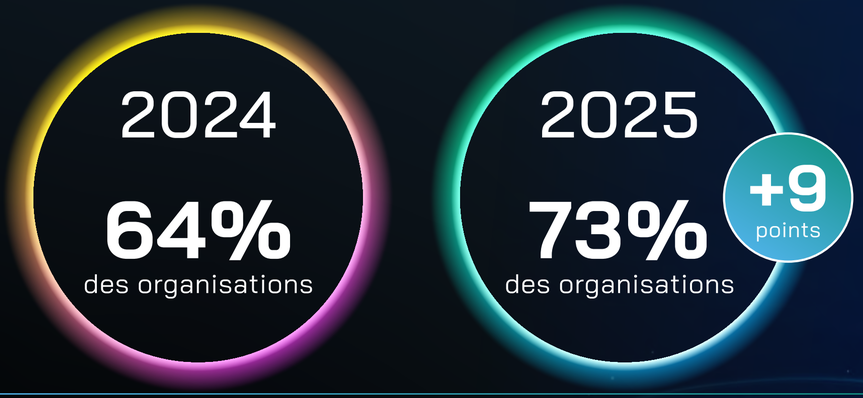
Ce basculement est particulièrement marqué chez les TPE : 40 % des décideurs de TPE confirment ce constat, soit +10 points comparé à 2024.

HORNETSECURITY
BY proofpoint.

2. L'IA REND LES CYBERATTAQUES PLUS COMPLEXES

De plus, pour certaines organisations l'IA complexifie de manière claire les attaques existantes, en les rendant plus difficiles à contrer.

L'IA PERÇUE COMME UN OUTIL COMPLEXIFIANT DES ATTAQUES EXISTANTES



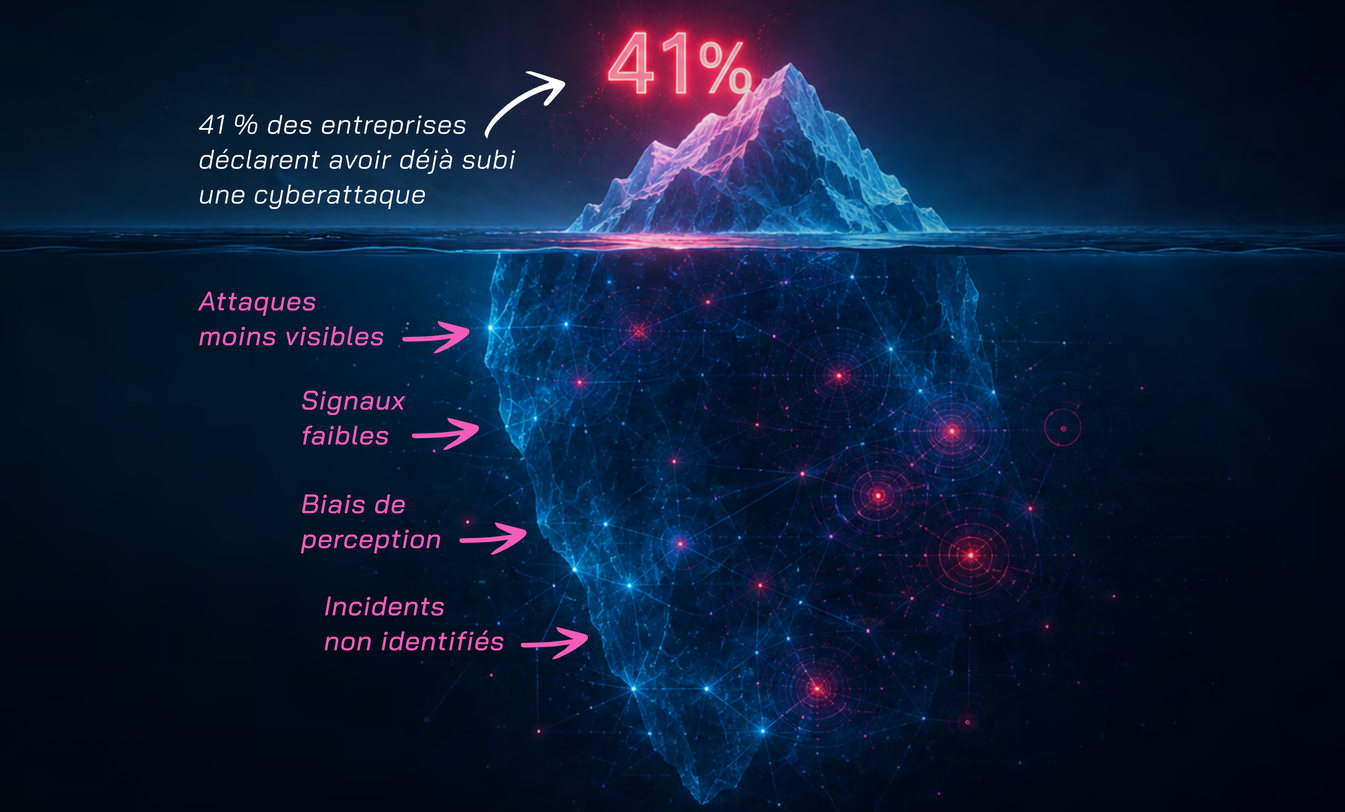
Les cybercriminels peuvent désormais produire des messages plus crédibles, plus personnalisés et automatisés en masse. L'IA ne crée pas forcément de nouveaux vecteurs d'attaque, mais elle rend les attaques existantes plus difficiles à détecter et plus convaincantes.



HORNETSECURITY
BY proofpoint.

3. LES CYBERATTAQUES RESTENT UNE RÉALITÉ, MÊME SI LA PERCEPTION BAISSE

En effet, cette baisse déclarative ne signifie pas nécessairement que le risque diminue. Au contraire, l'analyse indique que cela peut cacher des attaques plus complexes, donc plus difficiles à identifier, ou un biais de perception lié à des incidents majeurs très médiatisés.



4. L'IA ACCENTUE LES MENACES, MAIS NE LES RÉ-INVENTE PAS

Les attaques les plus préoccupantes restent les mêmes, mais elles deviennent plus crédibles et plus industrialisées.

PARMI LES ATTAQUES BASÉES SUR L'IA QUI PRÉOCCUPENT LE PLUS LES ENTREPRISES :

POURCENTAGES	ATTAQUES CITÉES
52 %	Phishing, spear phishing
50 %	Attaques automatisées
49 %	Compromission des emails
36 %	deepfakes

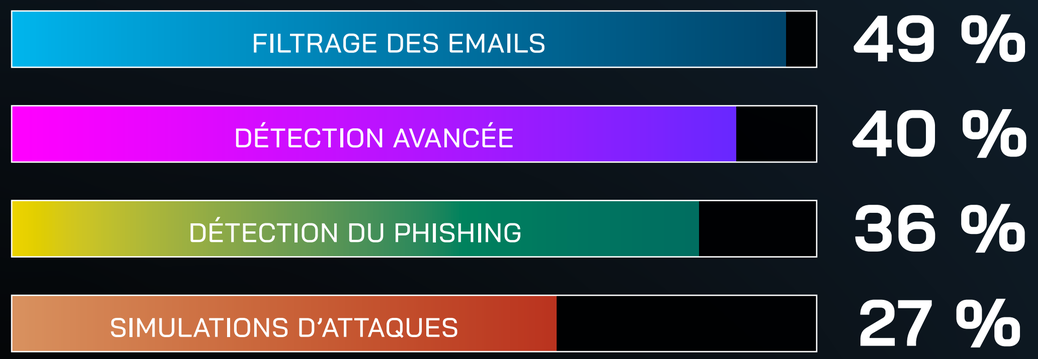
Le point clé du communiqué est très fort : la porte d'entrée numéro 1 des menaces demeure l'email. L'IA permet surtout aux attaquants de rédiger des messages sans faute, de créer des scénarios crédibles et de personnaliser à grande échelle.

HORNETSECURITY
BY proofpoint.

3. LES ENTREPRISES RIPOSTENT AVEC L'IA

L'intelligence artificelle n'est pas seulement un risque. Elle devient aussi un outil de défense déjà largement intégré.

EN EFFET, 85% DES ORGANISATIONS INTÈGRENT DÉJÀ L'IA DANS LEUR DÉFENSE.



Les résultats sont déjà visibles : 74 % des répondants confirment que l'IA permet d'atténuer avec succès les menaces, soit 6 points de plus qu'en 2024. L'analyse indique également que 7 sur 10 des organisations se disent suffisamment préparés pour faire face à une attaque de type zero-day.

PRIORITÉ D'INVESTISSEMENT DANS LES 12 À 24 PROCHAINS MOIS



L'investissement va se poursuivre : dans les années à venir, 68 % des décideurs cyber interrogés confirment que l'investissement dans l'IA sera une forte priorité. En revanche, pour 22 %, il s'agira d'une priorité absolue.



HORNETSECURITY
BY proofpoint

MESURES CLÉS **POUR RENFORCER VOTRE SÉCURITÉ**

1. PLACER L'EMAIL AU CENTRE DE LA STRATÉGIE CYBER

Le communiqué est explicite : la porte d'entrée numéro 1 des menaces reste **l'email.**

Les entreprises doivent donc renforcer la sécurité email, notamment contre

- le phishing & spear phishing,
- la compromission des emails,
- les messages crédibles générés par IA…

L'objectif n'est pas uniquement de **bloquer plus d'attaques**, mais aussi de **réduire la probabilité** qu'un utilisateur averti se fasse piéger par un **message personnalisé, sans faute et contextualisé.**

HORNETSECURITY
BY proofpoint.

2. UTILISER L'IA POUR RENFORCER LA DÉTECTION

Avec **85 %** des décideurs qui intègrent déjà l'IA dans leur cybersécurité, l'enjeu n'est plus de savoir si l'IA doit être utilisée, mais **où elle apporte le plus de valeur.**

- le filtrage des emails,
- la détection avancée des menaces,
- la détection du phishing,
- et les simulations d'attaques.

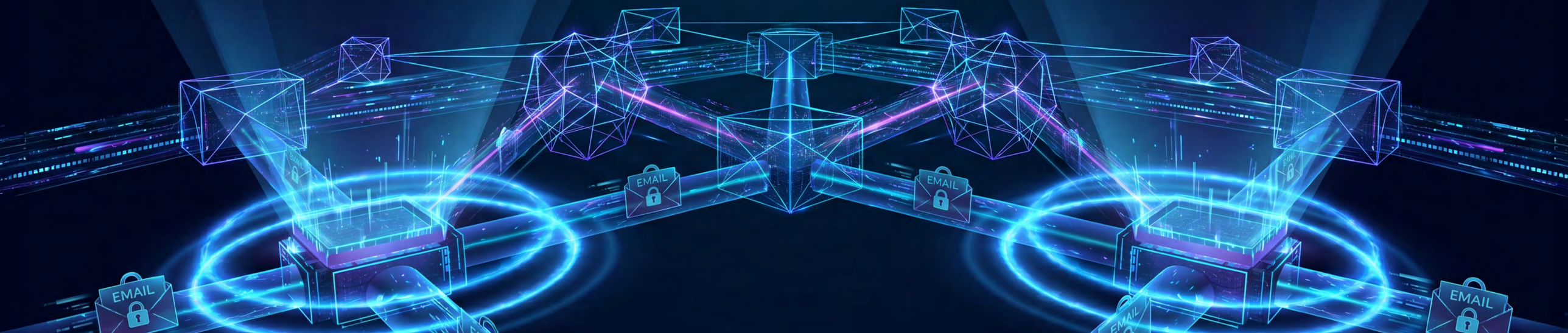
L'objectif n'est pas uniquement de **bloquer plus d'attaques**, mais aussi de **réduire la probabilité** qu'un utilisateur averti se fasse piéger par un **message personnalisé, sans faute et contextualisé.**

3. SENSIBILISER D'AVANTAGE LES ÉQUIPES

Les organisations doivent non seulement renforcer leurs défenses, mais aussi **sensibiliser davantage leurs équipes** à la cybersécurité.

Face à des emails plus **crédibles, personnalisés et automatisés**, la sensibilisation ne peut pas être ponctuelle. Elle doit être **continue, contextualisée et liée** aux menaces réellement observées :

- phishing,
- compromission des emails,
- deepfakes
- et demandes frauduleuses.



4. PRÉPARER LES SCÉNARIOS D'ATTAQUES COMPLEXES

Comme mentionné, **7 entreprises sur 10** se disent suffisamment préparées pour faire face aux attaques de type zéro-day.



Cette confiance doit être testée. Les entreprises doivent vérifier leurs procédures : **détection, escalade, réponse, communication interne, restauration et continuité d'activité**. Le risque n'est pas seulement l'attaque, mais l'incapacité à réagir vite lorsque les signaux sont ambigus.

5. INVESTIR DANS LA CYBERSÉCURITÉ

Pour conclure cette analyse sur un message clair, il est important de garder en tête que les entreprises doivent investir dans les bons outils et s'associer aux **bons partenaires** pour garder une **longueur d'avance**.

L'IA doit donc être intégrée dans une **approche structurée** :

- outils,
- gouvernance,
- sensibilisation,
- partenaires
- et mesure de l'efficacité.

L'objectif n'est pas d'ajouter de la complexité, mais de mieux détecter, mieux prioriser et mieux répondre.

HORNETSECURITY
BY proofpoint.

CONCLUSION

L’IA change profondément la nature des cyberattaques. **Elle les rend plus rapides, plus crédibles et plus difficiles à détecter.**

Mais l’IA est aussi une réponse. Certaines organisations l’intègrent déjà massivement dans leur cybersécurité, avec des usages concrets autour **du filtrage des emails, de la détection des menaces, du phishing et des simulations d’attaques.**

La priorité pour 2026 est claire : **ne pas laisser l’avantage aux attaquants**. Les entreprises doivent **renforcer leurs défenses, sensibiliser leurs équipes et structurer leurs investissements IA autour de cas d’usage concrets.**



HORNETSECURITY
BY proofpoint.

À PROPOS DE **NOUS**

Hornetsecurity by Proofpoint est l'unité commerciale de Proofpoint exploitant la suite de produits Hornetsecurity, dédiée aux fournisseurs de services gérés (MSP) et aux petites et moyennes entreprises (PME). Elle propose des solutions de sécurité cloud de nouvelle génération, de conformité, de sauvegarde et de sensibilisation à la sécurité, aidant les entreprises et organisations de toutes tailles dans le monde entier. Son produit phare, 365 Total Protection, est la solution de sécurité cloud la plus complète pour Microsoft 365 sur le marché. Portée par l'innovation et l'excellence en cybersécurité, Hornetsecurity contribue à construire un futur numérique plus sûr et des cultures de sécurité durables. Hornetsecurity opère dans plus de 120 pays via son réseau international de distribution comptant plus de 12 000 partenaires et MSP. Ses services premium sont utilisés par plus de 125 000 clients.

Pour plus d'informations, rendez-vous sur hornetsecurity.com

