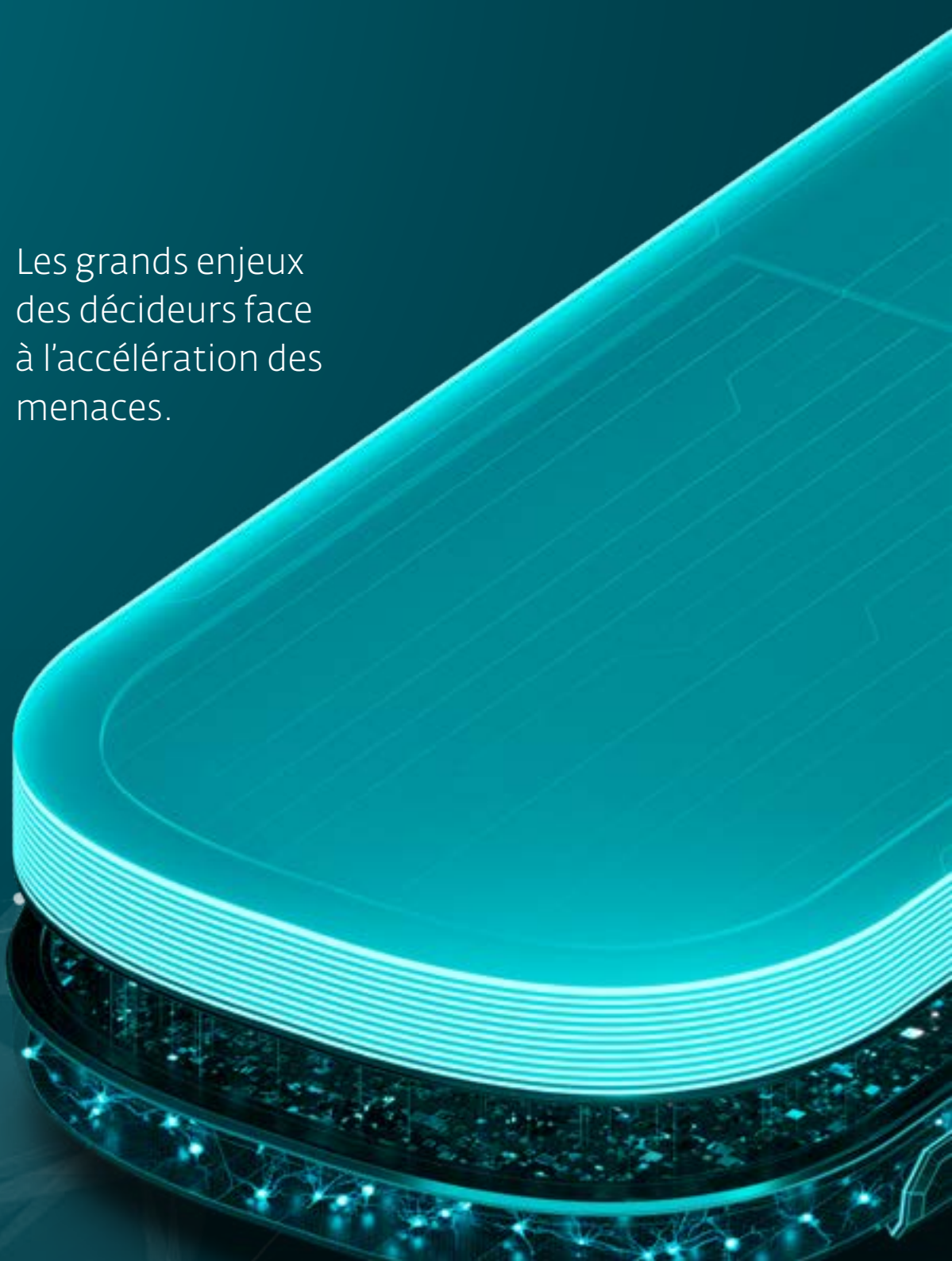
Cybersecurity
Progress. Protected.

Panorama ESET 2026 de la Cybersécurité PME en France : Entre Confiance et Nouvelles Réalités

Les grands enjeux des décideurs face à l'accélération des menaces.



Edito

En 2026, relever les défis de la cybersécurité implique de comprendre la corrélation des besoins de votre entreprise, du comportement humain, de l'IA et d'un paysage instable. Il n'y a qu'une seule solution : devenir plus résilient, en commençant par évaluer son propre niveau de préparation.

Michal Jankech
Vice-président chargé des grandes entreprises, des PME et des MSP chez ESET

DONNÉES DE L'ÉTUDE

- → Focus **France** (avec comparatif monde)
- → **500 décideurs**
- → Entreprises de **25 à 1000 endpoints**
- → Taille de l'échantillon monde : **4 400**

Introduction

Les PME françaises abordent 2026 avec **une confiance élevée dans leur capacité à faire face aux cyberattaques.** Pourtant, les incidents restent fréquents et leurs conséquences dépassent désormais le cadre de l'IT pour toucher directement l'activité globale.

Cette étude met en évidence un paradoxe : malgré une maturité croissante et des investissements en progression, les entreprises **restent exposées à des faiblesses souvent connues**.

L'objectif de ce panorama est d'aider les décideurs à dépasser la lecture des chiffres pour **identifier les priorités d'action** et **transformer la confiance déclarée en résilience mesurable, pilotée et durable.**

Sommaire

Un sentiment de **confiance établi**…

Les décideurs français affichent une forte sérénité. **78 %** ont confiance dans leur résilience face aux cyberattaques et **75 %** des organisations estiment être en mesure d'en limiter les impacts.

78% ont confiance dans leur résilience face aux cyberattaque

75% des organisations estiment être en mesure d'en limiter les impacts

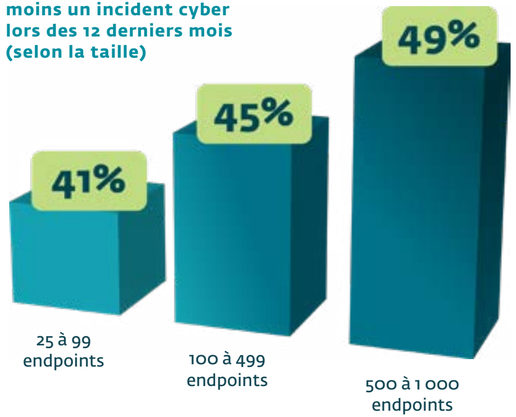
À RETENIR

Si les PME françaises affichent une forte confiance, près d'une sur deux a pourtant subi un incident cyber au cours des douze derniers mois. Pour les DSI, l'enjeu est donc de couvrir les angles morts et d'objectiver leur résilience avec des indicateurs concrets : délai de détection, d'investigation et de remédiation.

Une exposition aux menaces cyber **toujours élevée**

Malgré la confiance affichée, **44 %** des entreprises françaises ont subi au moins un incident au cours des 12 derniers mois. Cette proportion frôle même **une organisation sur deux** pour les structures comptant entre 500 et 1 000 endpoints.

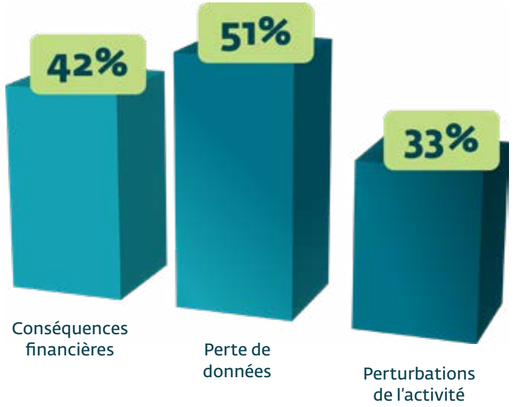
Entreprises ayant subi au moins un incident cyber lors des 12 derniers mois (selon la taille)



La cybersécurité s'impose comme **un risque stratégique**

Les entreprises redoutent avant tout les conséquences opérationnelles. Les trois principales craintes sont **la perte de données (51 %)**, les **conséquences financières (42 %)** et les **perturbations de l'activité (33 %)**.

Top 3 des préoccupations liées aux répercussions des cyberattaques



À RETENIR

La cybersécurité n'est plus seulement un sujet IT, mais une condition de continuité d'activité. En ce sens, le rôle de la DSI n'est pas seulement de protéger les actifs numériques de l'entreprise, elle est stratégiquement impliquée dans les enjeux business.

Une maturité croissante qui ne fait **pas disparaître le risque**

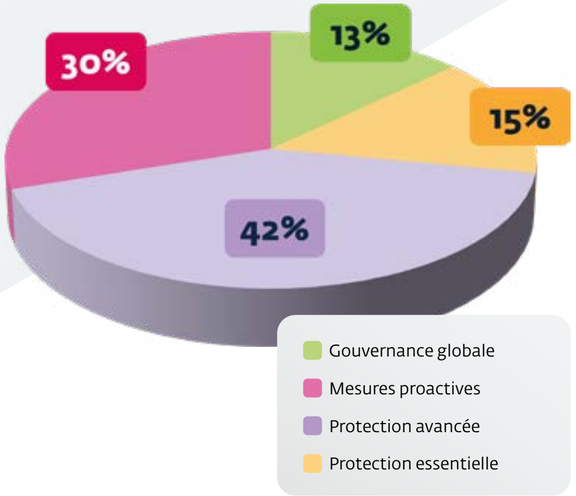
En France, la maturité cyber des PME est globalement élevée : **42 %** disposent d'une protection avancée et **43 %** ont mis en place des mesures proactives ou une gouvernance globale.

Les entreprises ayant subi plusieurs incidents optent plus franchement pour **un niveau de protection essentielle (25 %) que la moyenne des entreprises interrogées (14 %).**

À RETENIR

Bien que conscient des risques encourus, de nombreuses entreprises peinent encore à obtenir un niveau de protection suffisant. Pour la DSI, chaque incident doit devenir un levier de structuration, en renforçant la gouvernance, les processus et les priorités d'investissements cyber.

Posture de cybersécurité des PME françaises



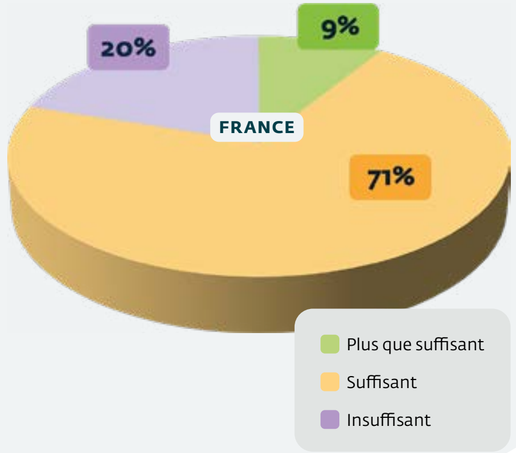
Les budgets progressent, mais **leur allocation devient stratégique**

Le budget n'est plus le point bloquant majeur en France. **80 %** des organisations françaises jugent leur budget suffisant, voire plus que suffisant. De plus, **42 %** d'entre elles prévoient une augmentation de leurs investissements l'année prochaine.

À RETENIR

Pour une majorité de PME françaises, le budget n'est plus le principal frein, mais les incidents persistent malgré des moyens jugés suffisants. L'enjeu est donc de passer d'une logique de dépense à une logique d'efficacité, centrée sur la réduction concrète du risque.

Appréciation des PME sur leurs budgets cybersécurité

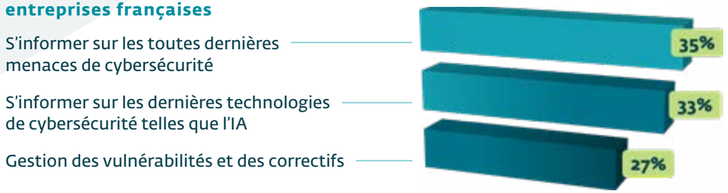


La multiplication des outils **complexifie la cybersécurité**

Le véritable défi réside dans l'efficacité des solutions à mettre en place. Les principaux obstacles sont la **complexité et les difficultés d'intégration (21 %)**, ainsi que la **pénurie de compétences (20 %).** Les équipes peinent surtout à s'informer **sur les toutes dernières menaces (35 %)** et **les nouvelles technologies (33 %).**

Obstacles actuels à l'amélioration de la cybersécurité dans l'entreprise

Préoccupations cybersécurité des entreprises françaises



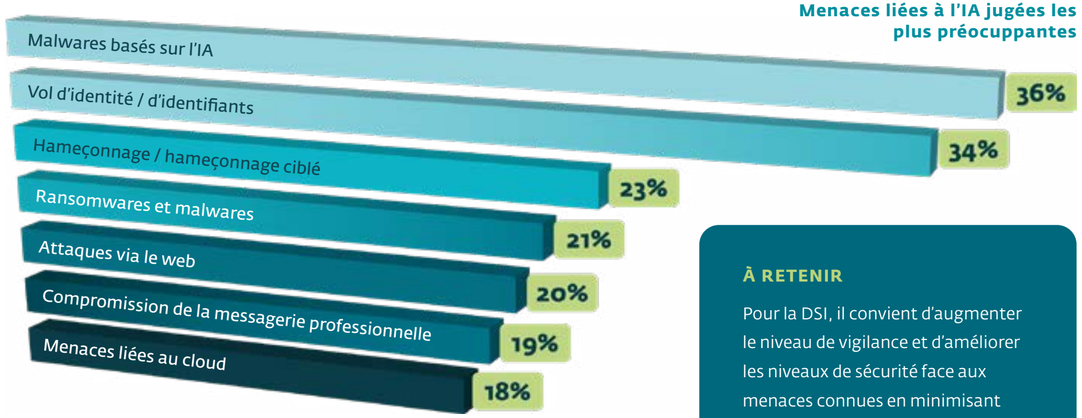
À RETENIR

Si le budget reste le principal frein à l'amélioration de la cybersécurité, les enjeux d'intégration des solutions et de disponibilité des compétences continuent également de peser sur les organisations. Pour les DSI, l'enjeu est de rationaliser les investissements et de simplifier la gestion de la cybersécurité afin de gagner en efficacité.

L'IA intensifie la menace mais **ne la révolutionne pas** (encore)

Les malwares générés par l'IA inquiètent **36 %** des PME. Cependant, l'IA est aujourd'hui surtout utilisée par les cybercriminels pour accélérer des méthodes classiques. Les données de télémétrie d'ESET montrent que **l'hameçonnage** reste de loin la cause n°1 des incidents. L'ensemble de données de MDR d'ESET ne recense aucun incident dans lequel l'IA générative aurait joué un rôle significatif.

Menaces liées à l'IA jugées les plus préoccuppantes



À RETENIR

Pour la DSI, il convient d'augmenter le niveau de vigilance et d'améliorer les niveaux de sécurité face aux menaces connues en minimisant leur surface d'attaque.

L'adoption des outils IA progresse plus vite que son encadrement

Les entreprises françaises intègrent l'IA à un rythme soutenu : **66 %** l'utilisent déjà. La France se distingue toutefois par sa rigueur : **72 %** des entreprises considèrent qu'elle entraîne des risques de sécurité supplémentaires. Ainsi, **62 %** des entreprises ont mis en place des politiques pour restreindre l'usage d'IA non approuvées, témoignant d'une volonté de contrôle, malgré la rapidité de l'adoption.

66% Des entreprises françaises utilisent déjà l'IA

72% des entreprises considèrent qu'elle entraîne des risques de sécurité supplémentaires

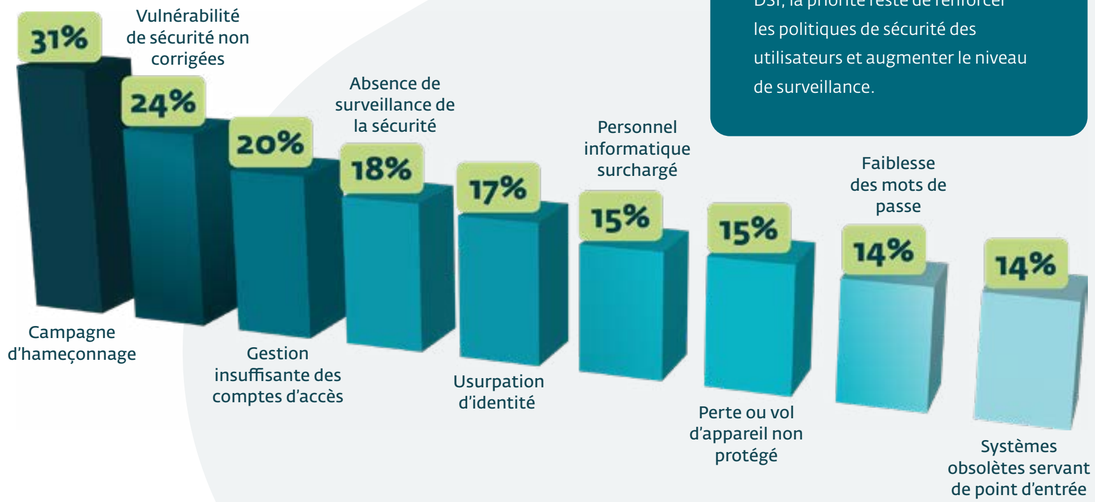
62% des entreprises ont mis en place des politiques pour restreindre l'usage d'IA non approuvées

À RETENIR

L'IA est à la fois un levier de productivité et une nouvelle surface de risque, notamment lorsqu'elle est utilisée sans cadre par les métiers. Pour la DSI, l'enjeu est de définir une gouvernance claire : outils autorisés, protection des données sensibles et règles d'usage.

Les attaquants exploitent encore largement les **failles humaines et opérationnelles**

Les organisations doivent composer avec une accumulation de vulnérabilités techniques, de lacunes de gouvernance et de contraintes humaines qui, combinées, élargissent la surface d'attaque.



À RETENIR

Les incidents exploitent encore majoritairement des failles connues et évitables : la sophistication des menaces ne doit donc pas faire oublier les fondamentaux. Pour les DSI, la priorité reste de renforcer les politiques de sécurité des utilisateurs et augmenter le niveau de surveillance.

Le paradoxe de l'inaction face aux **risques connus**

Les PME s'inquiètent des menaces du futur mais négligent les bases. Les **vulnérabilités non corrigées (24 %)** demeurent l'une des principales portes d'entrée pour les attaquants

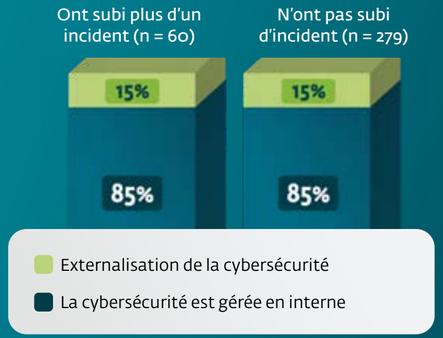
La gestion de la cybersécurité reste largement **internalisée dans les entreprises françaises**

Si l'externalisation se développe progressivement, elle demeure minoritaire. Par ailleurs, le fait d'avoir subi un ou plusieurs incidents ne semble pas influencer ce choix, qui apparaît davantage guidé par des considérations organisationnelles et stratégiques que par une réaction aux attaques.

À RETENIR

Pour les DSI, l'enjeu n'est plus de choisir entre gestion interne et externalisation, mais de trouver le bon équilibre. Les services managés, comme le MDR, permettent de compléter les compétences internes, d'accéder à une expertise spécialisée et de renforcer les capacités de détection et de réponse.

Gestion de la cybersécurité selon survenue d'attaques



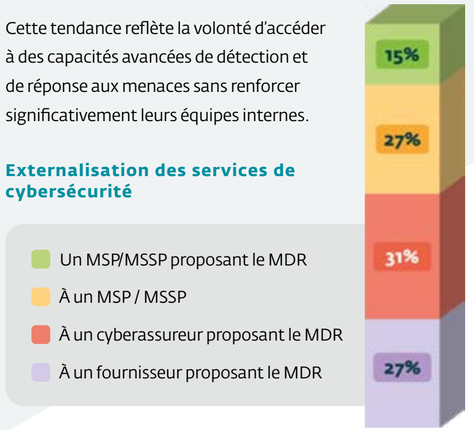
14% Des entreprises externalisent la cybersécurité

Détecter et réagir plus vite : pourquoi le MDR s'impose progressivement

Pour pallier le manque de ressources, l'externalisation intelligente s'impose. En France, **58 %** des entreprises qui délèguent leur sécurité s'appuient sur un service de type **MDR** (Managed Detection and Response) pour bénéficier d'une défense approfondie.

Cette tendance reflète la volonté d'accéder à des capacités avancées de détection et de réponse aux menaces sans renforcer significativement leurs équipes internes.

Externalisation des services de cybersécurité



INVESTIGUER PLUS VITE POUR RÉDUIRE L'IMPACT BUSINESS

Seules **41 % des investigations cyber** sont finalisées en moins de deux semaines en France. Pour la majorité des entreprises, l'analyse d'un incident s'étend jusqu'à 6 semaines (53%), parfois il leur faut plus de 3 mois (6%). Cette lenteur pèse sur l'activité : elle prolonge l'incertitude, mobilise les équipes et retarde le retour à la normale. Réduire le temps d'investigation devient clé pour limiter l'impact business d'une cyberattaque.

À RETENIR

Le MDR répond aux besoins d'expertise, de continuité et de rapidité de réponse, faisant de l'externalisation un choix stratégique de ressources plutôt qu'une solution de secours. Pour la DSI, il constitue un levier concret pour garantir des capacités de détection et d'investigation en continu.

La souveraineté devient **un critère clé de confiance cyber**

Dans un contexte où **78 %** des entreprises françaises considèrent la cyberguerre comme une menace réelle, la souveraineté devient un critère de confiance concret. Origine des fournisseurs, localisation des données et maîtrise de l'hébergement pèsent désormais dans le choix des solutions cyber.

83% Vérifient la localisation des serveurs qui stockent leurs données.

77% Privilégient des solutions développées par des entreprises européenne

À RETENIR

L'origine des fournisseurs et la localisation des données sont désormais des critères de choix à part entière. Face aux tensions géopolitiques, les entreprises recherchent désormais à garantir leur souvereinté tout en gardant un équilibre entre performance technologique, coût et efficacité des solutions.

ESET : la cybersécurité européenne de confiance, portée par l'IA

Avec ESET, les entreprises s'appuient sur une cybersécurité européenne, éprouvée et proactive.

Gartner

CHALLENGER MAGIC QUADRANT™
Endpoint Protection Platforms

FORRESTER®

STRONG PERFORMER THE FORRESTER WAVE™
Dans la catégorie Managed Detection and Response (MDR) Q3 2025

IDC

LEADER IDC MARKETSCAPE
Worldwide Endpoint Security

ADN EUROPÉEN

- → Éditeur européen basé dans l'UE
- → Conformité **NIS2 & RGPD**
- → Certifications **ISO 27001 & ISO 9001**
- → Support local **100 % francophone**

PROTECTION MULTICOUCHE & IA

- → Détection des menaces connues et inconnues
- → IA enrichie par la télémétrie mondiale
- → Analyse comportementale en temps réel
- → **21 technologies intégrées** pour protéger les endpoints

EXPERTISE INTERNATIONALE

- → **1+ milliard** d'internautes protégés
- → **500 000+** entreprises clientes
- → **176** pays et territoires
- → **11** centres de recherche

Cybersecurity
Progress. Protected.

Ne laissez pas la complexité **freiner votre résilience cyber**.

www.eset.com/fr

Ce document est à jour au 15 mai 2026 et peut être modifié à tout moment par ESET.

Pour plus d'informations, veuillez contacter le service des relations publiques d'ESET à l'adresse presse@eset-nod32.fr.