Cybersécurité à l'ère de l'IA : pourquoi renforcer la protection de ses données critiques

Proposé par **FREE PRO**

Face à l'intensification de la menace cyber due à l'usage de l'IA, Free Pro invite les organisations à concentrer leurs efforts sur leurs données critiques en leur dédiant des infrastructures souveraines et sécurisées.

La menace cyber n'est plus une hypothèse, mais une réalité opérationnelle quasi-quotidienne pour les organisations de toute taille et de tout secteur. L'intelligence artificielle est au cœur de cette transformation : elle constitue à la fois un accélérateur de risques, mais également un levier défensif essentiel. L'IA est devenue un acteur à double tranchant qui redéfinit les règles du jeu pour les attaquants comme pour les défenseurs. Face à cette nouvelle donne, où l'automatisation des menaces devient la norme, quelle stratégie adopter pour protéger l'actif le plus précieux des organisations : leurs données ?

L'IA, accélérateur de menaces

Aujourd'hui, pour toutes les organisations, appréhender la nature évolutive des cybermenaces est un impératif stratégique. Deux phénomènes majeurs redéfinissent ce paysage. Le premier est l'intensification des attaques : non seulement leur volume croît, mais leur taux de réussite augmente également, et touche indistinctement tous les secteurs, de la santé à la finance.

Le second est l'essor de l'intelligence artificielle comme multiplicateur de risques. D'une part, elle génère de nouvelles surfaces de vulnérabilité, l'usage croissant de l'IA agentique devenant une cible de choix pour les cybercriminels. D'autre part, elle perfectionne et industrialise les méthodes d'attaque. Désormais, les machines automatisent les tentatives d'intrusion. Pourtant, aussi sophistiquées soient-elles, ces menaces externes proviennent la plupart du temps de vulnérabilités internes aux organisations.

Quand la menace vient de l'intérieur et de la réglementation

La forteresse numérique traditionnelle, protégée par de simples firewalls, est un concept dépassé. Les risques les plus insidieux sont aujourd'hui internes, qu'ils soient humains ou technologiques, et sont amplifiés par une pression réglementaire croissante qui exige une approche de sécurité plus holistique.

Le phénomène du shadow IA illustre bien ce risque. Des collaborateurs, en quête d'efficacité, utilisent des outils d'IA publics sans validation interne, et exposent ainsi

contrats et données sensibles sur des plateformes échappant à tout contrôle. Or les données constituent le premier actif stratégique des entreprises et ne doivent pas être confiées à n'importe quel acteur. À cela s'ajoute la vulnérabilité persistante des postes de travail, qui rend nécessaire le déploiement de solutions de détection et réponse sur les terminaux (EDR), d'orchestration de la sécurité (SOAR) et d'analyse comportementale (UEBA).

Enfin, le renforcement du contexte réglementaire européen (NIS2, Dora) ajoute une pression supplémentaire. Car loin d'une contrainte, il représente le vecteur d'une démarche stratégique essentielle – l'occasion unique de se poser les bonnes questions en matière de sécurité des données en identifiant et cartographiant les principales données critiques des organisations. Dès lors, dans un paysage défini par des vulnérabilités internes et des mandats réglementaires externes, la souveraineté cesse d'être une préférence pour devenir le pilier de la résilience d'entreprise.

La souveraineté comme réponse stratégique

Dans ce contexte, la souveraineté numérique, qui garantit la maîtrise complète des données et des infrastructures qui les hébergent, est passée du statut d'effet de mode à celui de critère de sélection indispensable. Elle constitue aujourd'hui le pilier de la confiance entre une entreprise et ses partenaires technologiques.

Cette exigence n'est plus théorique. Une récente enquête d'Hexatrust révèle que près de 80 % des entreprises françaises intègrent la souveraineté dans leurs appels d'offres. Plus révélateur encore, la moitié d'entre elles a déjà écarté une solution faute de garanties suffisantes. Cette tendance de fond s'explique par la prise de conscience des risques liés aux législations extra-européennes, tel le Cloud Act américain, qui peuvent permettre un accès légal et une gestion de données sensibles hébergées par des fournisseurs étrangers.

Pour Free Pro, la réponse à ces enjeux repose sur un triptyque de confiance : la maîtrise des technologies, des lieux d'hébergement et des équipes. Cette vision se traduit par des garanties concrètes en matière de :

- **Localisation :** L'ensemble des datacenters, des infrastructures et des équipes Free Pro sont situés en France.
- **Technologie propriétaire :** La Solution Cyber XPR s'appuie sur ITrust, son centre d'expertise cybersécurité et sa technologie souveraine d'intelligence artificielle Reevelium. Cet outil SIEM/SOC UEBA/XDR permet de détecter les menaces au plus tôt, afin de prévenir les dommages causés aux organisations.
- **Maîtrise de bout en bout :** Free Pro contrôle l'intégralité de la chaîne de valeur de la donnée, de la collecte, à l'hébergement et de l'exploitation à la sécurisation.

C’est cette philosophie de maîtrise qui se concrétise opérationnellement à travers la Solution Cyber XPR.

Cyber XPR : une approche de sécurité à 360 degrés

La Solution Cyber XPR est la matérialisation de l'engagement de Free Pro en faveur d'une cybersécurité souveraine, intégrée et complète. Elle est conçue pour couvrir l'ensemble du cycle de vie de la sécurité, selon un modèle structuré en trois temps.

- **Jour 0 : Audit et diagnostic / scan de vulnérabilité.** Cette première étape est dédiée à l'analyse des vulnérabilités existantes. Elle permet de cartographier les données critiques de l'entreprise — son fameux « or noir » — afin de définir des priorités claires en matière de protection.
- **Jour 1 : Mise en place technique.** Une fois le diagnostic établi, les équipes procèdent au déploiement des agents de sécurité et à l'intégration des différents flux d'information dans le SIEM, pour une installation simple et maîtrisée.
- **Jour 2 : Exploitation continue.** Dès le déploiement achevé, la surveillance devient permanente. Les incidents de sécurité sont supervisés en continu par le SOC (Security Operations Center) d'ITrust, qui assure la prévention, la détection et le traitement des menaces, et les technologies d’UEBA (analyse comportementale usagers et entités). En parallèle, les infrastructures sont surveillées 24/7 par le Centre des Opérations de Free Pro, un service inclus pour l’ensemble des clients. Cette double supervision est fondamentale : Free Pro va bien au-

delà de la fourniture d'infrastructures pour apporter une sécurité opérationnelle complète et un accompagnement quotidien.

La crédibilité de cette approche est renforcée par un engagement fort en matière de certifications (ISO 27001, HDS) et de démarches qualité, notamment avec la démarche de qualification SecNumCloud initiée en janvier 2024 pour l'offre Dedicated Secure Cloud de sa Solution Cloud XPR.

De la dépense contrainte à l'investissement stratégique

L'ère de l'intelligence artificielle impose un changement de paradigme en cybersécurité. Face à des menaces automatisées et de plus en plus sophistiquées, la réponse ne peut être que stratégique, souveraine et intelligente. Face à l'objection récurrente du coût, la réponse de Free Pro ne consiste pas à tout sécuriser uniformément, mais à demander aux organisations de concentrer leurs efforts sur les données critiques en leur dédiant des infrastructures souveraines et sécurisées.

Loin d'être seulement une arme pour les attaquants, l'intelligence artificielle est ainsi réintégrée au cœur des solutions défensives, à l'image des technologies de machine learning et d'UEBA utilisées par Free Pro pour détecter les signaux faibles d'une intrusion. C'est là le rôle d'un partenaire souverain : non de déresponsabiliser, mais de fournir les outils de défense

appropriés et d'inciter ses clients à rester acteurs de leur protection.