BlackBerry
Cybersecurity

Gartner
Peer Insights

Combattre les rançongiciels

Les ransomwares font partie du quotidien des responsables Sécurité de la plupart des entreprises du monde entier dont ils peuvent interdire l’accès aux postes de travail, aux terminaux mobiles et aux réseaux à l’aide d’une clé de chiffrement inviolable. Ce phénomène n’épargne personne, et ses conséquences peuvent être dévastatrices pour les entreprises, indépendamment de leur taille.

Le cabinet Gartner Peer Insights et BlackBerry ont interrogé 300 responsables IT, Ingénierie et Sécurité impliqués dans l’achat de solutions de cybersécurité afin de savoir ce qu’ils pensent de la posture de sécurité de leur entreprise et s’ils envisagent d’évoluer vers une approche fondée sur la prévention.

Principaux enseignements :

- Indépendamment de leur taille et de leur secteur d’activité, les entreprises sont exposées à des attaques par ransomware.
- Les responsables de la cybersécurité ne font pas confiance à la posture de sécurité de leur entreprise.
- Dans leur grande majorité, les équipes en charge de la cybersécurité ne disposent pas de plans de visibilité totale, de surveillance et de réponse aux incidents, ce qui expose leur entreprise à de multiples attaques.
- L’intelligence artificielle (IA) est un composant de sécurité majeur pour les responsables de la sécurité qui souhaitent protéger leur parc de terminaux.

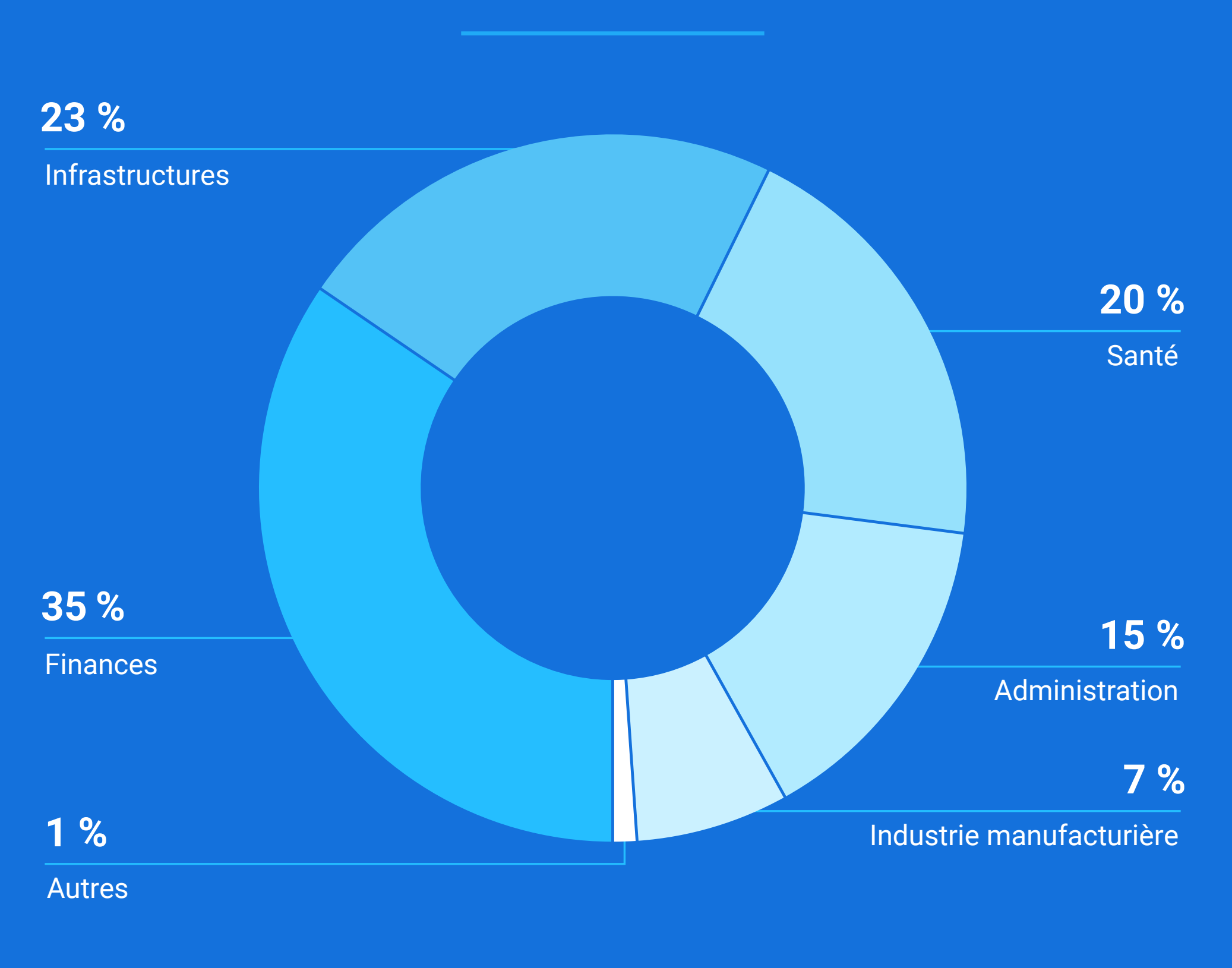
Collecte de données : du 19 juillet au 1er septembre 2022

Panel : 300 responsables de l’informatique, de l’ingénierie et de la sécurité.

Indépendamment de leur taille et de leur secteur d’activité, les entreprises sont exposées à des attaques par ransomware.

Plus d’un tiers des personnes interrogées pensent que le secteur financier sera le plus visé par les attaques par ransomware en 2022.

À votre avis, quel est le secteur d’activité privilégié des attaques par ransomware en 2022 ?



Pour en savoir plus sur la protection et la prévention des attaques par ransomware.

EN SAVOIR PLUS →

Plus de 75 % des personnes interrogées estiment que les ransomwares visent principalement les entreprises qui emploient entre 2 000 et 10 000 personnes.

À votre avis, quelles sont les entreprises les plus visées par les ransomwares ?

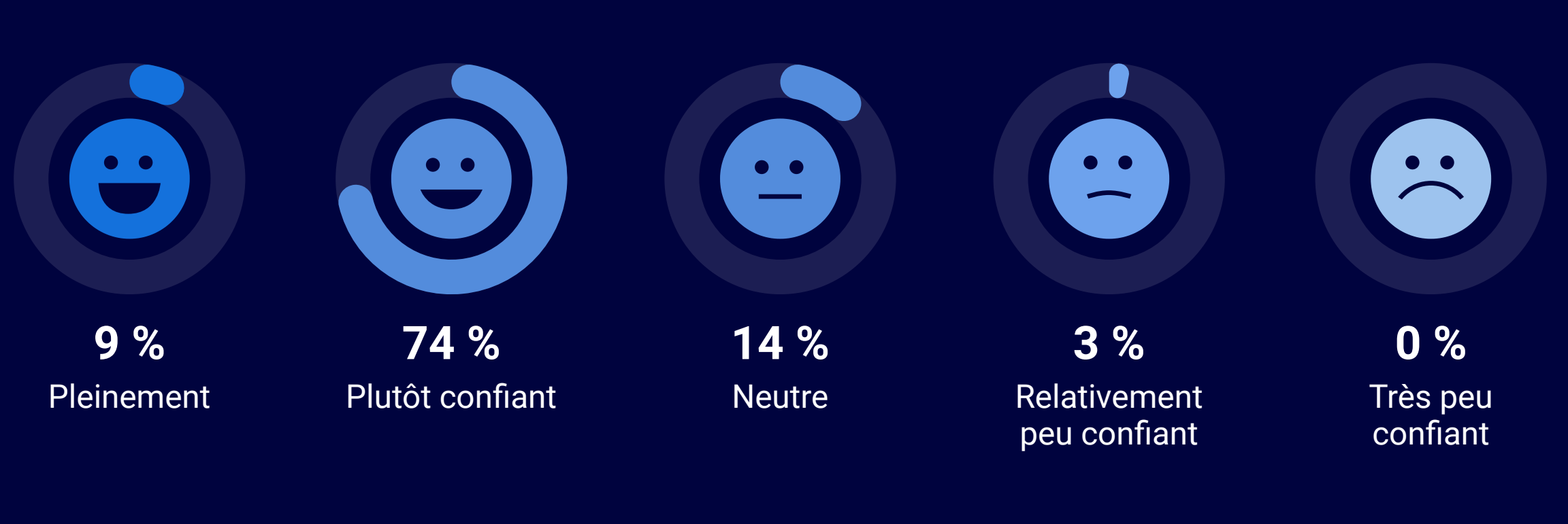
Pour 60 % des responsables Cybersécurité, de 26 à 75 % des victimes d’une attaque par ransomware finissent par verser la rançon demandée.

À votre avis, quel est le pourcentage de victimes de ransomware qui finissent par verser la rançon ?

Les responsables de la cybersécurité ne font pas confiance à la posture de sécurité de leur entreprise.

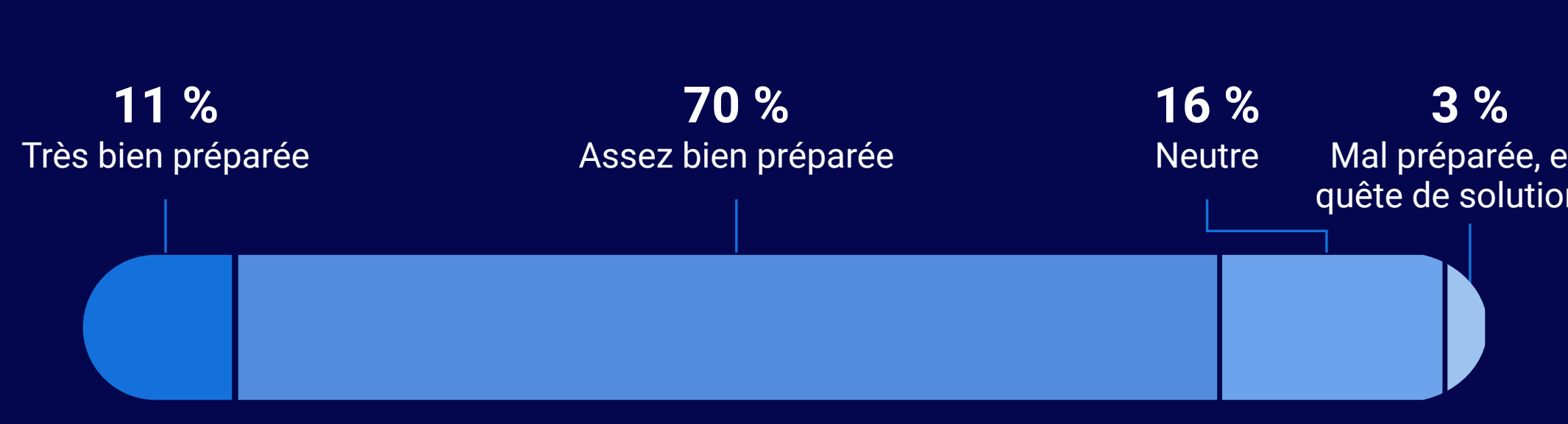
Seulement 9 % des responsables de la cybersécurité accordent une très grande confiance à la posture de sécurité de leur entreprise pour se protéger contre les cyberattaques.

Dans quelle mesure faites-vous confiance à la posture de sécurité de votre entreprise pour se protéger contre les cyberattaques ?



Seulement 11 % des personnes interrogées estiment que leur entreprise est très bien préparée en cas d’attaque par ransomware.

Comment évaluez-vous le degré de préparation de votre entreprise face à une attaque par ransomware ?

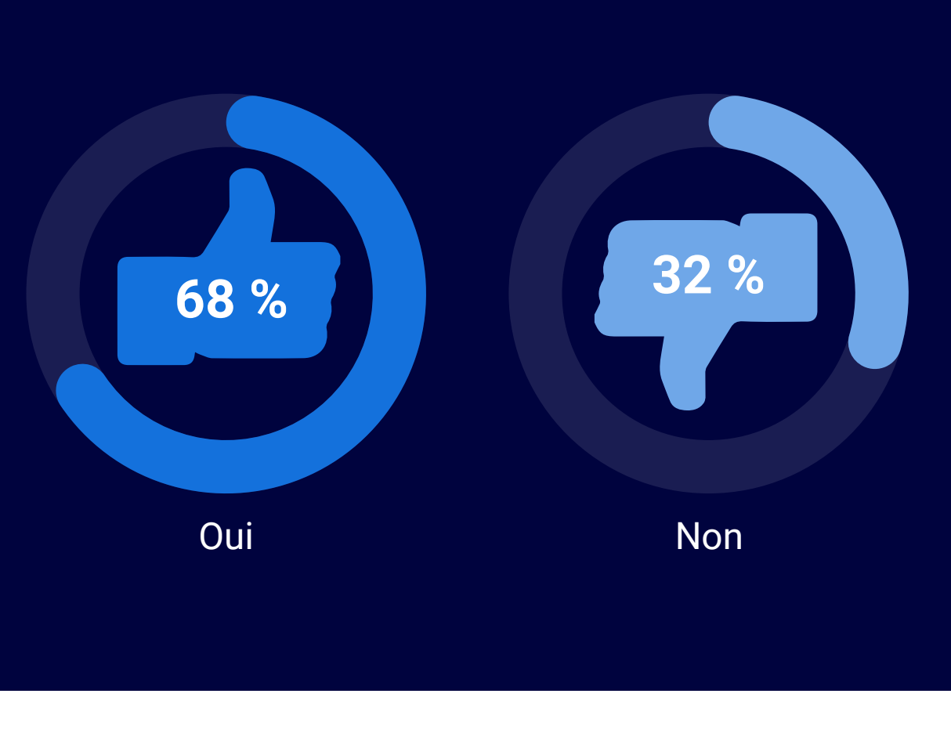


0 % Non préparée et ne cherche pas de solutions

0 % Ne sais pas

En outre, près d’un tiers des personnes interrogées n’ont pas mis en œuvre une infrastructure de sécurité axée sur la prévention.

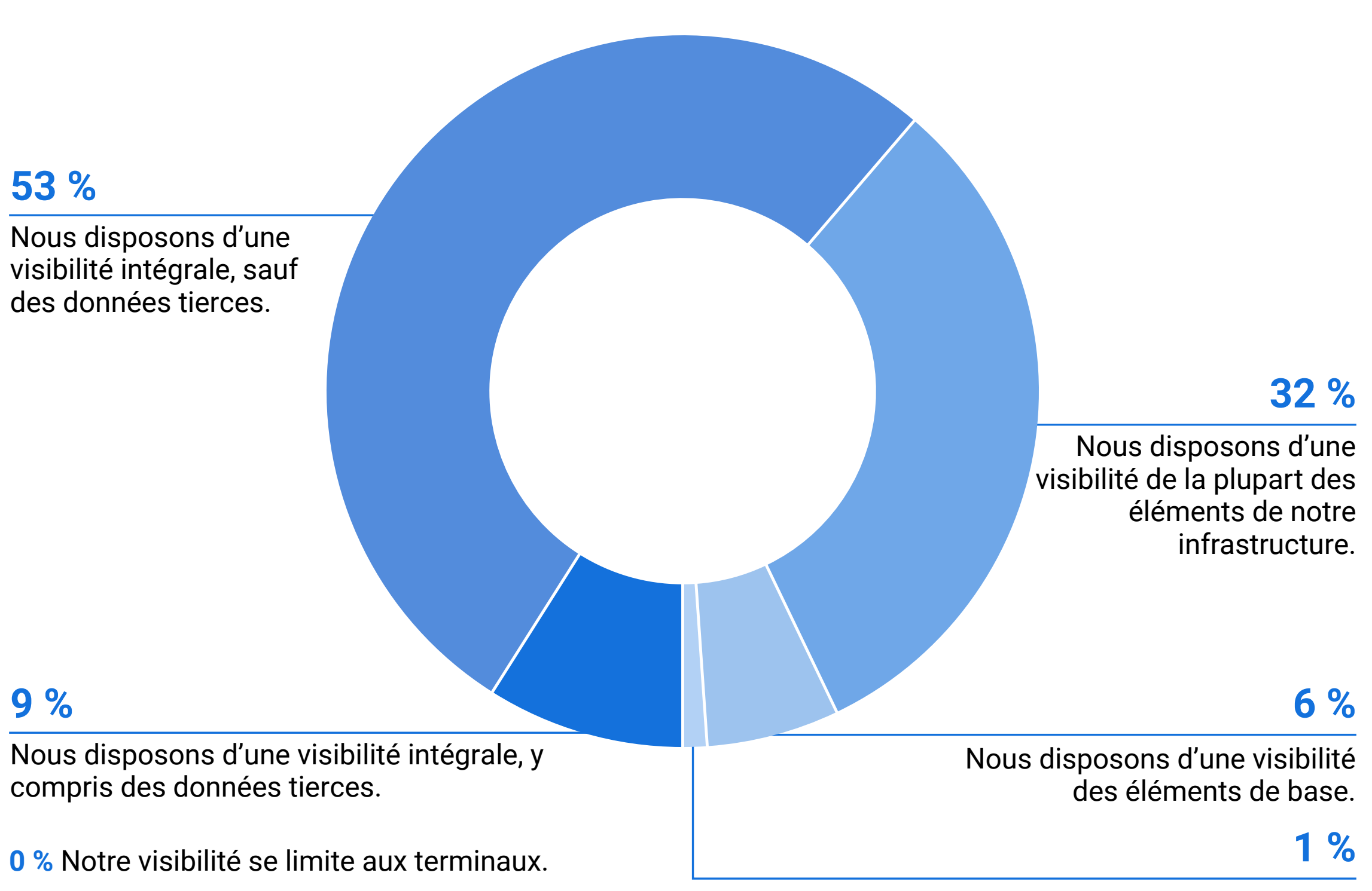
Avez-vous mis en œuvre une infrastructure de sécurité axée sur la prévention ?



Dans leur grande majorité, les équipes en charge de la cybersécurité ne disposent pas de plans de visibilité totale, de surveillance et de réponse aux incidents, ce qui les expose à de multiples attaques.

91 % des responsables Cybersécurité déclarent ne pas disposer d’une visibilité totale de l’ensemble des utilisateurs, terminaux, données et services connectés.

Est-ce que votre équipe Sécurité dispose d’une visibilité de l’ensemble des utilisateurs, terminaux, données et services connectés ?

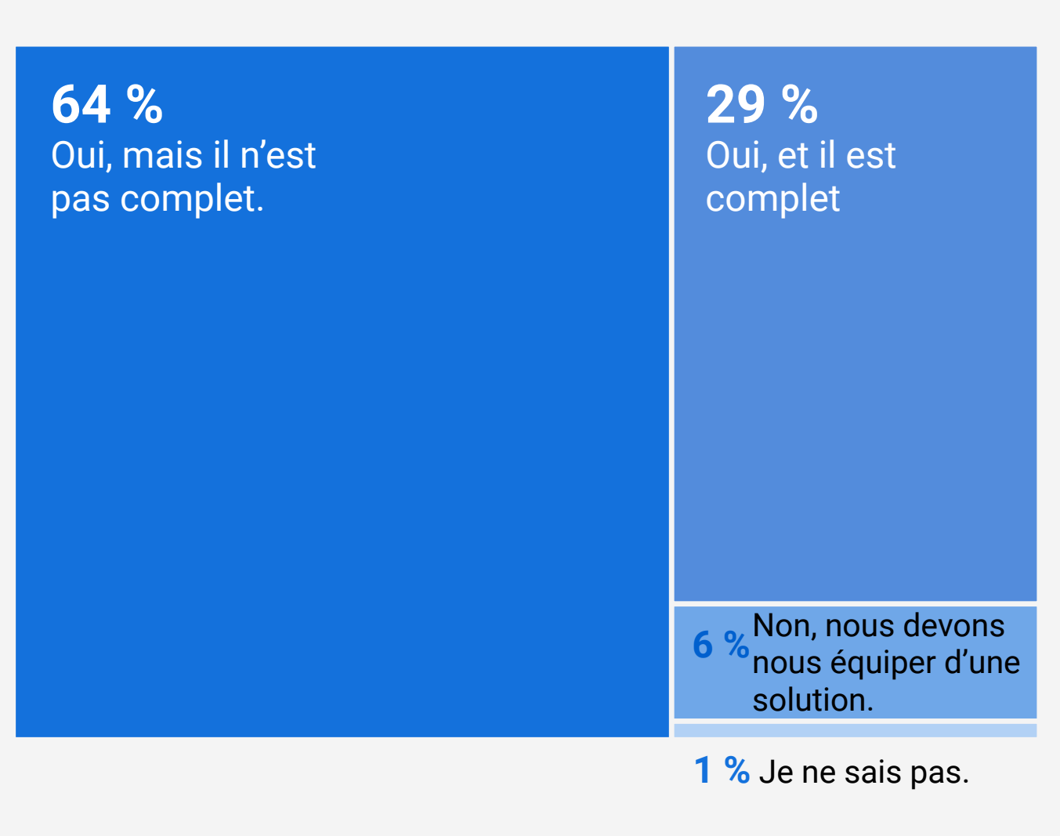


0 % Notre visibilité se limite aux terminaux.

0 % Autres

Moins d’un tiers des personnes interrogées (29 %) déclarent avoir mis en place un plan complet de réponse aux incidents.

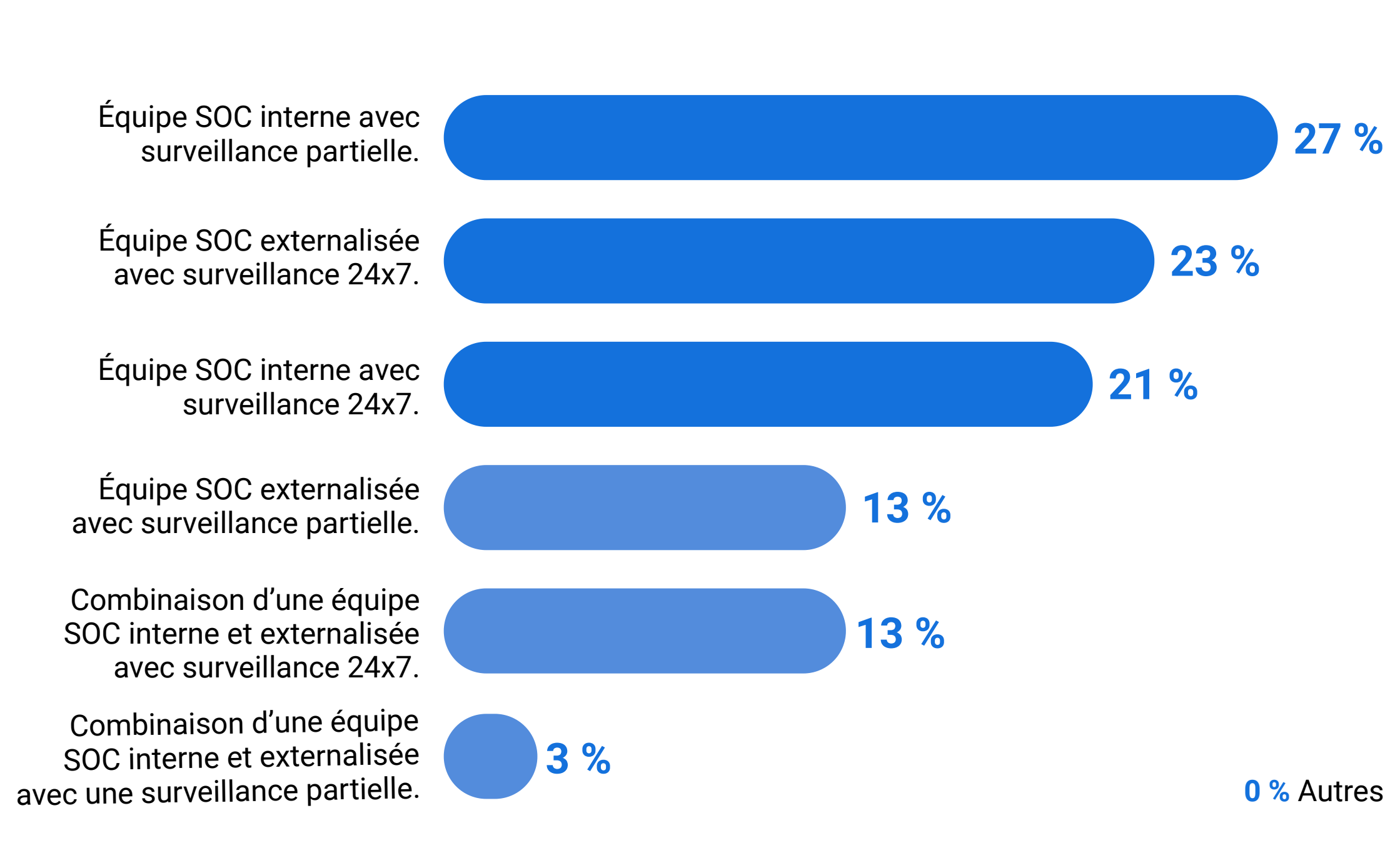
En cas d’attaque, disposez-vous d’un plan de réponse aux incidents ?



0 % Non, et nous ne prévoyons pas d’en mettre une en place

De plus, 43 % des personnes interrogées ont déclaré que leur entreprise n’est pas équipée d’une solution de surveillance opérationnelle 24x7.

Comment gérez-vous votre infrastructure de sécurité ?

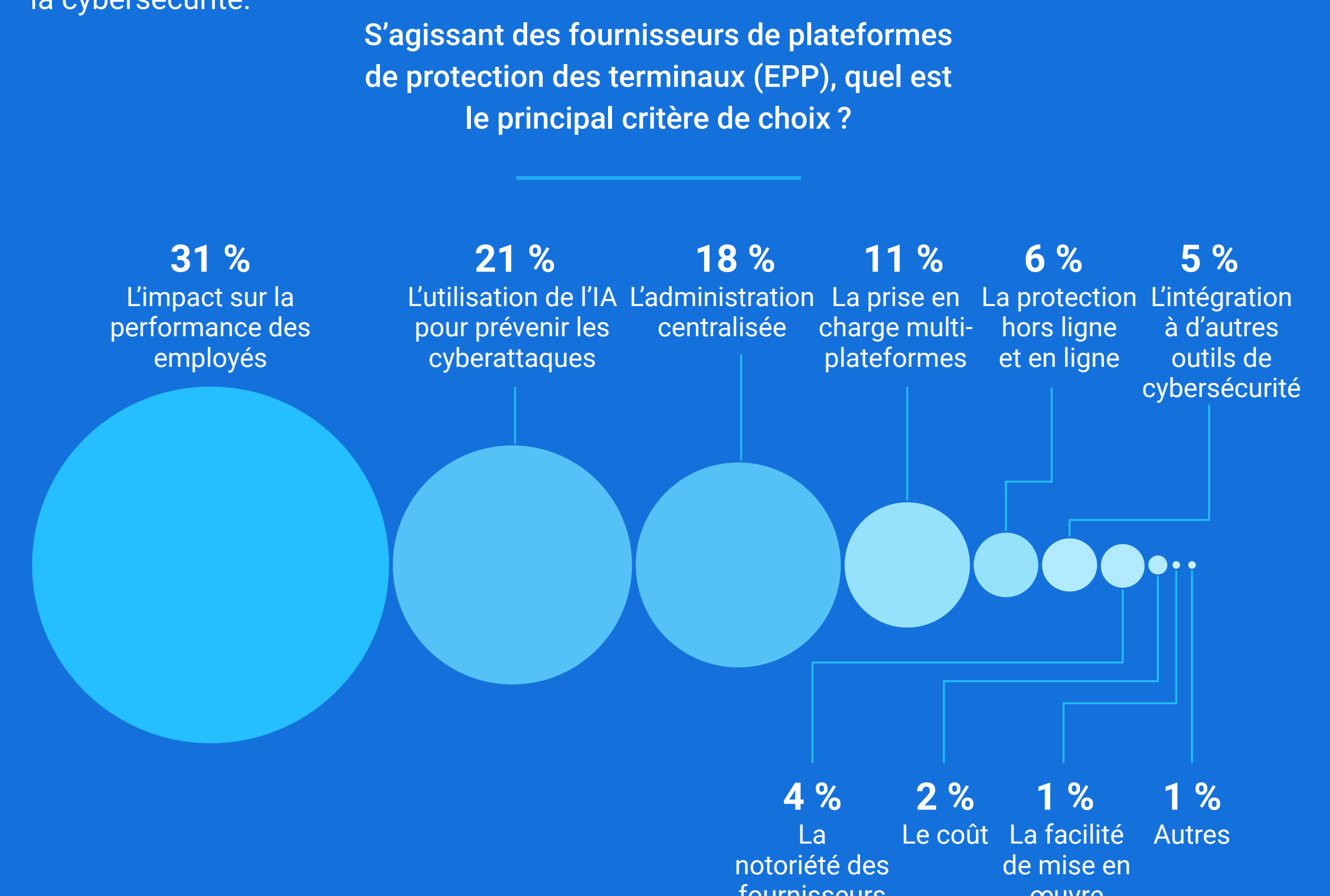


0 % Autres

L’intelligence artificielle est une composante de sécurité clé pour les responsables de la cybersécurité qui souhaitent protéger leur parc de terminaux.

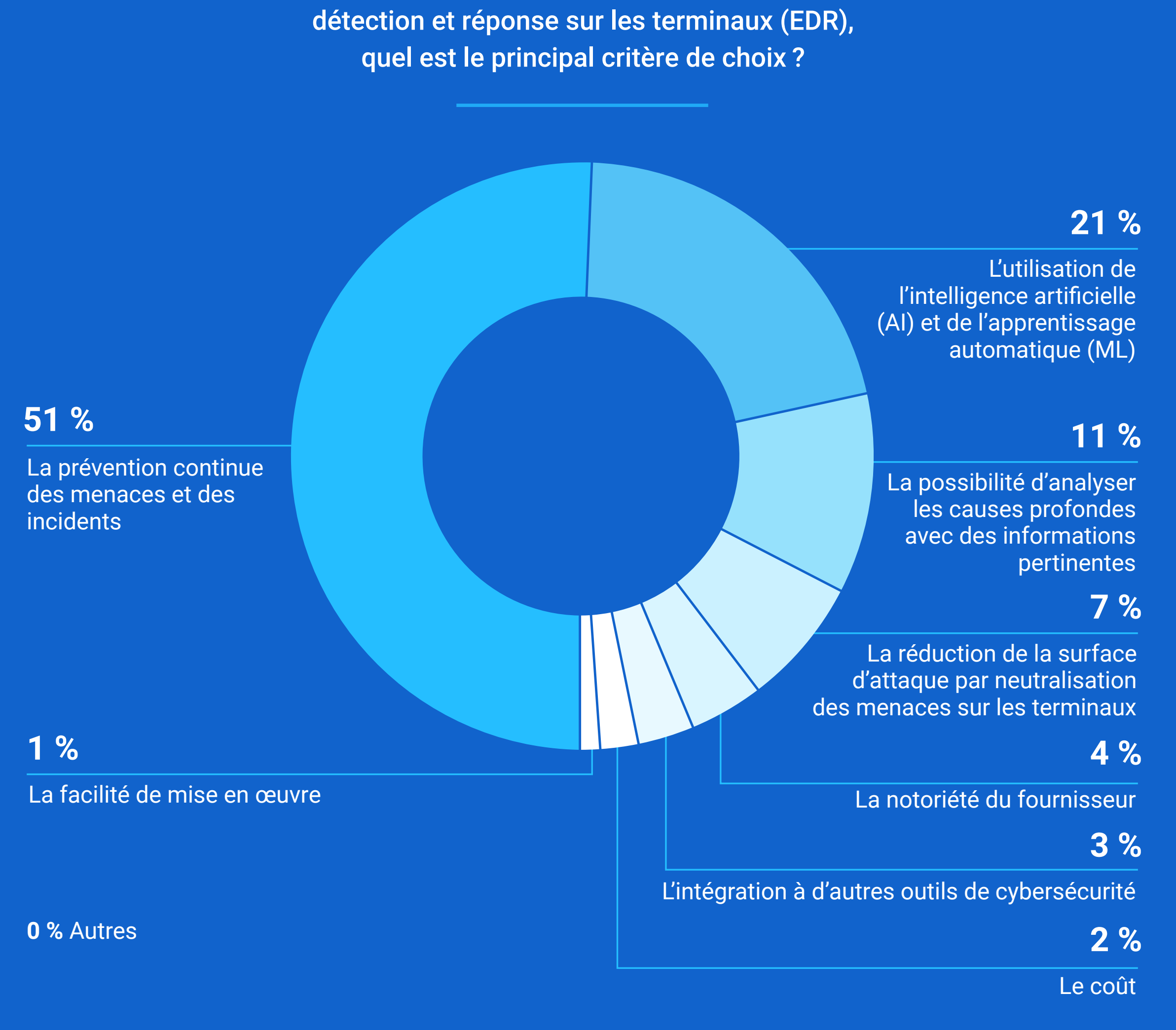
Au moment d’évaluer les fournisseurs de plateformes de protection des terminaux (EPP), l’impact sur la performance des employés (31 %), l’utilisation de l’intelligence artificielle (21 %) et l’administration centralisée (18 %) pointent en tête des priorités des responsables de la cybersécurité.

S’agissant des fournisseurs de plateformes de protection des terminaux (EPP), quel est le principal critère de choix ?



Par ailleurs, la prévention continue des menaces et incidents (51 %), l’intelligence artificielle et l’apprentissage automatique (21 %), et l’analyse des causes profondes (11 %) forment le podium des priorités énoncées par responsables amenés à choisir un fournisseur de solutions de détection et réponse sur les terminaux (EDR).

S’agissant des fournisseurs de solutions de détection et réponse sur les terminaux (EDR), quel est le principal critère de choix ?



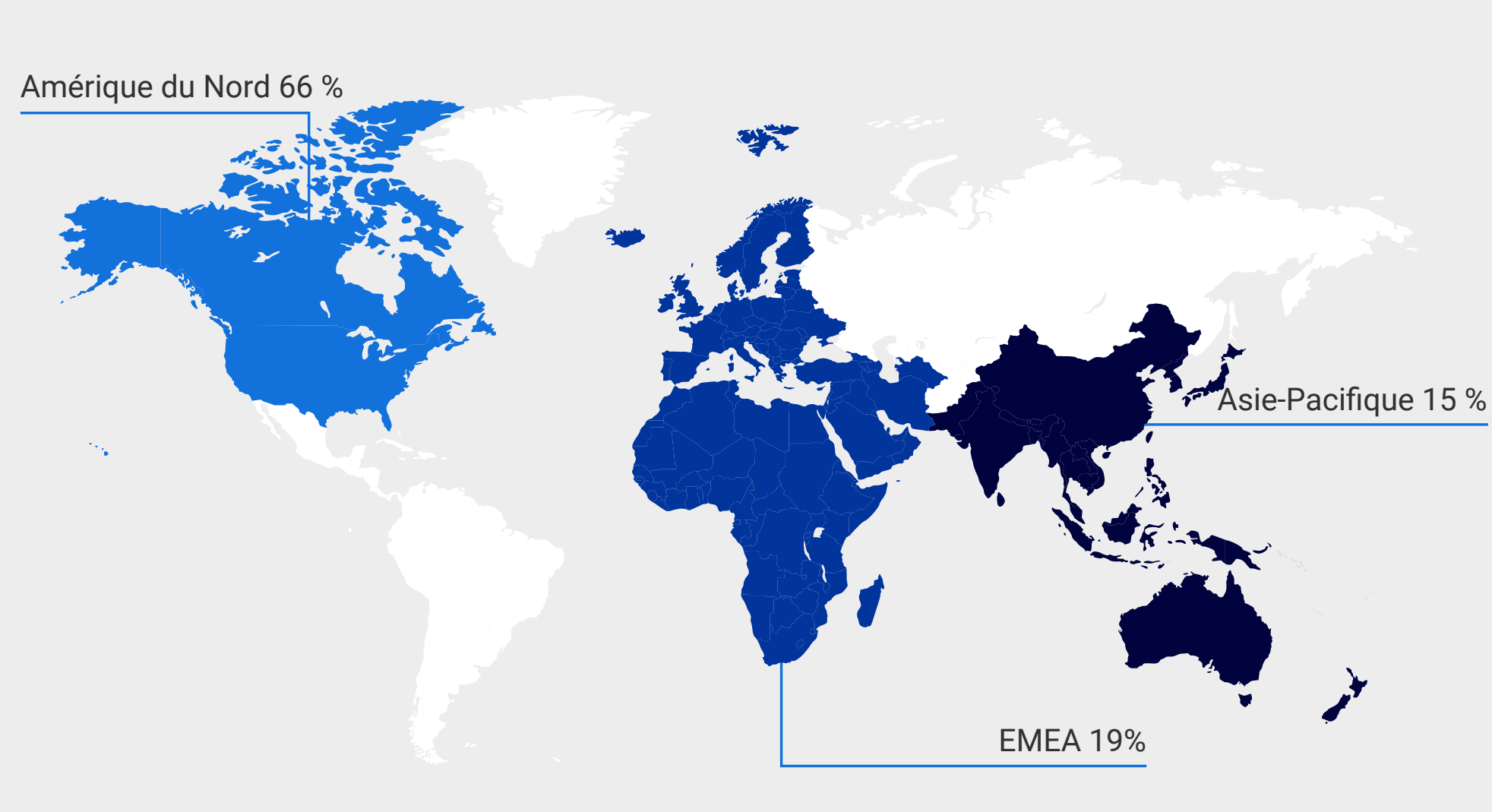
0 % Autres

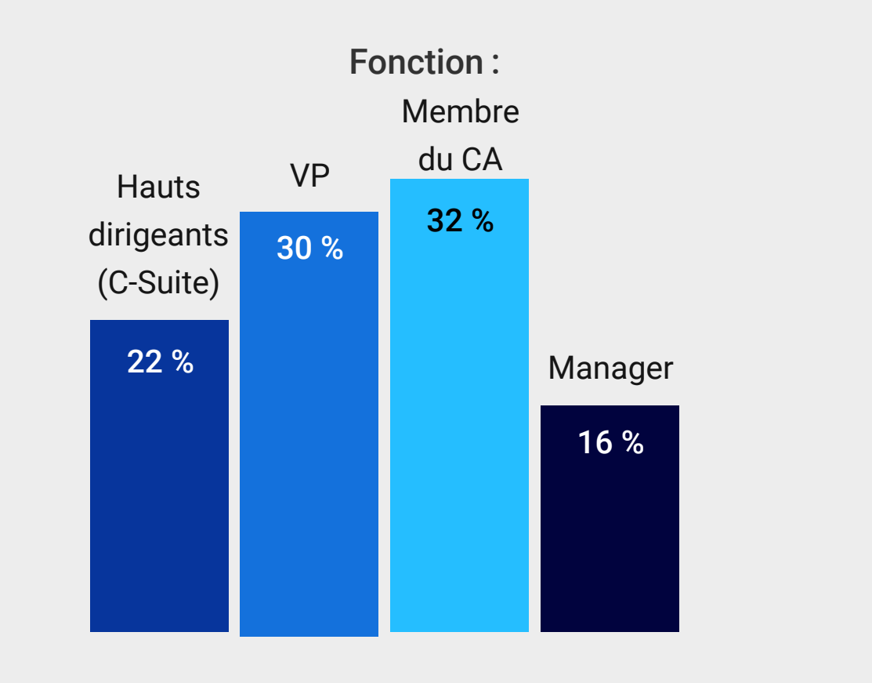
Comment doter votre entreprise d’une protection optimale contre les ransomwares ?

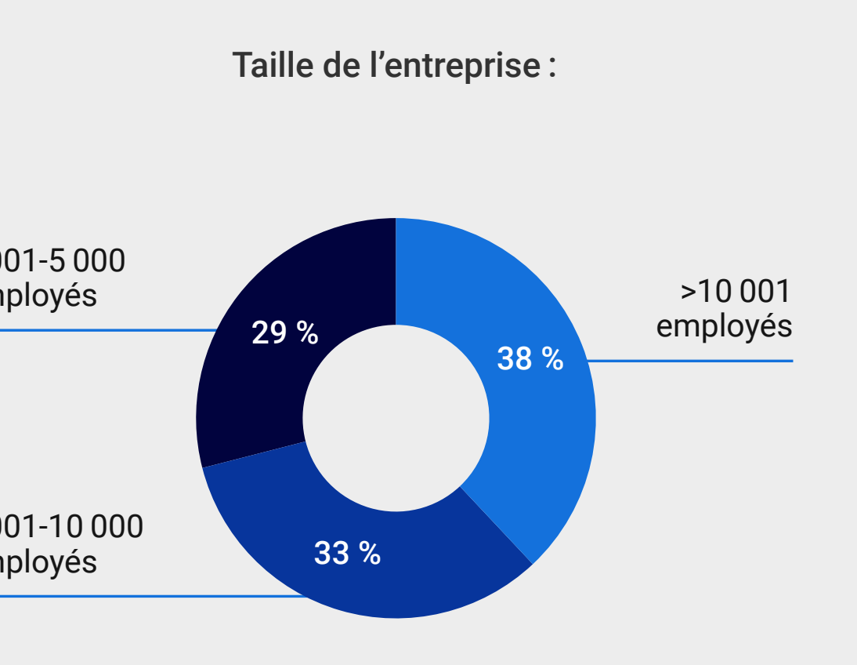
EN SAVOIR PLUS →

Répartition des personnes interrogées

Région







Gartner

Ce contenu présente des opinions et des points de vue exprimés par les utilisateurs et ne représente pas le point de vue de Gartner ; Gartner ne le cautionne pas et ne donne aucune garantie quant à son exactitude ou son exhaustivité.

Source : Gartner Peer Insights, étude Combating Ransomware