zscaler

THE RESILIENCE FACTOR

# L'industrie manufacturière : la confiance envers la cyber-résilience doit être justifiée

Un nouveau rapport de Zscaler, intitulé **« Déverrouiller le pouvoir de la résilience : pourquoi être « Resilient by Design » est le prochain impératif de cybersécurité »**, souligne qu'une hiérarchisation plus pertinente des priorités et qu'un investissement plus important s'imposent pour garantir que les stratégies de cyber-résilience soient adaptées aux inévitables scénarios de défaillance futurs.

## LA PRODUCTION INDUSTRIELLE : PRINCIPALES CONCLUSIONS

**Dans un contexte de menaces en constante évolution et d'un environnement opérationnel de plus en plus versatile, la continuité d'activité est en péril.**

**41 %** des entreprises ont connu un **scénario de défaillance important** au cours des 6 derniers mois

**59 %** des entreprises s'attendent à connaître un scénario de défaillance important au cours des **12 prochains mois**

## Les responsables informatiques se sentent bien préparés à ces scénarios de défaillance.

**47 %** des responsables informatiques estiment que leur infrastructure informatique est **hautement résiliente**

**78 %** qualifient de mature l'approche de cyber-résilience de leur entreprise

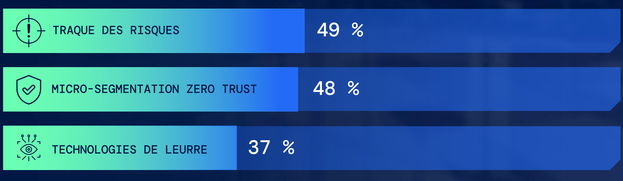
**97 %** estiment que leurs mesures actuelles de cyber-résilience sont **efficaces**

## Cependant, un examen plus approfondi révèle des incohérences, des lacunes et des pratiques peu efficaces.

SEULEMENT **46 %** des responsables informatiques déclarent que leur stratégie de cyber-résilience est **à jour** face à l'IA.

**45 %** admettent **ne pas avoir réévalué** leur stratégie de cyber-résilience au cours des 6 derniers mois.

## Moins de la moitié des entreprises utilisent tous les outils de sécurité proactifs suivants.




## Les dirigeants d'entreprise se montrent peu investis, ce qui constitue une problématique.

**SEULS 42 %** des responsables informatiques estiment que la cyber-résilience est une priorité absolue pour les dirigeants

**47 %** s'accordent à penser que le budget alloué à la cyber-résilience ne répond pas à l'escalade des besoins

**SEULS 35 %** déclarent que la stratégie de cyber-résilience est incluse dans la stratégie globale de résilience de leur entreprise

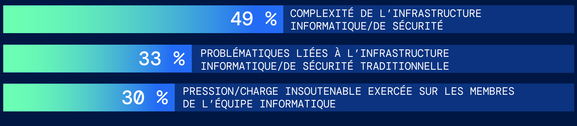
**SEULS 46 %** déclarent que le RSSI est impliqué dans la planification de la résilience

### Un changement de culture s'impose pour lever les principaux freins au déploiement d'une stratégie de cyber-résilience robuste.

**57 %** des responsables informatiques estiment que leur entreprise accorde une priorité excessive à la prévention dans sa stratégie de cybersécurité

**57 %** déclarent que leurs dirigeants continuent de penser d'un échec de la cybersécurité est lié à l'accès initial obtenu par un acteur malveillant.

**Les trois principaux freins à une meilleure résilience :**




## Intégrer d'emblée la cyber-résilience dans la stratégie d'entreprise.

Les responsables informatiques voient le lien entre une stratégie de cyber-résilience robuste et de meilleures performances d'entreprise, mais peinent à obtenir des résultats dans le cadre de leurs efforts actuels.

**58 %** constatent une **réduction** des pertes de données.

**54 %** observent une restauration **plus rapide** après un incident.

**51 %** font état d'une détection et d'un confinement **accélérés** des incidents.

Le contexte économique actuel exige que les entreprises du secteur de la production industrielle accordent davantage d'attention à la cyber-résilience, qu'elles la financent mieux, la révisent plus fréquemment et qu'elles augmentent leurs attentes à son égard. Un changement fondamental d'approche et de mentalité est indispensable pour faire de la cyber-résilience un élément essentiel de la stratégie de sécurité dès le départ. C'est ce que nous appelons l'approche **« Resilient by Design »**.

**Pour en savoir plus sur la mise en œuvre d'une approche « Resilient by Design », rendue possible par la plateforme Zero Trust Exchange, cliquez ici. Consultez le rapport.**

## MÉTHODOLOGIE

En décembre 2024, Zscaler a chargé Sapio Research de mener une enquête auprès de 1 700 décideurs informatiques sur 12 marchés (Australie, France, Allemagne, Inde, Italie, Japon, Pays-Bas, Singapour, Espagne, Suède, Royaume-Uni et Irlande, États-Unis). 302 de ces dirigeants informatiques travaillent dans des entreprises du secteur de la production industrielle.

## À PROPOS DE ZSCALER

Zscaler accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossée à plus de 160 data centers dans le monde, Zero Trust Exchange, basée sur le SASE, est la plus vaste plateforme de sécurité cloud opérant en mode inline.

zscaler