Informations sur la cyberrésilience

Lacunes en matière de cyberrésilience, menaces en pleine évolution, défenses optimisées par l'IA et stratégies de récupération

Les défis liés à la cyberrésilience s'intensifient à mesure que les cyberattaques et les lacunes en matière de protection des données augmentent les risques de perturbation. Les organisations dotées de stratégies de résilience matures* ont environ 3 fois plus de chances de récupérer correctement. En modernisant les stratégies de résilience, en améliorant les capacités de détection et en privilégiant une optimisation continue, les responsables IT peuvent réduire les risques et renforcer la confiance dans leur aptitude à s'adapter à des menaces en constante évolution.

Excès de confiance de la direction

63 % des professionnels de l'IT estiment que leur direction sous-estime la préparation aux cyberincidents. L'excès de confiance crée des zones d'ombre risquées qui retardent les investissements essentiels et laissent des vulnérabilités non corrigées.

Le fossé entre confiance et capacités

99,5 % des organisations ont mis en place des stratégies de cyberrésilience

Néanmoins, **57 %** n'ont pas réussi à récupérer efficacement lors de leur dernier test ou incident

Prévention ou récupération ? Une approche qui manque d'équilibre

78 %
estiment que leur organisation se concentre davantage sur la prévention des attaques que sur la préparation à leur capacité de récupération

Pourtant, seulement **30 %**
des organisations disposent d'une plateforme complète de détection des menaces englobant le stockage principal, le stockage de sauvegarde et l'infrastructure réseau

Et seulement **40 %**
ont réussi à contenir une attaque ou un cybercrident et à récupérer avec un impact minimal

Lorsque des violations se produisent (comme c'est inévitablement le cas), de nombreuses organisations ne sont par conséquent pas préparées à la phase de récupération, pourtant déterminante pour la survie de l'entreprise.

La voie à suivre :
Les organisations matures obtiennent des résultats

Les organisations dotées de stratégies de cyberrésilience matures ont environ 2,6 fois plus de chances de récupérer correctement

La maturité stratégique repose sur trois piliers essentiels pour créer une résilience à toute épreuve.

SÉCURISER :
Établir les bases de la confiance

Les organisations dotées de stratégies de cyberrésilience matures sont :

- **1,4 fois** plus susceptibles de protéger les appareils au moyen de contrôles de sécurité au niveau du firmware/BIOS
- **Plus susceptibles** d'utiliser le chiffrement pour les données au repos et en transit
- **Plus susceptibles** d'utiliser des cybercoffres-forts pour protéger les données stratégiques contre des menaces en constante évolution

Mais la sécurité n'est que le début. Le véritable avantage réside dans une détection intelligente capable d'identifier les menaces avant qu'elles ne compromettent vos actifs les plus précieux.

DÉTECTER :
Une intelligence toujours active

Le défi de la visibilité :
Seules 30 % des organisations disposent d'une détection des menaces robuste englobant le stockage de sauvegarde, le stockage de données principal et l'infrastructure réseau

La solution optimisée par l'IA :

- **62 %** privilégient les investissements dans la détection des menaces basée sur l'IA/le ML
- **48 %** analysent en profondeur les données de sauvegarde à l'aide de l'IA/du ML à la recherche d'indicateurs de compromission
- Les organisations dotées de stratégies matures sont **3,1 fois plus susceptibles** d'utiliser des outils d'IA/de ML et des playbooks d'atténuation proactive et de réponse

RÉCUPÉRER :
La préparation associée aux performances

L'avantage des tests :

- **55 %** des organisations qui simulent des cyberattaques tous les mois ou plus fréquemment réussissent à récupérer après des incidents
- **62 %** des organisations qui effectuent des tests moins d'une fois par mois réussissent à récupérer correctement après des incidents

Résultat :
Les organisations qui effectuent des tests fréquents sont beaucoup plus susceptibles d'atteindre à la fois leurs objectifs de temps de reprise et de perte de données maximale admissible que celles qui effectuent des tests occasionnels.

La voie vers l'excellence en matière de cyberrésilience

Les organisations dotées de stratégies de cyberrésilience matures sont 2 fois plus susceptibles de respecter systématiquement leurs SLA

Bâtir un socle solide
Mettez l'accent à la fois sur la prévention et une récupération rapide.

- **Sécuriser :** réduisez les risques grâce aux contrôles de sécurité au niveau du BIOS, au chiffrement des données et aux cybercoffres-forts destinés aux données critiques.
- **Détecter :** utilisez l'IA/le ML en temps réel pour détecter les menaces sur l'ensemble du stockage (stockage principal et de protection compris) et y répondre.
- **Récupérer :** effectuez régulièrement des tests de récupération ; les organisations qui en font chaque mois sont beaucoup plus susceptibles d'atteindre leurs objectifs de temps de reprise.

Prêt à renforcer votre cyberrésilience ?

Prêt à renforcer votre cyberrésilience ? Découvrez les principales conclusions de l'*étude Cyber Resilience Insights 2026 de Dell.*

DELL Technologies

Source : enquête de 2025 sur la cybersécurité réalisée par Vanson Bourne et Dell Technologies.

* Les organisations dotées de stratégies de cyberrésilience matures sont des organisations qui disposent d'une stratégie pleinement définie et optimisée en permanence, s'appuyant sur une analytique prédictive, une automatisation et des informations en temps réel (par exemple, flux de cyber-intelligence, ajustements fondés sur le ML, améliorations basées sur les KPI)