Renseignements sur la cyberrésilience

Découvrir les lacunes en matière de cyberrésilience, l'évolution des menaces, les défenses basées sur l'IA et les stratégies de reprise en Amérique du Nord

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 qui disposent de stratégies de résilience matures* sont presque trois fois plus susceptibles de reprendre leurs activités avec succès. En modernisant les stratégies de résilience, en améliorant les capacités de détection des menaces et en mettant l'accent sur l'optimisation constante des systèmes, les responsables des TI peuvent minimiser les risques et renforcer la confiance en leur capacité à s'adapter aux menaces en constante évolution.

Excès de confiance de la direction

69 % des professionnels des TI croient que la direction surestime leur niveau de préparation aux cyberévénements. Lorsque l'excès de confiance règne, cela crée des zones d'ombre dangereuses où certains investissements sont retardés et où certaines vulnérabilités ne sont pas renforcées.

Le fossé entre confiance et capacité

99 % des organisations disposent d'une stratégie de cyberrésilience en place

53 % n'ont pas réussi à assurer une reprise efficace lors de leur dernier test ou incident

Prévention ou reprise : une approche déséquilibrée

86 % estiment que leur organisation s'attache davantage à prévenir les attaques qu'à se préparer à la reprise en cas d'attaque

Pour l'instant, seulement **36 %** des organisations disposent d'une plateforme complète de détection des menaces pour l'unité de sauvegarde, l'unité de stockage des données principale et l'infrastructure du réseau

Et seulement **46 %** des organisations ont réussi à contenir la menace et à assurer une reprise avec un impact minimal lors d'une attaque ou d'un cyberincident

Par conséquent, lorsque des violations finissent inévitablement par se produire, de nombreuses organisations manquent de préparation pour la phase de reprise essentielle à la survie de l'entreprise.

La voie à suivre :

Les organisations avec une stratégie mature obtiennent des résultats

Les organisations qui disposent de stratégies de cyberrésilience matures sont presque trois fois plus susceptibles de reprendre leurs activités avec succès

Une stratégie mature s'exerce selon trois axes essentiels qui permettent de garantir une résilience inattaquable.

SÉCURITÉ :

Bâtir votre base de confiance

Les organisations dotées de stratégies de cyberrésilience matures sont :

- **2 fois** plus susceptibles de protéger leurs appareils à l'aide de contrôles de sécurité au niveau du micrologiciel ou du BIOS
- **Plus susceptibles d'**utiliser le chiffrement pour les données au repos et en transit
- **Plus susceptibles** d'utiliser des chambres fortes numériques pour protéger les données critiques contre les menaces en constante évolution

Mais la sécurité n'est que la pointe de l'iceberg. Le véritable avantage réside en la détection intelligente qui permet d'identifier les menaces avant qu'elles ne compromettent vos ressources les plus précieuses.

DÉTECTION :

Une intelligence qui ne dort jamais

Le défi de la visibilité :
Seulement 36 % des organisations disposent d'un système de détection des menaces robuste pour l'unité de sauvegarde, l'unité de stockage des données principale et l'infrastructure du réseau

La solution alimentée par l'IA :

- **65 %** des organisations mettent l'accent sur les investissements liés à la détection des menaces alimentée par l'IA ou l'apprentissage automatique
- **62 %** des organisations analysent les données de sauvegarde en profondeur à l'aide de l'IA ou de l'apprentissage automatique pour détecter les indicateurs de compromission
- Les organisations dotées de stratégies matures sont **3,2 fois plus susceptibles** d'utiliser les outils d'IA ou d'apprentissage automatique accompagnés de guides proactifs d'atténuation et de réponse

REPRISE :

Là où la préparation rencontre la performance

L'avantage des tests :

- **61 %** des organisations qui effectuent des simulations de cyberattaque mensuelles ou plus fréquentes ont repris leurs activités avec succès après des incidents
- **60 %** des organisations qui effectuent des tests moins d'une fois par mois n'ont pas été en mesure de reprendre leurs activités après des incidents

Le résultat :
Les organisations qui effectuent des tests fréquemment sont beaucoup plus susceptibles d'atteindre les objectifs relatifs au temps et au point de reprise que celles qui effectuent des tests occasionnellement.

Votre parcours vers l'excellence en matière de cyberrésilience

Les organisations dotées de stratégies de cyberrésilience matures sont 2,3 fois plus susceptibles de respecter systématiquement leurs ENS

Construire une base solide
Concentrez-vous à la fois sur la prévention et sur la reprise rapide.

- **Sécurité :** réduisez les risques grâce à des contrôles de sécurité au niveau du BIOS, au chiffrement des données et aux chambres fortes numériques pour les données critiques.
- **Détection :** utilisez l'IA ou l'apprentissage automatique en temps réel pour détecter et répondre aux menaces sur l'ensemble du stockage, y compris le stockage principal et le stockage de sauvegarde.
- **Reprise :** testez fréquemment vos procédures de reprise. Les organisations qui s'y soumettent chaque mois sont beaucoup plus susceptibles d'atteindre leurs objectifs en matière de reprise.

Prêt à améliorer votre cyberrésilience?

Prêt à améliorer votre cyberrésilience? Lisez toutes les conclusions importantes de l'*étude 2026 sur la cyberrésilience de Dell.*

DELL Technologies

Tous les répondants pour l'Amérique du Nord viennent des États-Unis.
Source : Vanson Bourne et sondage Dell Technologies sur la cyberrésilience 2025

* Les organisations dotées de stratégies de cyberrésilience matures sont définies comme celles disposant d'une stratégie pleinement établie et continuellement optimisée, qui s'appuie sur les analyses prédictives, l'automatisation et l'information en temps réel (p. ex., les flux de surveillance des menaces, les ajustements basés sur l'apprentissage automatique et les indicateurs clés de performance pour orienter les améliorations)