# La cyberrésilience en action

Évaluation de la préparation globale des entreprises en matière de sécurité/détection/récupération
Enquête et résultats
Janvier 2026

DELL Technologies

# Programme

- Objectifs et données firmographiques
- Le fossé de la cyberrésilience
- Sécurisé
- Détecter
- Récupération
- Complexité, culture et perspectives d’avenir

# Objectifs métiers

- Positionner Dell en tant que leader éclairé et partenaire stratégique de la cyberrésilience
- Réaffirmer la décision de passer du concept de « protection des données » à celui de « cyberrésilience »

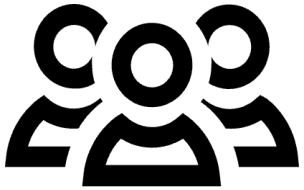
# Objectifs de l’étude

- Évaluer la maturité et l’intégration des stratégies de cyberrésilience
- Évaluer l’efficacité des pratiques de sécurité, de détection et de récupération des organisations
- Comprendre les obstacles à l’amélioration de la cyberrésilience, notamment les lacunes en matière de compétences, le budget et la complexité
- Savoir comment les organisations sécurisent leur environnement IT et protègent leurs données face aux menaces de ransomware

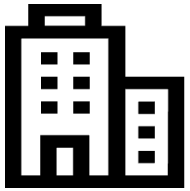
# Qui avons-nous interrogé ?

Les personnes ont été interrogées en juillet et octobre 2025

850 décideurs IT issus d'organisations internationales



Organisations de plus de 1 000 collaborateurs



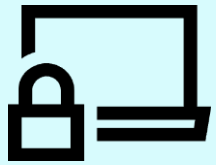
Organisations issues d'un éventail de secteurs publics et privés

Personnes interrogées : membres du conseil d'administration, dirigeants Cadres supérieurs Cadres intermédiaires

# Principales conclusions

**39 %**

des organisations disposent d'une stratégie de cyberrésilience pleinement établie et optimisée en permanence



L'optimisation continue est essentielle : sans elle, les stratégies peuvent rapidement devenir obsolètes face à l'évolution des menaces, exposant ainsi les organisations à des risques plus élevés

**46 %**

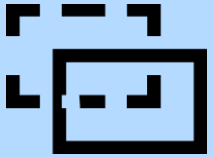
conviennent que leurs données de sauvegarde ne sont pas aussi protégées qu'elles devraient l'être

Renforcer la protection des sauvegardes est essentiel pour garantir que la récupération reste possible lorsque les systèmes principaux sont compromis.

Sécurisé

**30 %**

utilisent une plateforme complète pour la détection des menaces sur le réseau, la sauvegarde et le stockage principal



Sans détection unifiée, la visibilité des menaces et les temps de réponse peuvent être plus lents, ce qui augmente le risque de violations non détectées.

Détecter

**55 %**

des organisations ayant mené des simulations de cyberattaque mensuelles (ou plus fréquentes) ont réussi leur exercice/surmonté le cyberincident

Des tests fréquents aident les équipes à se préparer face aux risques. Les équipes mal préparées risquent de retarder leur capacité de réponse et de récupération au moment le plus crucial.

Récupération

**63 %**

pensent que leur direction surestime la préparation de l'organisation à un événement cybernétique majeur

Un excès de confiance peut freiner les investissements, retarder la planification des réponses et laisser des vulnérabilités critiques non remédiées.

DELL Technologies

# Section 1 : le fossé de la cyberrésilience

## Comprendre le problème et l’urgence d’évoluer

# L’optimisation continue des stratégies de résilience améliore la reprise… mais la réussite n’est pas garantie

**99,5 %**

disposent d’une stratégie de cyberrésilience sous une forme ou une autre

**39 %**

estiment que cette stratégie est pleinement établie et continuellement optimisée (stratégie mature)

**57 %**

n’ont pas réussi à contenir la menace ou à se remettre efficacement après leur dernier test ou incident

Les organisations dotées de stratégies de cyberrésilience matures ont **2,6 fois plus de chances de se remettre rapidement et efficacement d’une cyberattaque**

**65 %** contre **25 %**

**63 %**

pensent que **leur direction surestime la préparation de l’organisation** à un événement cybernétique majeur

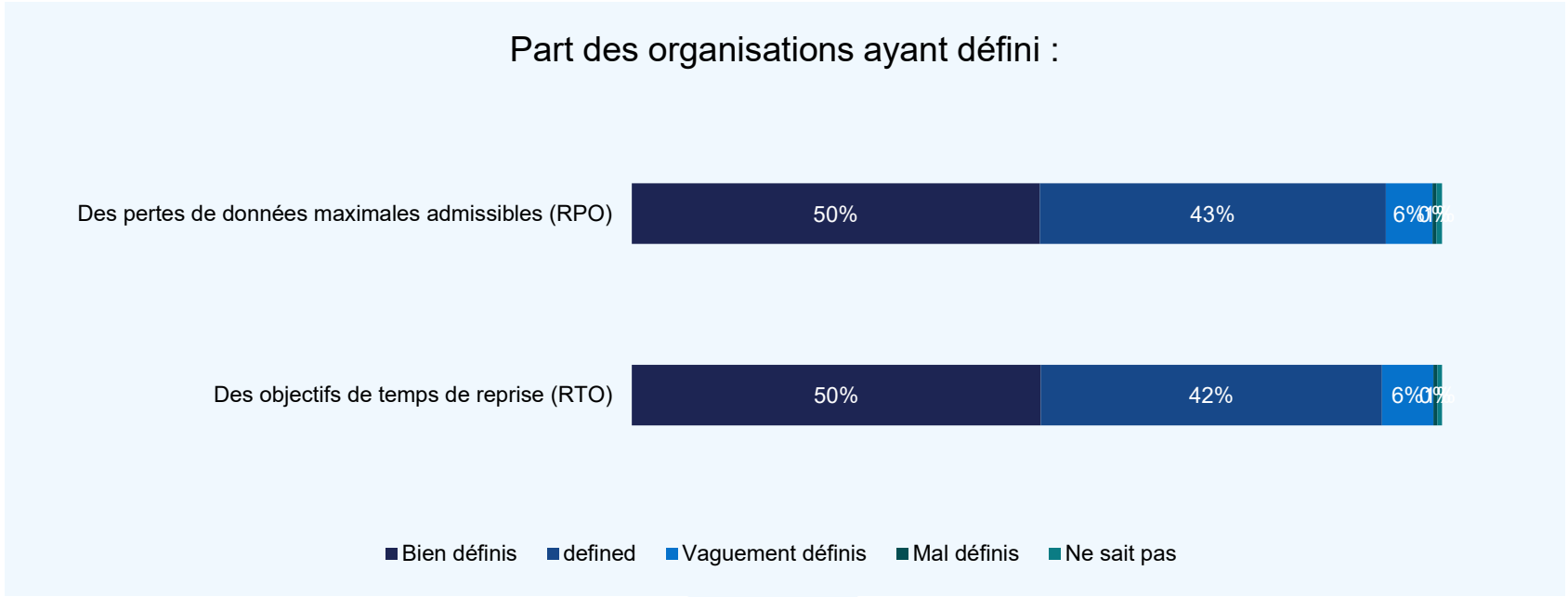
# Pourquoi cela est important aujourd'hui

**97 %**

reconnaissent la nécessité de renforcer continuellement leur organisation face à l'évolution des menaces

**78 %**

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




**32 %**

ont bien défini **à la fois les RTO et les RPO**

Parmi celles disposant d'une stratégie de cyberrésilience mature

**58 %**

ont bien défini les RTO et les RPO

# Section 2 : sécuriser

## Prévention des attaques et renforcement du parc numérique

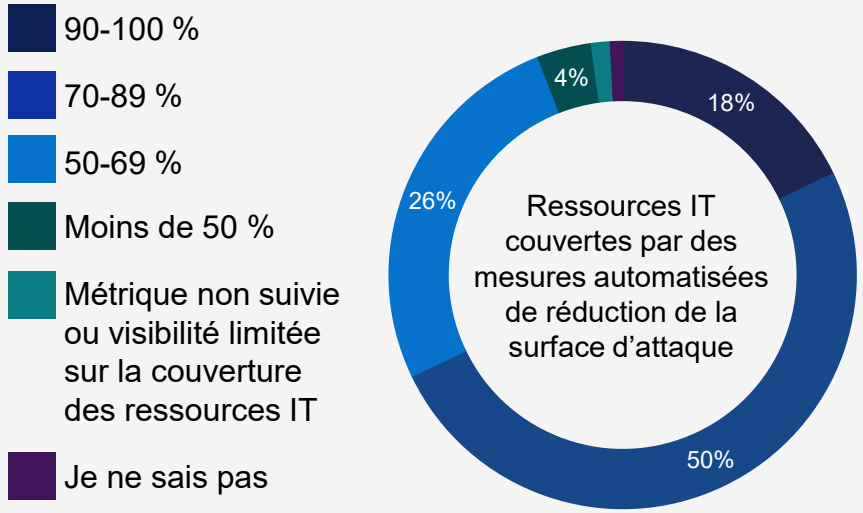
# Lacunes en termes de visibilité et de protection

**46 %**

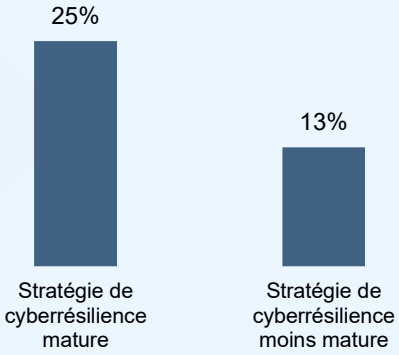
conviennent que leurs données de sauvegarde ne sont pas aussi protégées qu'elles devraient l'être

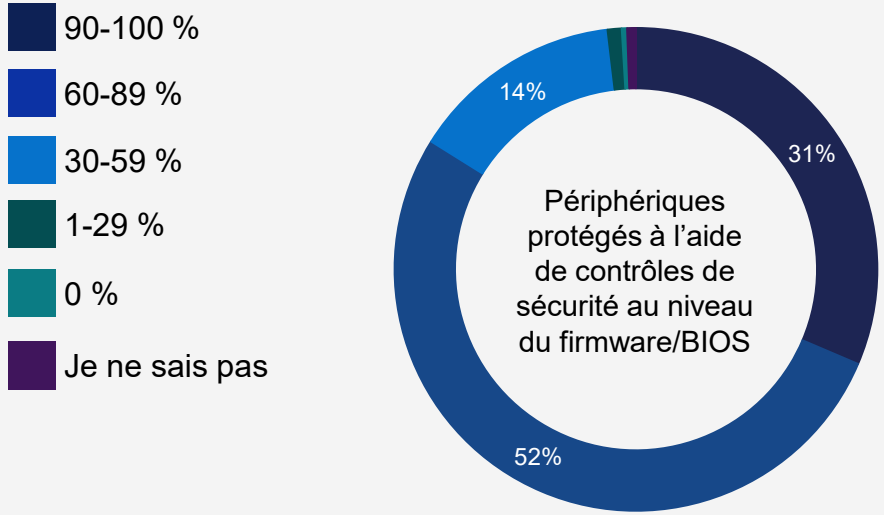
| | |
|---|---|
| S/O | **59 %** |
| EMEA | **43 %** |
| Amérique latine | **41 %** |
| APJ | **39 %** |

## L'optimisation continue n'élimine pas les lacunes de couverture, mais offre aux organisations un avantage stratégique en matière de résilience

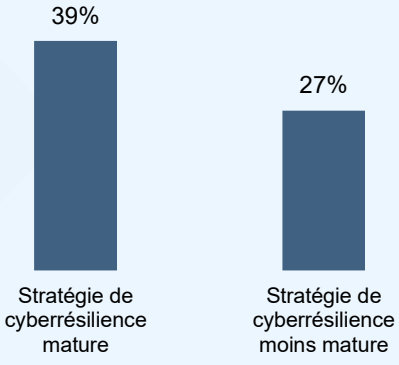



**Organisations disposant d'une couverture de 90 à 100 % :**




**Organisations disposant d'une couverture totale ou presque (90 à 100 %) :**



# De l’intégrité pré-déploiement à la récupération post-attaque : renforcez la sécurité d’une extrémité à l’autre

Processus/méthodes employés par les organisations pour assurer l’intégrité des logiciels et du matériel IT

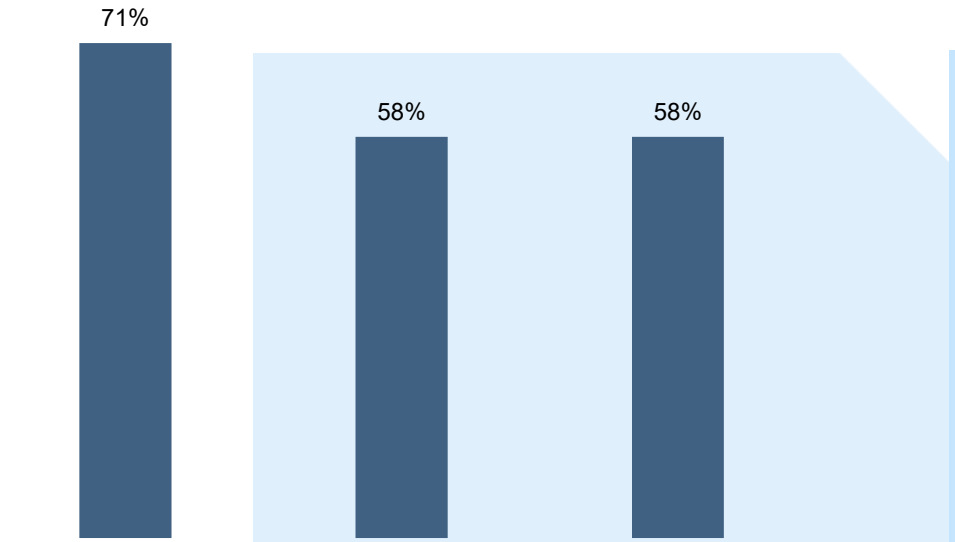
**72 %**

se tournent vers des fournisseurs pour obtenir des certifications, des attestations et des systèmes dotés d’outils intégrés qui vérifient l’intégrité des composants

**64 %**

effectuent des audits internes ou des examens manuels pendant la préparation/le déploiement

Méthodes utilisées par les organisations pour protéger les données critiques en cas d’attaques par ransomware




Les organisations disposant de stratégies de résilience matures sont plus susceptibles d’utiliser :

- **Chiffrement de données (59 % contre 57 %)**
- **Cybercoffres-forts (63 % contre 55 %)**

par rapport aux organisations disposant de stratégies de résilience moins matures

# Section 3 : détecter

## Identification et lutte contre les menaces avant qu'elles n'aient un impact

# L’IA et l’automatisation peuvent identifier les menaces avant que celles-ci ne compromettent les sauvegardes

**38 %**

des organisations utilisent des outils d’IA/ML avec des playbooks d’atténuation et de réponse proactives

Les organisations dotées d’une stratégie de cyberrésilience mature sont **3,1 fois** plus susceptibles de le faire

**65 %** contre **21 %**

**48 %**

des organisations **utilisent largement l’IA/le ML pour analyser les données de sauvegarde** à la recherche d’indices de compromission

**L’utilisation étendue** de l’IA/du ML est **2,3 fois plus fréquente dans les organisations dotées d’une stratégie de cyberrésilience mature**

**72 %** contre **32 %**

**83 %**

estiment que les acteurs de menaces **attaquent de plus en plus les sauvegardes** lors des attaques par ransomware

**62 %** investissent en priorité dans l’automatisation et la détection des menaces basée sur l’IA/le ML

# Une visibilité incomplète accroît les risques

**54 %**

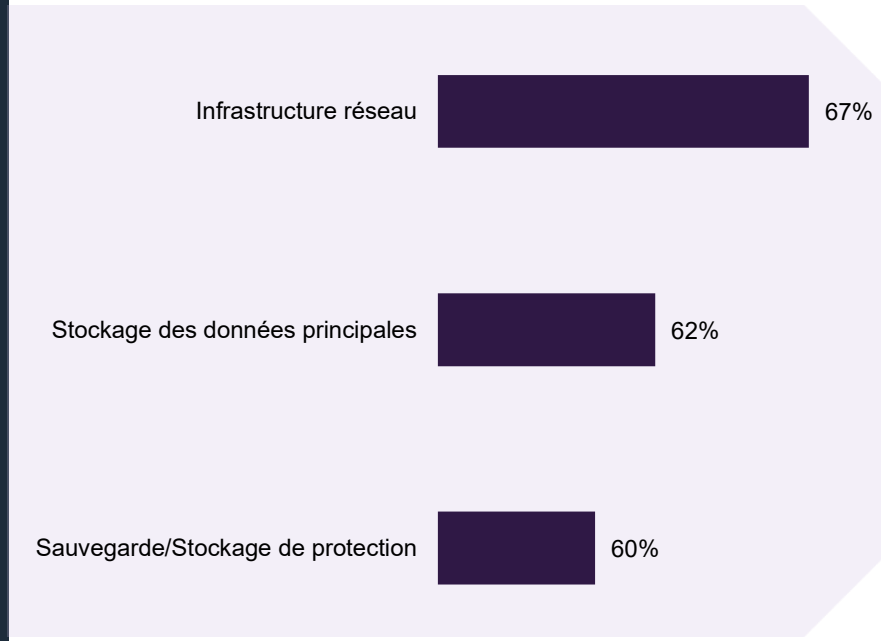
affirment disposer d'une visibilité accrue sur les activités suspectes ou les données compromises au sein de leurs systèmes de sauvegarde

**74 %** d'organisations dotées d'une stratégie de cyberrésilience mature

comparé aux

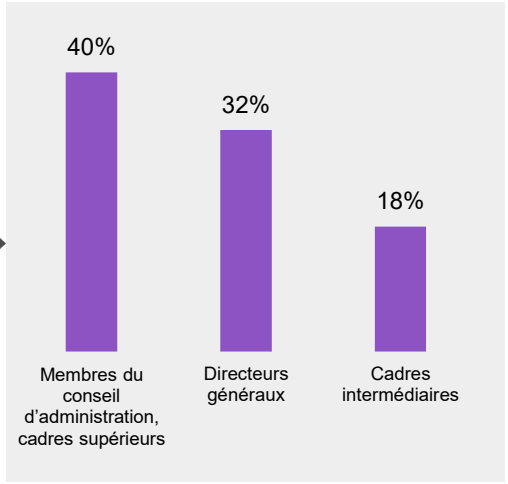
**42 %** d'organisations dotées d'une stratégie de cyberrésilience moins mature

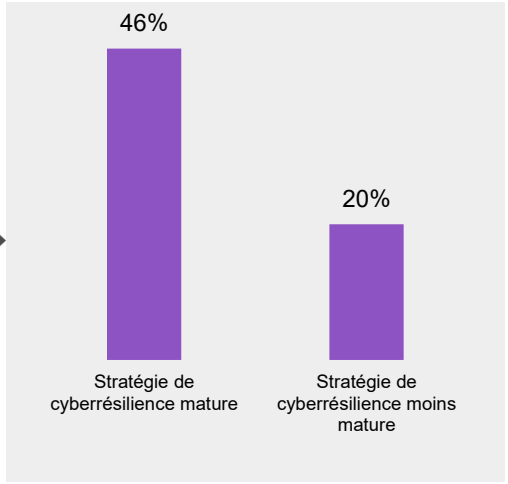
Organisations disposant d'une plateforme robuste pour la détection des menaces dans les domaines suivants




**30 %**

disposent d'une plateforme complète **couvrant les 3 domaines**



# Section 4 : récupérer

## Reprise rapide et conforme aux attentes du SLA

# État de la reprise : de nombreuses organisations atteignent leurs objectifs, mais une amélioration continue est essentielle pour rester en phase avec l'évolution du paysage des menaces

## 40 %

**ont contenu efficacement la menace et se sont remises avec succès** avec un impact minimal

Les **membres du conseil d'administration (53 %)** sont plus susceptibles d'affirmer cela que les **cadres intermédiaires (30 %)**

## 54 %

des organisations ont atteint leurs **objectifs RTO/RPO**

Par poste : membres du conseil d'administration (66 %) par rapport aux cadres intermédiaires (45 %)

## N° 4

Le principal moteur de l'investissement en cybersécurité est un **récent incident de cybersécurité ou un incident évité de justesse** au sein de l'organisation

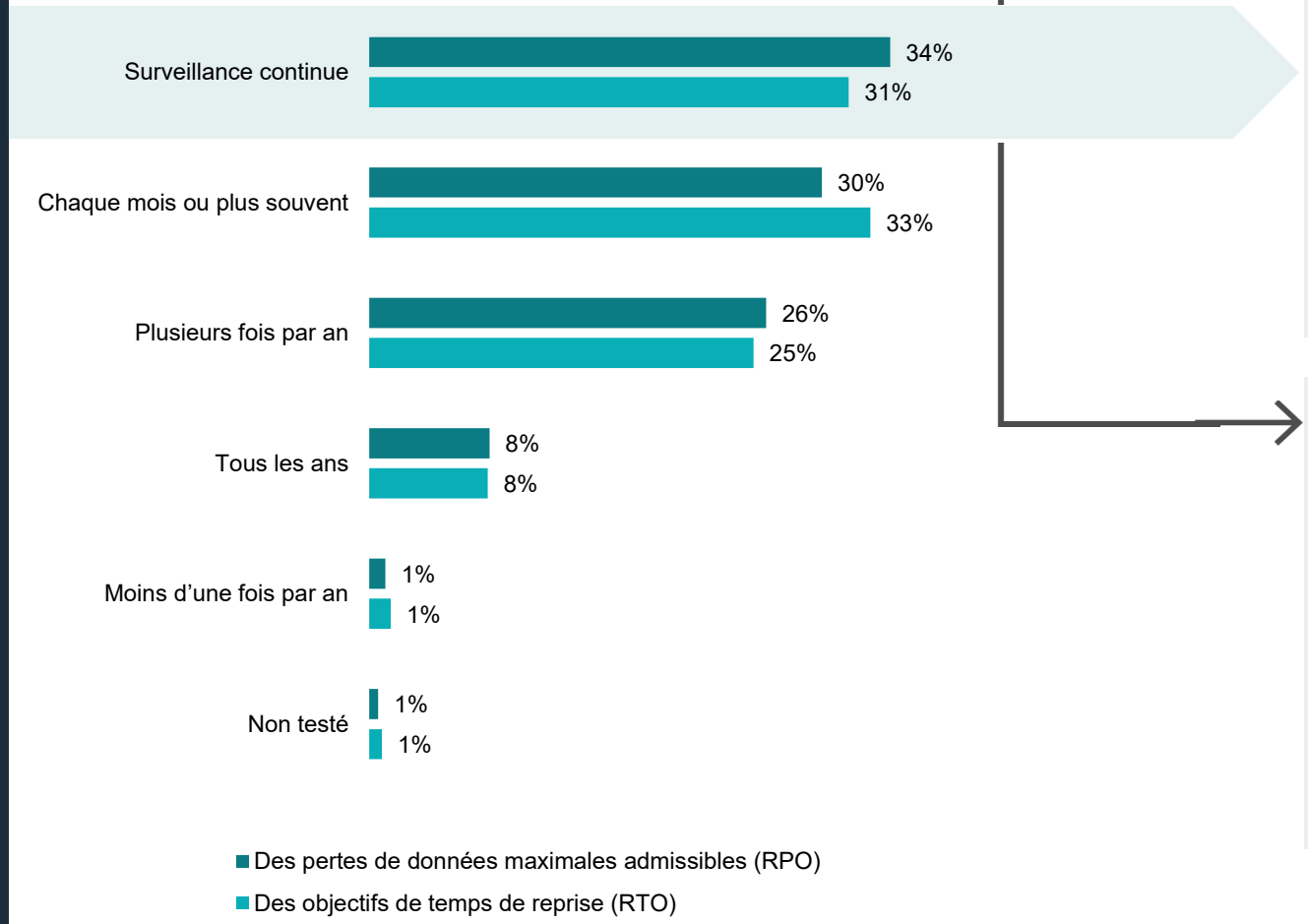
57 % améliorent les capacités de résilience pour **répondre aux exigences réglementaires ou de conformité**

# Des tests fréquents peuvent améliorer la récupération

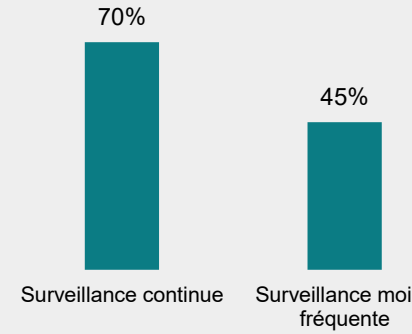
> En fin de compte, la résilience est renforcée par une culture de vigilance et d'amélioration continue.
>
> *Directeur général, entreprise de services aux consommateurs, Brésil*

# Les tests sont essentiels à la résilience, car ils offrent aux organisations de meilleures chances de récupération

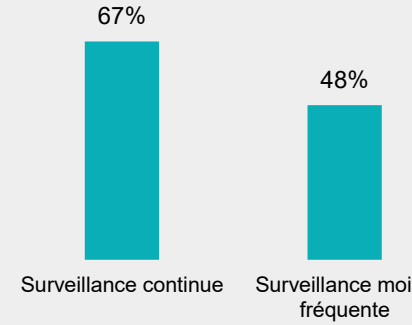
## Fréquence des tests RTO/RPO




Atteinte des objectifs RPO/RTO grâce aux tests : pertes de données maximales admissibles (RPO)




Atteinte des objectifs RPO/RTO grâce aux tests : objectifs de temps de reprise (RTO)



# Les tests sont fondamentaux pour assurer la résilience

**48 %**

ont déclaré que les tests de cybersécurité de leur organisation ne simulent pas de manière réaliste les techniques d'attaque modernes

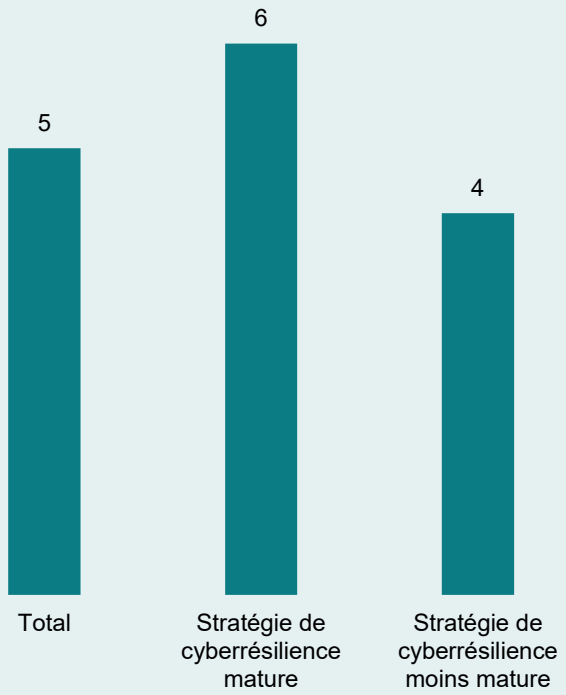
**53 %** des membres du conseil d'administration et des cadres supérieurs

comparé aux

**48 %** des cadres intermédiaires

## La pratique régulière est essentielle pour stimuler la récupération, mais les organisations doivent planifier en permanence face à l'évolution des menaces

Nombre moyen de simulations de cyberattaque par an




**55 %**

des organisations ayant mené des simulations de cyberattaque **mensuelles (ou plus fréquentes)** ont réussi leur exercice/surmonté le cyberincident

**35 %**

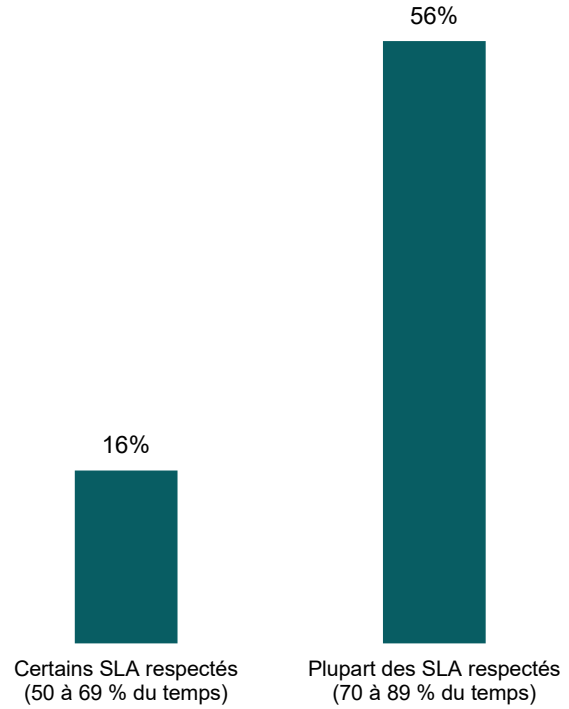
des organisations ayant mené des simulations de cyberattaque **moins d'une fois par mois** ont réussi leur exercice/surmonté le cyberincident

> *Plutôt que de nous concentrer sur la couverture ou des tests ponctuels, nous devons tester et évaluer de manière globale toutes les surfaces d'attaque potentielles.*
>
> Directeur général, entreprise IT et télécom, Royaume-Uni

> *Les cyberattaques nous rappellent l'importance d'exercices de sécurité réguliers.*
>
> *Les formations de sensibilisation à la sécurité ont été renforcées, ce qui permet à chaque employé d'identifier les menaces potentielles.*
>
> Membre du conseil d'administration, entreprise de construction et d'immobilier, Australie

# Les SLA en sont la preuve : les organisations disposant de stratégies matures tiennent leurs promesses en matière de reprise

**Part des organisations respectant les SLA pour la récupération des systèmes critiques**



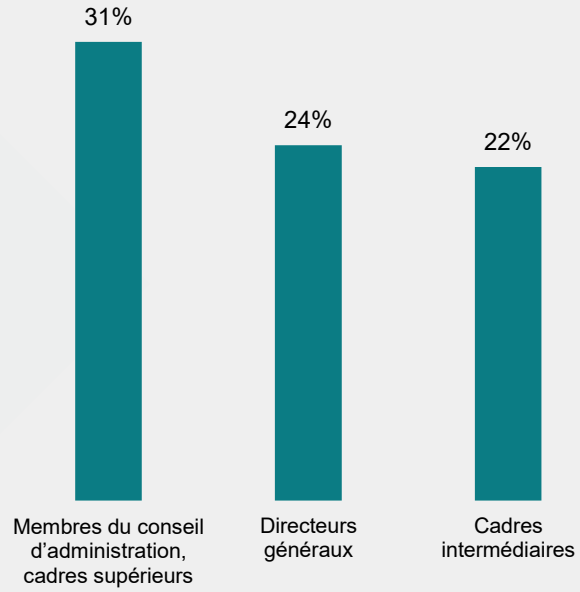


**2 x**

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

**36 %** contre **18 %**

Par poste :



# Section 5 : complexité, culture et perspectives d'avenir

## Obstacles organisationnels et plans d'investissement futurs

# La complexité, les lacunes en matière de compétences et l'excès de confiance menacent la cyberrésilience, mais l'IA et la formation pourraient être d'une précieuse aide

**Principaux défis :**

| | |
|---|---|
| Complexité de l'environnement IT | 49 % |
| Limitations budgétaires | 42 % |
| Manque de personnel qualifié | 39 % |
| Fragmentation des fournisseurs/outils | 38 % |
| Priorisation faible de la part des dirigeants | 23 % |

Les grandes organisations sont plus susceptibles d'être confrontées à ce défi :

- 50 % 5 000 collaborateurs ou plus
- 50 % 3 000 à 4 999 collaborateurs
- 46 % 1 000 à 2 999 collaborateurs

**63 %**

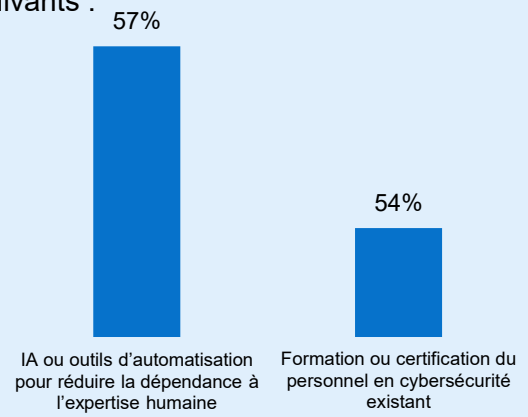
pensent que leur direction surestime la préparation de l'organisation à un événement cybernétique majeur

**96 %**

reconnaissent qu'elles ont des lacunes de compétences ou d'expertise en cybersécurité

**MAIS…**

Les organisations agissent via les moyens suivants :



# Anticiper les investissements

## N° 1

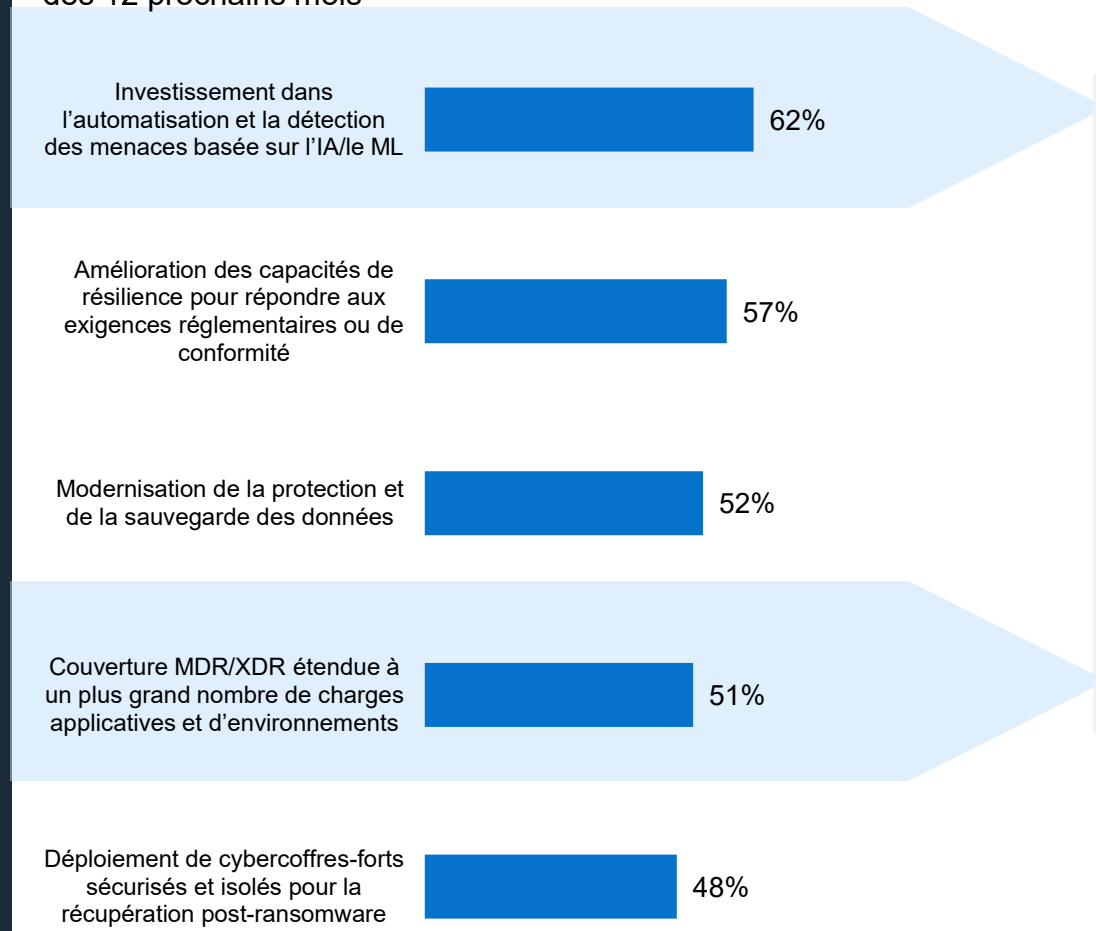
L'évolution du paysage des menaces est le premier facteur d'investissement

## 97 %

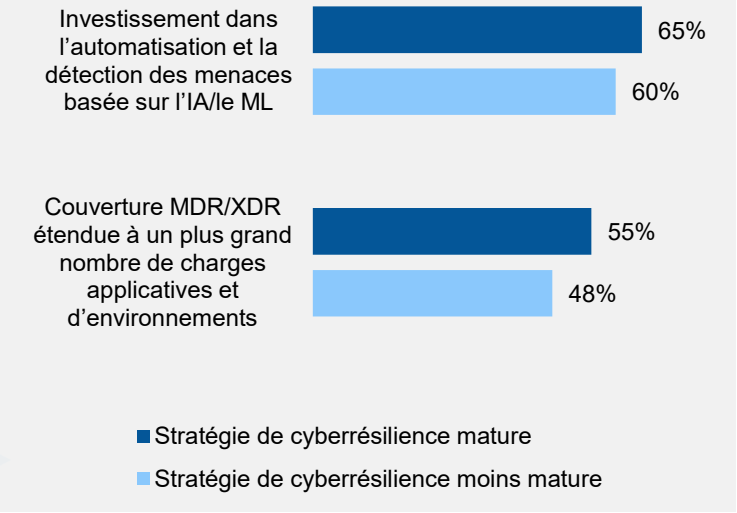
« Mon organisation doit constamment renforcer sa sécurité face à l'évolution des menaces »

## Pour maintenir une position mature, l'investissement et l'optimisation continus représentent la voie à suivre

Investissements en cyberrésilience prioritaires au cours des 12 prochains mois




### Les organisations cyberrésilientes et matures investissent en permanence

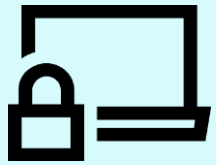


# Principaux points à retenir

# Principales conclusions

**39 %**

des organisations disposent d'une stratégie de cyberrésilience pleinement établie et optimisée en permanence



L'optimisation continue est essentielle : sans elle, les stratégies peuvent rapidement devenir obsolètes face à l'évolution des menaces, exposant ainsi les organisations à des risques plus élevés

**46 %**

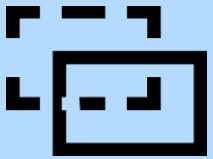
conviennent que leurs données de sauvegarde ne sont pas aussi protégées qu'elles devraient l'être

Renforcer la protection des sauvegardes est essentiel pour garantir que la récupération reste possible lorsque les systèmes principaux sont compromis.

Sécurisé

**30 %**

utilisent une plateforme complète pour la détection des menaces sur le réseau, la sauvegarde et le stockage principal



Sans détection unifiée, la visibilité des menaces et les temps de réponse peuvent être plus lents, ce qui augmente le risque de violations non détectées.

Détecter

**55 %**

des organisations ayant mené des simulations de cyberattaque mensuelles (ou plus fréquentes) ont réussi leur exercice/surmonté le cyberincident

Des tests fréquents aident les équipes à se préparer face aux risques. Les équipes mal préparées risquent de retarder leur capacité de réponse et de récupération au moment le plus crucial.

Récupération

**63 %**

pensent que leur direction surestime la préparation de l'organisation à un événement cybernétique majeur

Un excès de confiance peut freiner les investissements, retarder la planification des réponses et laisser des vulnérabilités critiques non remédiées.

DELL Technologies