

RAPPORT SUR LA CYBER-RÉSILIENCE

Être préparé aux risques ou y être exposé : Le fossé de la cyber-résilience dans les entreprises de taille moyenne

On parle beaucoup de détection et de prévention des cyberattaques, mais la réalité est tout autre. Il ne suffit plus de prévenir et de détecter. Même les entreprises les plus avancées sont victimes de perturbations paralysantes dont les répercussions s'étendent des opérations informatiques à la salle du conseil, et au-delà.

Afin de comprendre les causes de cette situation et ce qui distingue les entreprises résilientes de celles qui restent en difficulté, Cohesity a interrogé 3 200 décideurs en charge des opérations informatiques et de sécurité, dans 11 pays. Parmi les personnes interrogées figuraient près de 1 000 participants issus d'entreprises de taille moyenne. Leurs réponses révèlent une fracture croissante en matière de résilience entre les entreprises prêtes à faire face au risque, capables d'assurer une restauration rapide et maîtrisée, et leurs homologues plus exposées, qui demeurent vulnérables à des interruptions prolongées ainsi qu'aux conséquences financières qui en découlent.

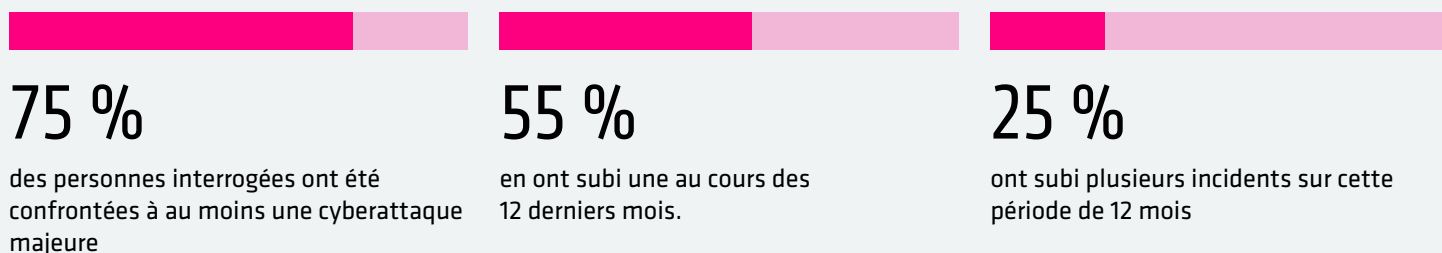
Notre étude examine les impacts concrets des cyberattaques majeures, la manière dont les entreprises de taille moyenne ont auto-évalué leur cyber-résilience par rapport aux bonnes pratiques, et les mesures qu'elles ont prises pour détecter ces incidents, y répondre et restaurer leur activité. Elle met également en évidence les enseignements qu'elles en ont tirés, et la manière dont elles se tournent vers l'IA et l'automatisation pour accélérer leur résilience et combler le fossé.



CYBERATTQUES MAJEURES : LA NOUVELLE RÉALITÉ DES ENTREPRISES MODERNES

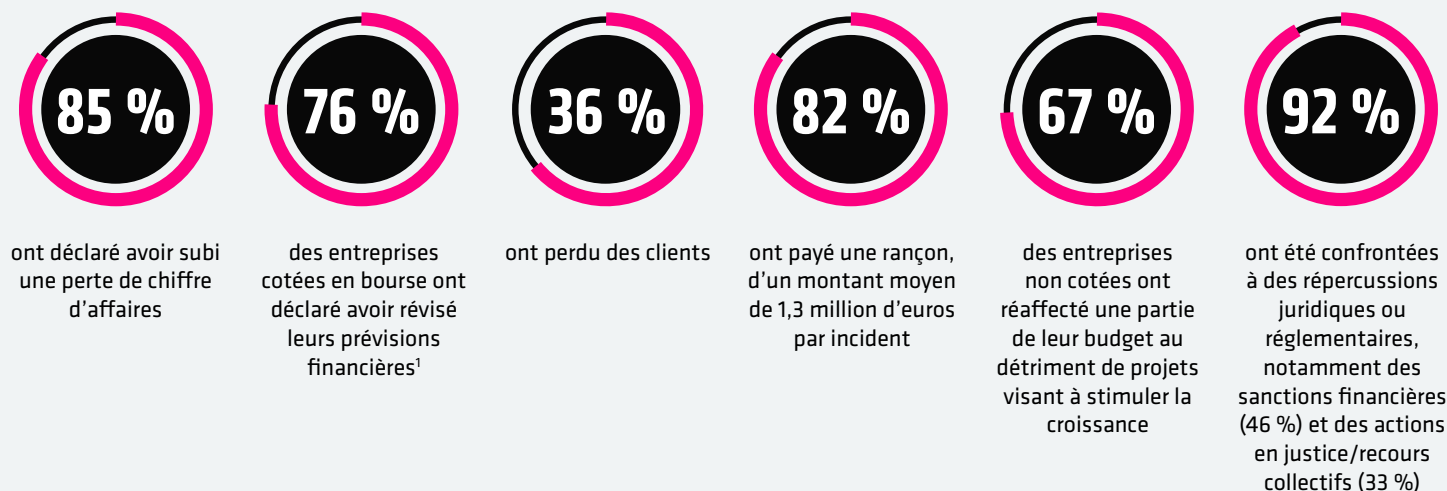
Tous les cyber incidents ne se valent pas. De nombreuses entreprises gèrent quasi-quotidiennement des tentatives de phishing, des scans de logiciels malveillants ou des pannes système. Mais les cyberattaques majeures sont différentes. Notre enquête définit une cyberattaque majeure comme un incident ayant causé un impact mesurable financier, réputationnel, opérationnel ou en matière de perte de clients.

DANS LES ENTREPRISES DE TAILLE MOYENNE, CES ATTAQUES LOURDES EN CONSÉQUENCES NE SONT PLUS L'EXCEPTION : ELLES S'INSCRIVENT DÉSORMAIS DANS UNE DYNAMIQUE RÉCURRENTÉ.



LE VÉRITABLE COÛT DES CYBERATTQUES MAJEURES

DES PRESSIONS FINANCIÈRES ET RÉGLEMENTAIRES SE SONT ÉGALEMENT FAIT SENTIR AU SEIN DES ENTREPRISES DE TAILLE MOYENNE QUE NOUS AVONS INTERROGÉES :



¹ Bien que relativement peu d'entreprises cotées en bourse aient officiellement annoncé avoir révisé leurs résultats suite à un cyber incident, ces conclusions suggèrent que les répercussions financières et opérationnelles vont bien au-delà de ce que révèlent les documents publics.

DE LA CONFIANCE MALGRÉ LES CONSÉQUENCES

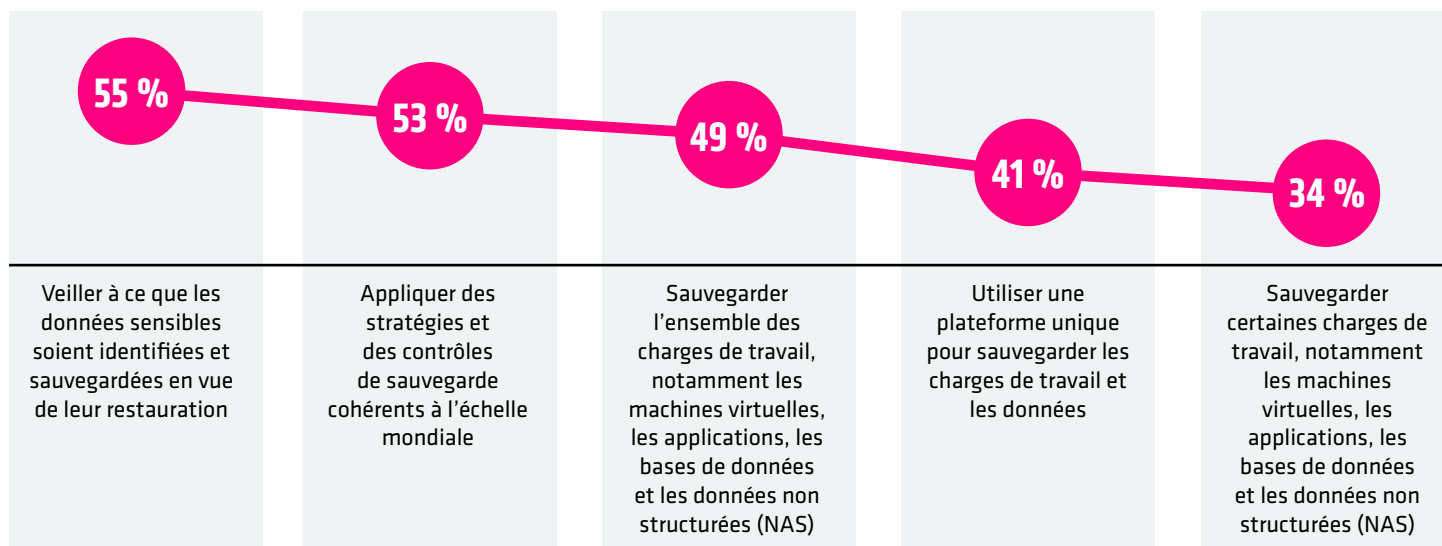
Compte tenu de l'ampleur des répercussions financières et opérationnelles révélées par notre étude, on pourrait s'attendre à ce que la résilience organisationnelle soit un sujet de préoccupation très répandu. Cependant, de nombreuses personnes interrogées (47 %) se sont dites totalement convaincues que leur stratégie de cyber-résilience pouvait résister aux menaces actuelles. Ce niveau de confiance contraste fortement avec les impacts majeurs subis par bon nombre de ces mêmes entreprises.

CE QUE LES ENTREPRISES FONT (ET NE FONT PAS)

Nous avons voulu aller plus loin et identifier les lacunes en matière de résilience. Pour ce faire, nous avons demandé aux personnes interrogées de décrire leur approche concernant certaines pratiques et capacités clés associées aux cinq dimensions fondamentales de la cyber-résilience : **la protection des données, la restauration des données, la détection et l'analyse des menaces, la résilience des applications et l'optimisation de la posture des risques liés aux données.**

LA PROTECTION DES DONNÉES RESTE FRAGMENTÉE DANS LES ENVIRONNEMENTS HYBRIDES ET MULTI-CLOUD

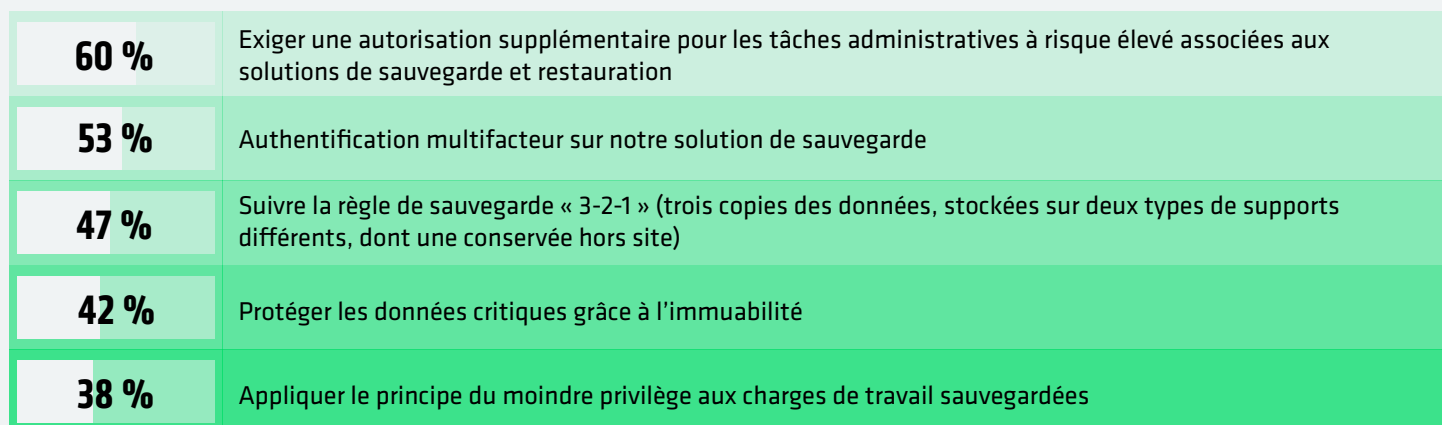
Que fait votre entreprise pour protéger toutes ses données dans des environnements hybrides et/ou multi-cloud ?



Un peu plus de la moitié des entreprises de taille moyenne veillent à ce que les données sensibles soient identifiées et sauvegardées pour permettre la restauration. À peu près la même proportion applique des stratégies et des contrôles de sauvegarde cohérents à l'échelle mondiale. Moins de la moitié sauvegardent toutes les charges de travail ou utilisent une plateforme unique pour protéger les charges de travail et les données. Un tiers ne protège par sauvegarde qu'une partie des charges de travail. Cette fragmentation limite la visibilité et la cohérence entre les environnements. La maturité en cyber-résilience dépend de la convergence de la sauvegarde et de la restauration/reprise au sein d'une plateforme unique, intelligente, et sécurisée par une approche fondée sur les principes du Zero Trust.

LES MESURES DE CAPACITÉ DE RÉCUPÉRATION DES DONNÉES SONT COURANTES, MAIS LEUR MATURITÉ VARIE

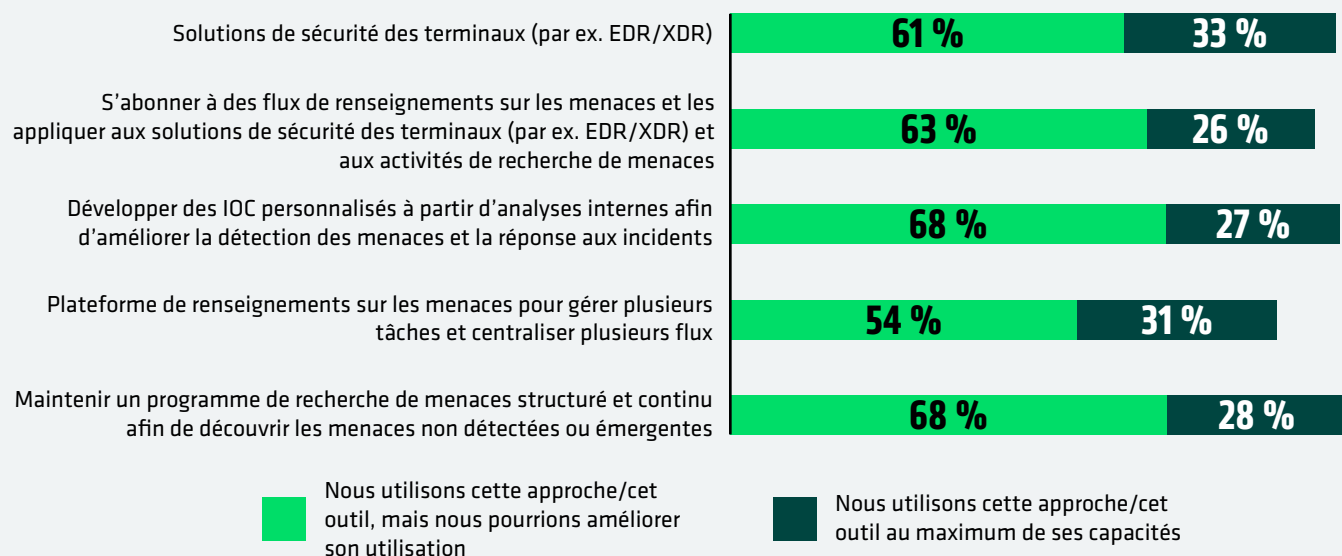
Que fait votre entreprise pour garantir la capacité de récupération de ses données ?



De nombreuses entreprises de taille moyenne ont renforcé les contrôles d'accès autour des environnements de sauvegarde, et plus de la moitié nécessitent une autorisation administrative supplémentaire pour les tâches à risque élevé. Environ la moitié appliquent l'authentification multifacteur, et presque la moitié appliquent la règle de sauvegarde 3-2-1. Moins de la moitié protègent les données critiques à l'aide de l'immuabilité ou mettent en œuvre des droits d'accès fondés sur le principe du moindre privilège. Ces lacunes ne permettent pas de garantir une restauration complète. Une cyber-résilience mature repose sur des copies de restauration vérifiées, isolées et infalsifiables.

LES OUTILS DE DÉTECTION ET D'ANALYSE DES MENACES SONT SOUS-UTILISÉS

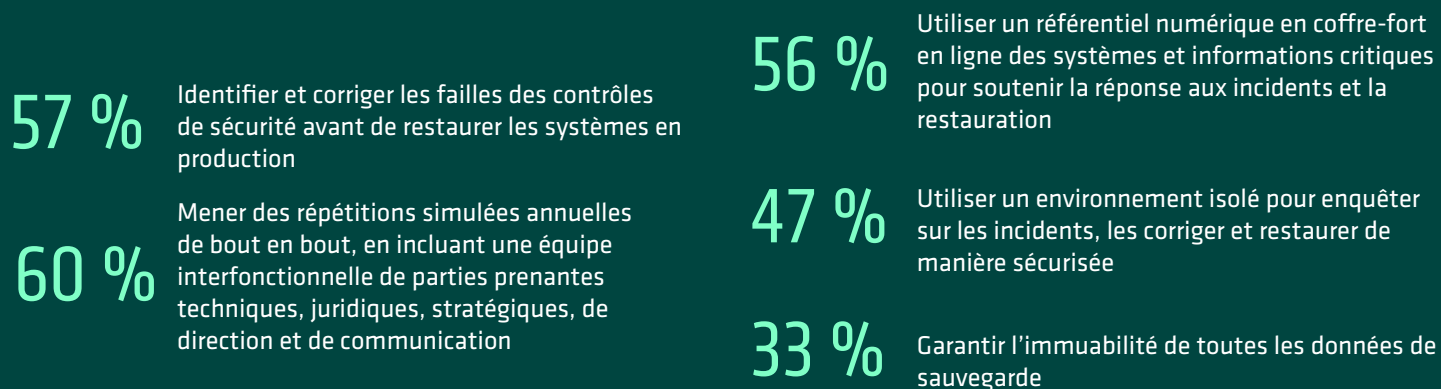
Dans quelle mesure votre entreprise utilise-t-elle chacun des outils ou méthodes suivants pour détecter et enquêter sur les menaces ?



Les solutions de détection et d'analyse des menaces sont largement mises en place, mais restent fréquemment sous-utilisées. La plupart des entreprises de taille moyenne ont recours à des solutions de sécurité des terminaux, à des flux de renseignements sur les menaces, à des indicateurs de compromission personnalisés, à des plateformes de renseignements sur les menaces et à des programmes structurés de recherche proactive de menaces. Pourtant, seule une minorité en tire pleinement parti. Une cyber-résilience mature repose sur l'intégration de ces outils dans une boucle continue de renseignement, afin d'améliorer la visibilité, la détection et la réponse.

LES MESURES DE RÉSILIENCE INCOMPLÈTES AUGMENTENT LE RISQUE DE RÉINFECTION

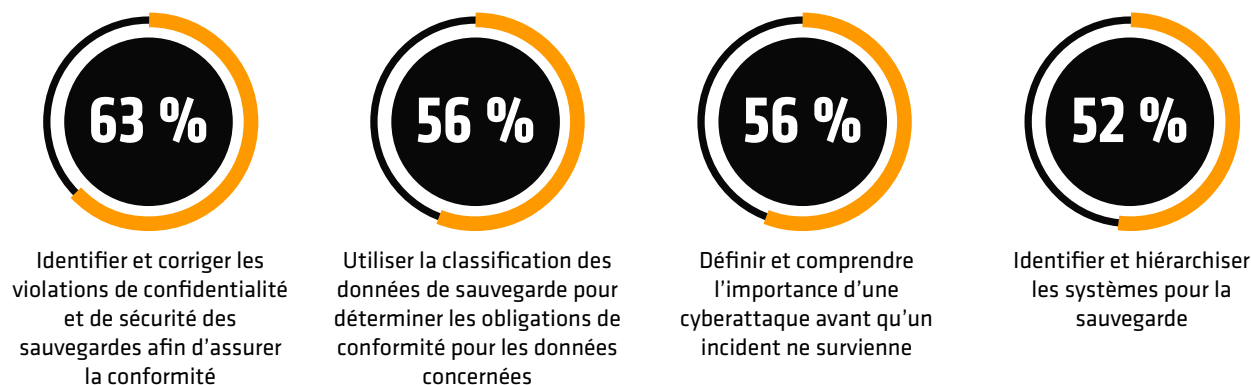
Que fait ou ferait votre entreprise pour garantir la résilience des applications face aux cyberattaques ?



L'approche des entreprises de taille moyenne en matière de résilience des applications progresse, mais des lacunes subsistent. La majorité identifie les lacunes en matière de contrôles de sécurité avant de restaurer les systèmes. Une proportion similaire gère des référentiels en coffre-fort sécurisés en ligne. Plus de la moitié mènent également des exercices annuels de restauration. Moins d'entreprises ont mis en place des environnements isolés pour une investigation et une restauration sécurisées. Un pourcentage encore plus faible applique l'immuabilité à toutes les données de sauvegarde. Ces lacunes rendent les processus de restauration vulnérables à la réinfection ou à la perte de données. Une cyber-résilience mature associe la préparation à des zones de restauration sécurisées et vérifiables.

LA CLASSIFICATION DES DONNÉES PROGRESSE À MESURE QUE LEUR UTILISATION S'ÉTEND.

Comment votre entreprise utilise-t-elle les approches/outils de découverte et de classification des données pour minimiser l'exposition aux risques liés aux données dans l'ensemble de son patrimoine de données ?

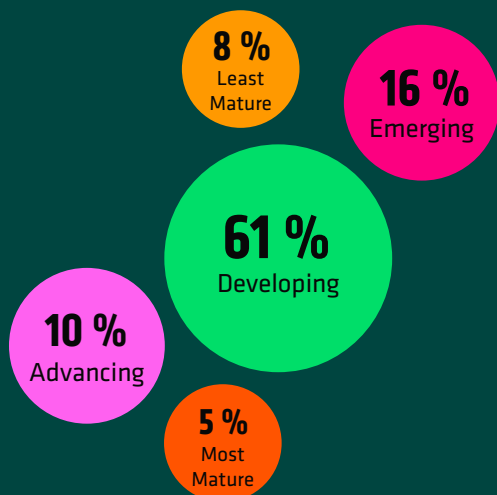


Les entreprises de taille moyenne utilisent la découverte et la classification des données de manière plus stratégique pour la conformité, la réponse et la restauration. Pratiquement deux-tiers d'entre elles gèrent les violations de confidentialité et de sécurité, tandis qu'un peu plus de la moitié utilisent la classification des données pour guider les démarches de conformité pendant une attaque. Plus de la moitié définissent l'importance avant un incident ou priorisent les sauvegardes en fonction du risque. Une cyber-résilience mature transforme la classification en une approche systématique permettant d'optimiser l'exposition au risque liée aux données et d'éclairer les stratégies de protection, de réponse et de restauration.

UNE VISION PLUS CLAIRE DE LA MATURITÉ DE LA RÉSILIENCE

Une fois compilées, les réponses des personnes interrogées ont permis d'établir un baromètre de haut niveau de la maturité de la cyber-résilience. Elles ont révélé des tendances claires dans la manière dont les entreprises de taille moyenne construisent (ou peinent à construire) leur résilience dans la pratique. Si la majorité des entreprises en sont encore au stade du développement, seules 5 % d'entre elles possèdent les capacités intégrées les plus matures qui caractérisent les entreprises préparées à faire face aux risques.

LA COURBE DE MATURITÉ DE LA CYBER-RÉSILIENCE



Moins mature (8 %) : Les sauvegardes, les stratégies et les mesures de sécurité sont en grande partie inexistantes ou incohérentes. La MFA et les contrôles administrateurs sont rarement appliqués, la restauration n'est souvent pas isolée et les évaluations de conformité ou d'importance sont généralement négligées.

Émergente (16 %) : Certaines pratiques de résilience sont en place, mais de manière incohérente. Les entreprises peuvent sauvegarder les données sensibles, appliquer des stratégies globales ou utiliser la MFA, mais rarement de manière combinée. Le renseignement sur les menaces et les efforts de conformité existent, mais ils restent immatures et fragmentés.

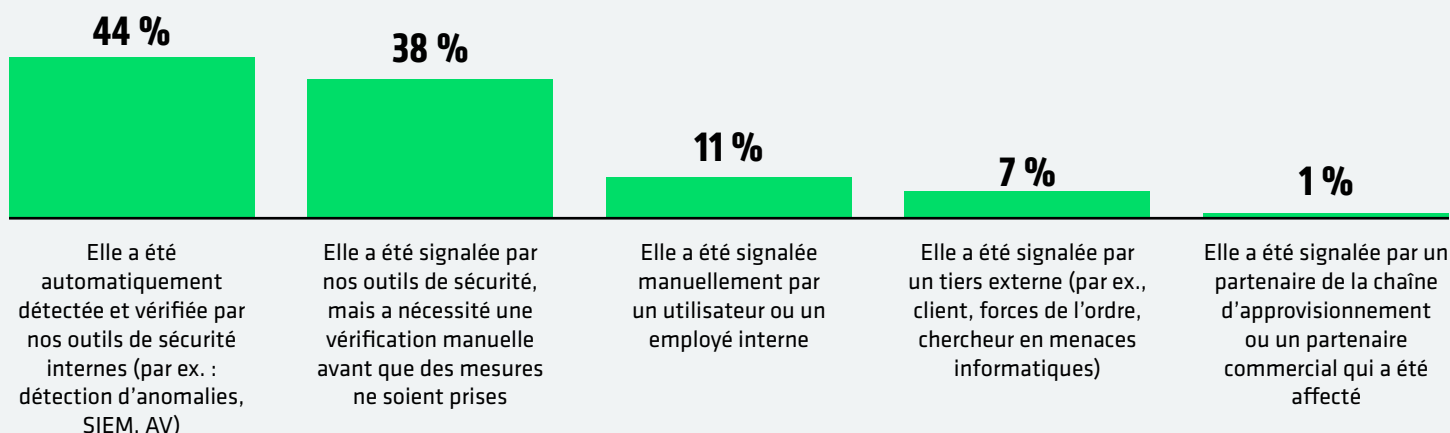
En cours de développement (61 %) : Les pratiques de base telles que les sauvegardes, les contrôles administratifs et les renseignements sur les menaces sont plus courantes, mais toujours inégales. Les environnements de restauration, les contrôles de conformité et la correction des lacunes de sécurité sont appliqués de manière sporadique, laissant les efforts de résilience partiellement efficaces.

En progression (10 %) : La plupart des pratiques clés sont systématiquement appliquées, notamment les stratégies de sauvegarde mondiales, les approbations administratives et les mesures correctives avant la restauration. Les renseignements sur les menaces sont utilisés, mais pas entièrement optimisés, et certaines lacunes subsistent concernant la restauration isolée et la couverture complète de la conformité.

La plus mature (5 %) : La résilience est systématique et complète. Les données sensibles sont sauvegardées à l'échelle mondiale, la MFA et les contrôles administratifs sont la norme, les renseignements sur les menaces sont maximisés, la restauration est sécurisée par des mesures correctives et les mesures de conformité sont systématiquement respectées.

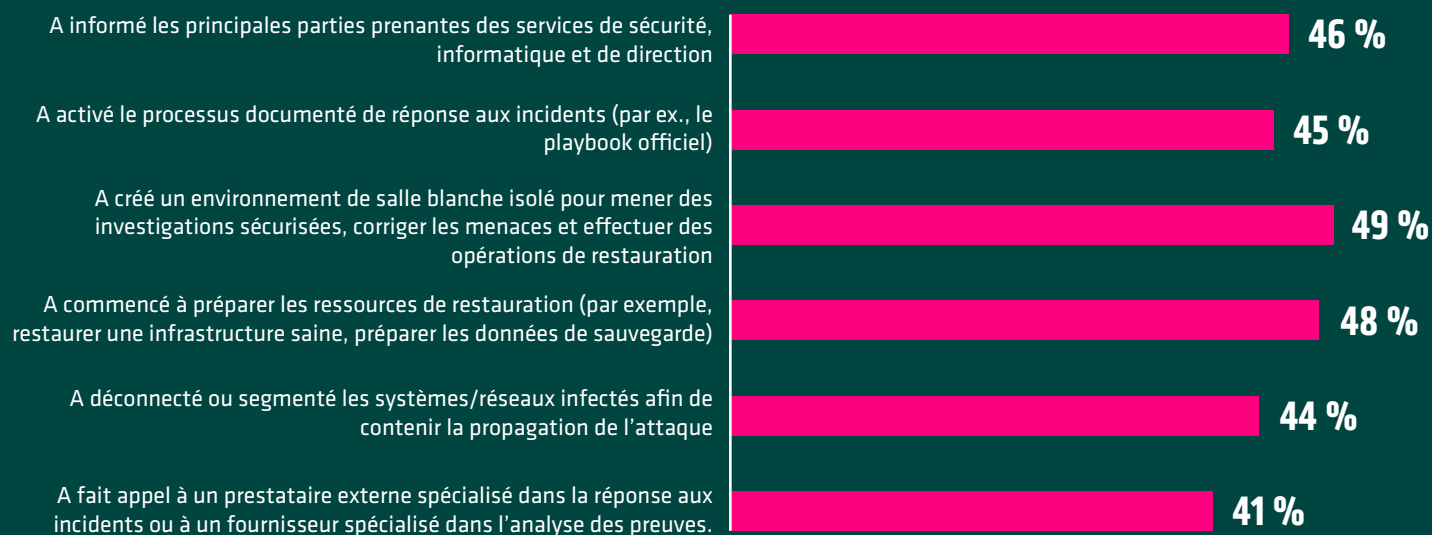
LA RÉSILIENCE DANS L'ADVERSITÉ

COMMENT LES ÉQUIPES ONT IDENTIFIÉ L'ATTAQUE



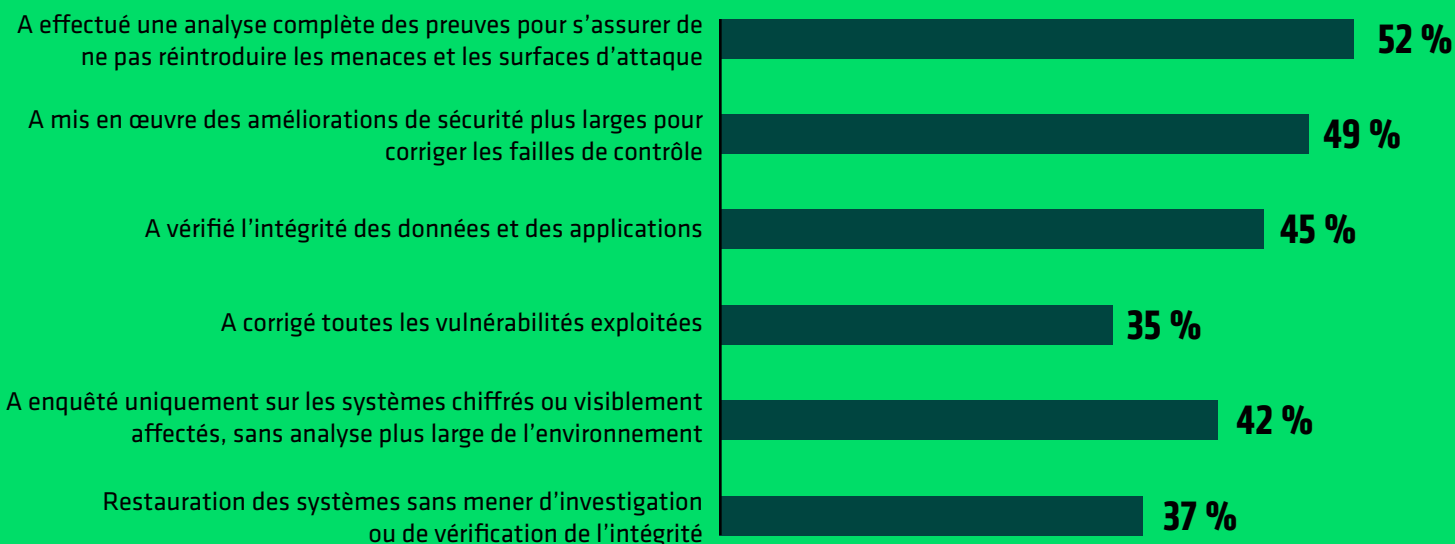
En cas de cyberattaque, la plupart des entreprises de taille moyenne détectent les incidents en interne, la plus grande partie étant identifiée automatiquement et vérifiée par des outils de sécurité. Beaucoup d'autres sont signalées par des outils, mais nécessitent une vérification manuelle avant que des mesures ne soient prises. Beaucoup moins d'incidents sont signalés par les employés ou les parties externes. La détection est largement axée sur les outils, bien que la validation humaine joue toujours un rôle important.

MESURES PRISES PAR LES ÉQUIPES APRÈS CONFIRMATION DE L'ATTAQUE



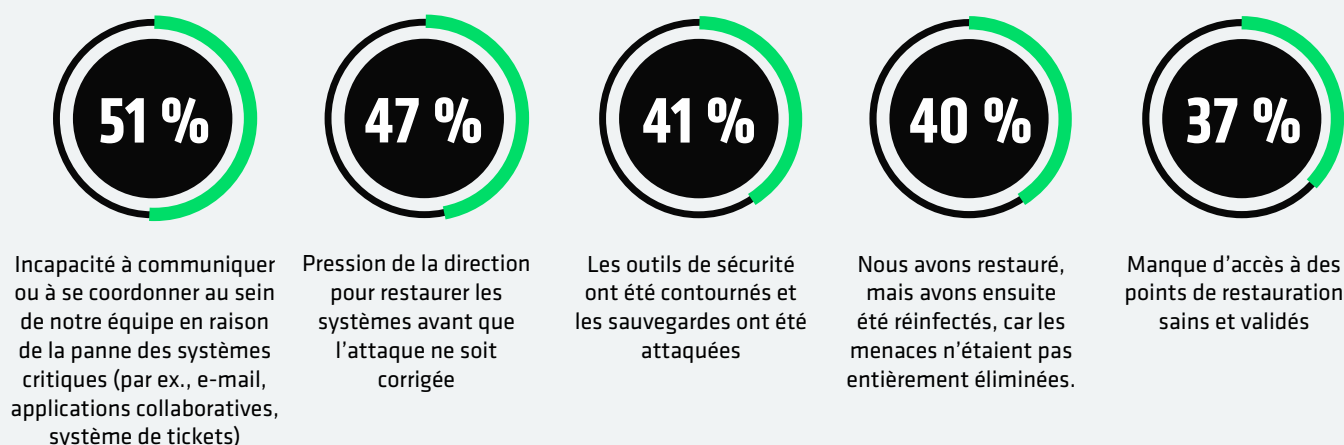
Après avoir confirmé une attaque, les entreprises de taille moyenne ont pris des mesures variées pour contenir la menace et commencer la restauration. Des pourcentages similaires d'entreprises ont commencé à préparer des ressources de restauration, à créer des environnements de salle blanche isolés, à informer les principales parties prenantes, à déconnecter les systèmes infectés et à activer les manuels de réponse. Une proportion légèrement plus faible a fait appel à des partenaires externes de réponse aux incidents. Ces modèles suggèrent que les efforts de réponse sont largement adoptés, mais pas encore entièrement normalisés pour toutes les actions critiques.

MESURES PRISES AVANT DE REMETTRE LES SYSTÈMES ET LES DONNÉES EN LIGNE



Avant de remettre les systèmes et les données en ligne, les entreprises de taille moyenne ont eu recours à un mélange de mesures d'analyse de preuves et de remédiation. Environ la moitié ont mené une analyse de preuves complète, renforcé leur dispositif de sécurité ou vérifié l'intégrité de leurs données et applications, tandis qu'une proportion similaire s'est concentrée uniquement sur les systèmes manifestement affectés. Des proportions plus faibles ont corrigé les vulnérabilités exploitées ou restauré des systèmes sans investigation ni vérification. Ces lacunes peuvent augmenter le risque de réinfection ou d'exposition résiduelle.

DIFFICULTÉS RENCONTRÉES PAR LES ÉQUIPES PENDANT L'ATTAQUE



Les équipes ont été confrontées à divers défis opérationnels et techniques pendant l'attaque. Environ la moitié d'entre elles ont eu du mal à communiquer alors que les systèmes critiques étaient en panne et ont ressenti une pression pour restaurer les systèmes avant que la remédiation ne soit terminée. Les équipes ont signalé une évasion des outils de sécurité, des sauvegardes attaquées, une réinfection après la restauration ou un manque d'accès à des points de restauration sains. Ces difficultés mettent en évidence des lacunes dans l'état de préparation qui peuvent compliquer la réponse et prolonger la perturbation.

LES LACUNES PERSISTANTES DES INVESTISSEMENTS DANS LA RÉSILIENCE

Même les entreprises bien préparées peinent à maintenir leur résilience en cas d'attaque. Plus la pression opérationnelle augmente, plus les failles de coordination, les corrections incomplètes et les risques de réinfection révèlent à quel point la restauration peut être fragile sans processus unifiés ni assurance continue.

Ces tendances reflètent la manière dont les entreprises de taille moyenne allouent actuellement leurs budgets de cyber-résilience. Nous avons demandé aux répondants comment ils répartissaient leurs dépenses entre les cinq fonctions clés du Cadre de cybersécurité du NIST : Identifier, Protéger, Détecter, Répondre et Restaurer.

La plupart continuent d'investir fortement dans la prévention, la protection et la détection, tandis que des financements comparativement moindres soutiennent la réponse et la restauration vérifiée. La courbe de maturité reste donc davantage axée sur la défense que sur la restauration, mettant en évidence une opportunité inexploitée de renforcer la résilience là où elle compte le plus : après l'attaque.

CADRE DE CYBERSÉCURITÉ DU NIST

La taille des cases indique la proportion des investissements en matière de cyber-résilience, de la plus élevée à la plus faible.



L'IA ET L'AUTOMATISATION S'IMPOSENT COMME DES MULTIPLICATEURS DE RÉSILIENCE

Les résultats montrent également que les entreprises de taille moyenne considèrent l'IA comme un puissant catalyseur de la cyber-résilience, notamment pour améliorer la rapidité de détection et la précision des réponses. Presque toutes les personnes interrogées ont jugé que des outils tels que la détection d'anomalies, l'analyse du comportement des utilisateurs, ainsi que l'investigation et la réponse aux menaces pilotées par l'IA étaient efficaces pour renforcer leur posture de sécurité.

Même les assistants basés sur l'IA générative plus récents, qui sont capables de traiter des requêtes en langage naturel et d'effectuer des analyses contextuelles, gagnent en popularité car ils permettent de simplifier et d'accélérer la prise de décision. Cinquante-six pour cent des entreprises de taille moyenne victimes d'une cyberattaque ont déclaré avoir notamment appris qu'il était primordial de renforcer l'automatisation des processus de détection, de réponse et de restauration. Cela reflète la demande croissante de plateformes intégrées d'automatisation et d'orchestration, sur lesquelles l'IA agit comme un multiplicateur de force et permet d'améliorer l'efficacité, la cohérence et la performance de ces processus.

Si l'on se projette dans l'avenir, la plupart des personnes interrogées s'attendent à ce que l'IA joue un rôle de plus en plus stratégique dans la cyber-défense d'ici fin 2026. Cinquante-six pour cent estiment que l'IA soutiendra la prise de décision humaine en renforçant les capacités d'analyse et de recommandation, l'humain conservant la maîtrise des décisions et des actions finales. Trente-sept pour cent s'attendent à ce que l'IA devienne un élément central des processus de détection et de réponse, voire qu'elle prenne certaines décisions de manière autonome. Cela indique une trajectoire claire : l'IA passe du statut d'assistant à celui de pilier opérationnel de la cyber-résilience, et s'apprête à améliorer la rapidité, la précision et la confiance dans les domaines de la détection, de la réponse et de la restauration.

L'AVENIR DE LA RÉSILIENCE COMMENCE MAINTENANT

Bien que les entreprises de taille moyenne fassent des progrès notables en matière de cyber-résilience, beaucoup d'entre elles ont encore du chemin à parcourir pour améliorer leur réponse, leur restauration et la validation de leur disponibilité après une attaque. La cyber-résilience représente un avantage concurrentiel considérable. L'avenir appartient aux entreprises qui investissent dans les personnes, les produits et les processus nécessaires pour restaurer plus rapidement, conserver la confiance de leurs clients et maintenir leur activité lorsque d'autres n'y arrivent pas. Lorsqu'il est pratiquement impossible d'éviter une perturbation, la résilience n'est pas seulement une protection, c'est un véritable levier de performance.

Renforcez votre résilience avant d'être confronté à une crise :

- [En savoir plus sur les solutions de cyber-résilience de Cohesity pour les entreprises de taille moyenne](#)
- [Évaluez votre maturité en matière de cyber-résilience avec cette fiche d'évaluation de la résilience](#)
- [Passez au niveau supérieur grâce à un plan d'action en cinq étapes pour renforcer votre cyber-résilience.](#)

MÉTHODOLOGIE

COHESITY

En septembre 2025, Cohesity a chargé Vanson Bourne d'interroger 3 200 décideurs informatiques et responsables de la sécurité. Cette enquête a permis d'établir les conclusions présentées ici. Les personnes interrogées représentent des entreprises aux États-Unis (500), au Brésil (200), au Royaume-Uni (400), en Allemagne (400), en France (400), aux Émirats arabes unis (100), en Australie (200), en Corée du Sud (200), au Japon (400), en Inde (200) et à Singapour (200). Ces entreprises comptaient au moins 1 000 employés et provenaient de divers secteurs publics et privés, notamment les services financiers, le secteur public et la santé.



© 2026 Cohesity Inc. Tous droits réservés.

Cohesity, le logo Cohesity et les autres marques Cohesity sont des marques déposées de Cohesity, Inc. ou de ses filiales, aux États-Unis et/ou à l'international. Les autres noms peuvent être des marques déposées de leurs propriétaires respectifs. Ce document (a) est destiné à vous fournir des informations sur Cohesity, ses activités et ses produits ; (b) est réputé véridique et exact au moment de sa rédaction, mais peut être modifié sans préavis ; et (c) est fourni « EN L'ÉTAT ». Cohesity décline toute responsabilité quant aux conditions, déclarations ou garanties, expresses ou implicites, de quelque nature que ce soit.

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000049-001-FR 7-2026