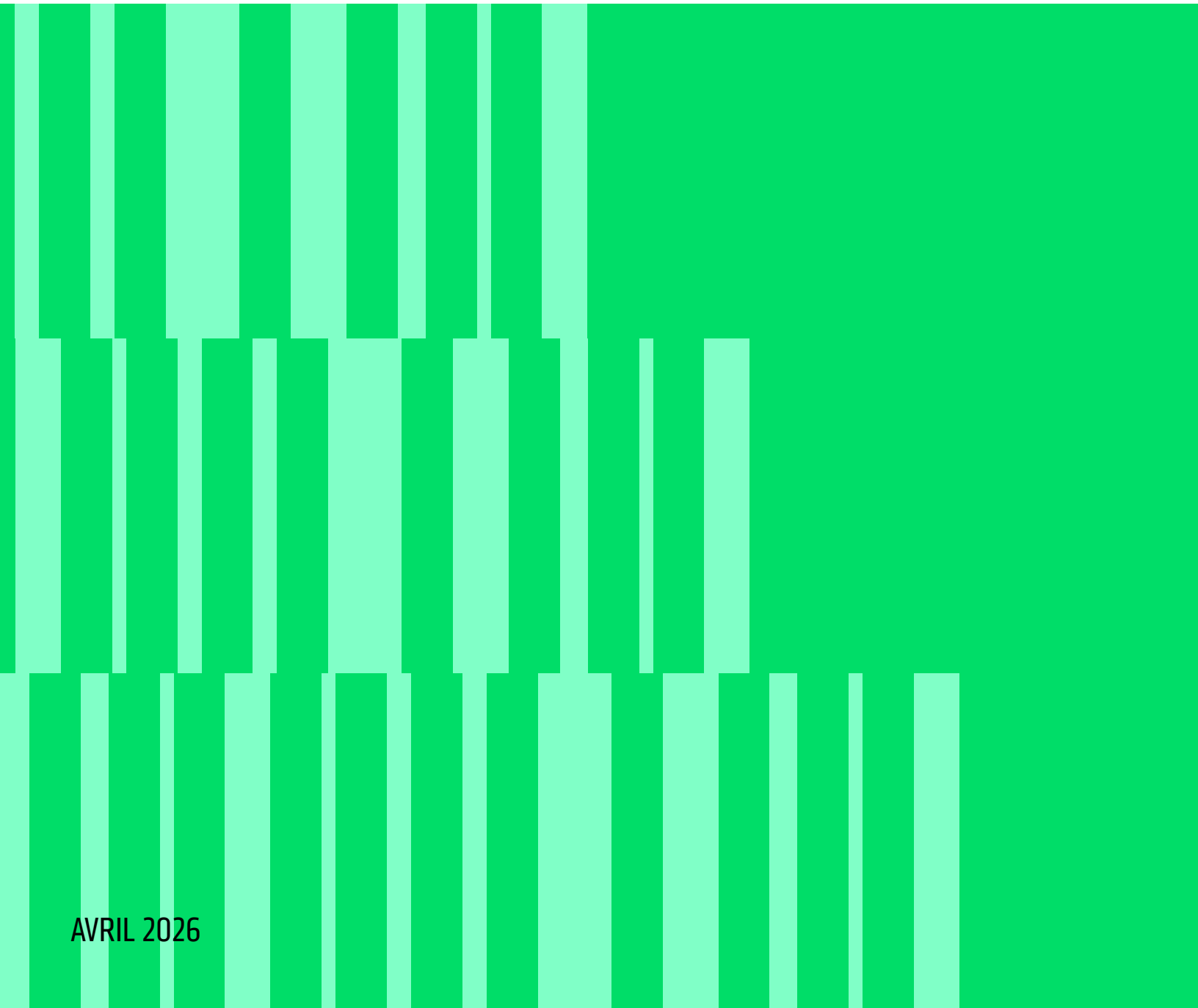
COHESITY

RAPPORT SUR LA CYBER-RÉSILIENCE

Être préparé aux risques ou y être exposé : le fossé de la cyber-résilience en les organisations de santé



AVRIL 2026

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 qui paralysent leurs opérations informatiques, leur conseil d'administration, et au-delà.

Cohesity a interrogé 3 200 décideurs des opérations IT et de la sécurité dans 11 pays afin de comprendre pourquoi, et ce qui distingue les organisations résilientes de celles qui rencontrent encore des difficultés Parmi les répondants figuraient 371 participants issus d'organisations de santé. Leurs réponses révèlent un fossé croissant en matière de résilience entre les organisations de santé prêtes à faire face aux risques, capables de se rétablir rapidement et en toute confiance, et leurs homologues plus exposées, qui restent vulnérables aux perturbations prolongées et aux dommages financiers qui en découlent.

Notre étude analyse les impacts concrets des cyberattaques majeures, la manière dont les organisations de santé ont auto-évalué leur cyber résilience par rapport aux bonnes pratiques, ainsi que les mesures qu'elles ont prises pour détecter ces incidents, y répondre et s'en remettre. Elle met également en lumière les enseignements tirés et la façon dont elles se tournent vers l'IA et l'automatisation pour accélérer leur résilience et réduire ce fossé.

CYBERATTAQUES MAJEURES : **LA NOUVELLE RÉALITÉ DES ENTREPRISES MODERNES**

ous les cyberincidents ne se valent pas. De nombreuses organisations de santé gèrent presque quotidiennement des tentatives de phishing, des analyses 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.

CES ATTAQUES AUX IMPACTS CONSIDÉRABLES NE SONT PLUS DES ÉVÉNEMENTS ISOLÉS :

85 %

des entreprises françaises ont subi au moins une cyberattaque majeure.

66 %

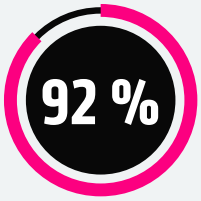
en ont subi une au cours des 12 derniers mois

35 %

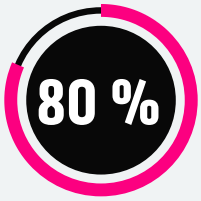
ont subi plusieurs incidents sur cette période de 12 mois

LE VÉRITABLE COÛT DES CYBERATTAQUES MAJEURES

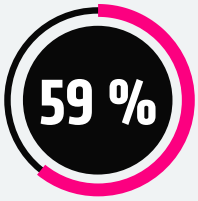
LES ORGANISATIONS DE SANTÉ QUE NOUS AVONS INTERROGÉES ONT TOUTES FAIT ÉTAT DE PRESSIONS FINANCIÈRES ET RÉGLEMENTAIRES :



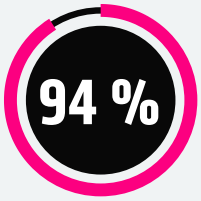
ont déclaré une perte de revenus



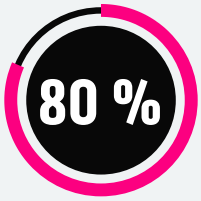
des organisations de santé cotées en bourse ont indiqué avoir révisé leurs prévisions financières[1]



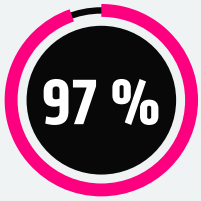
ont perdu des clients



ont payé une rançon – pour un montant moyen de 1,3 million de dollars US par incident



des organisations de santé privées ont réaffecté des budgets initialement destinés à des initiatives de croissance



ont été confrontées à des conséquences juridiques ou réglementaires, notamment des amendes réglementaires (54 %) et des poursuites ou actions collectives (39 %)

[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

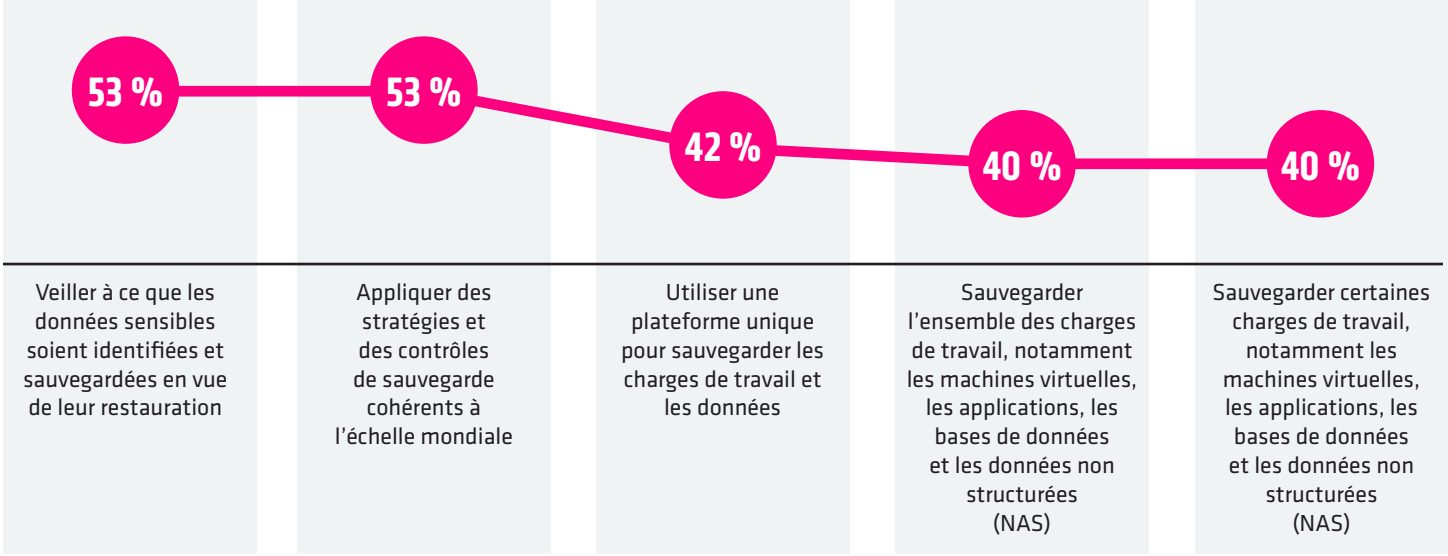
Compte tenu de l'ampleur des répercussions financières et opérationnelles révélées par notre étude, on pourrait s'attendre à ce que la résilience organisationnelle soit un sujet de préoccupation très répandu. Près de la moitié des personnes interrogées (49 %) se sont dites totalement convaincues que 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'investigation 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

Laquelle des mesures suivantes votre entreprise met-elle en œuvre pour protéger toutes ses données dans des environnements hybrides et/ou multi-cloud ?



Un peu plus de la moitié des organisations de santé veillent à ce que les données sensibles soient identifiées et sauvegardées pour permettre la restauration. La même proportion applique des politiques de sauvegarde cohérentes à l'échelle mondiale. Cependant, moins de la moitié sauvegardent l'ensemble des charges de travail ou s'appuient sur une plateforme unique. Un peu plus d'un tiers ne sauvegardent que certaines charges de travail sélectionnées. Cette fragmentation limite la visibilité et la cohérence entre les environnements. Une cyber-résilience mature nécessite d'unifier la sauvegarde et la restauration au sein d'une plateforme intelligente sécurisée par les principes du Zero Trust.

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

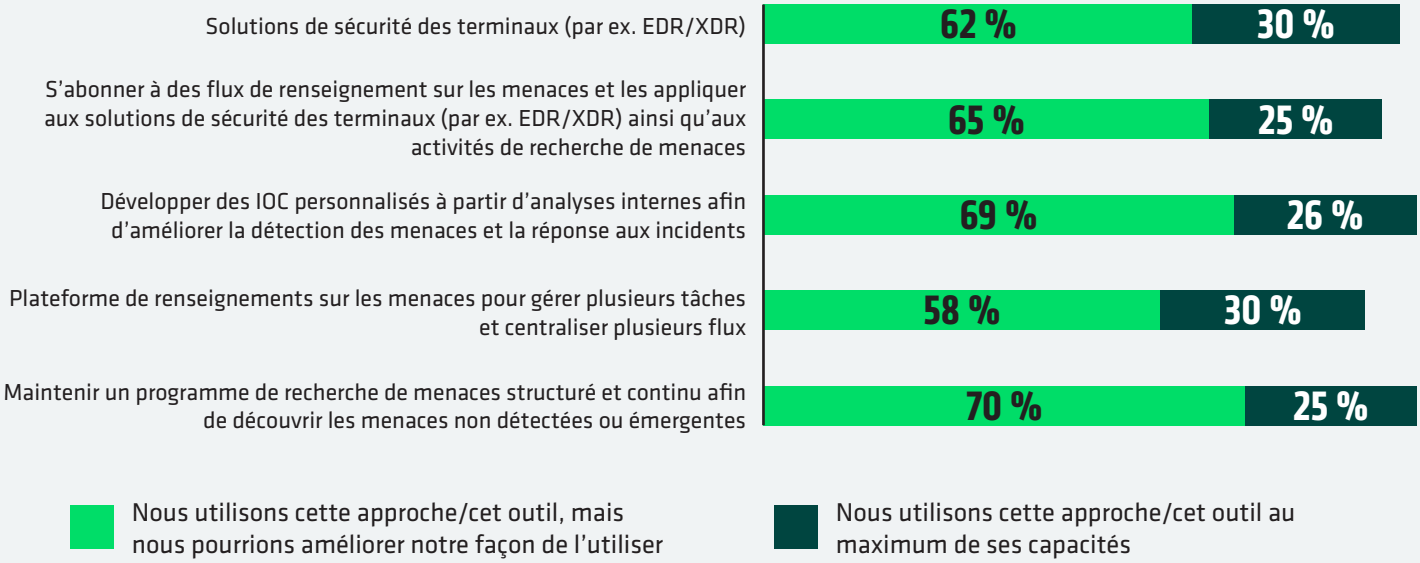
Que fait votre entreprise pour garantir la capacité de récupération de ses données ?

60 %	Exiger une autorisation supplémentaire pour les tâches administratives à risque élevé associées aux solutions de sauvegarde et de restauration
48 %	Authentification multifacteur sur notre solution de sauvegarde
44 %	Suivre la règle de sauvegarde « 3-2-1 » (trois copies des données, stockées sur deux types de supports différents, dont une copie conservée hors site)
42 %	Protéger les données critiques grâce à l'immuabilité
35 %	Appliquer le principe du moindre privilège aux charges de travail sauvegardées

De nombreuses organisations de santé ont renforcé les contrôles d'accès à leurs environnements de sauvegarde, six sur dix exigent une autorisation administrative supplémentaire pour les tâches à risque élevé. Moins de la moitié imposent l'authentification multifacteur, suivent la règle de sauvegarde 3-2-1 ou protègent les données critiques grâce à l'immuabilité. Seul environ un tiers applique le principe du moindre privilège en matière de droits d'accès. 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'INVESTIGATION 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 outils de détection et d'investigation des menaces sont largement déployés, mais souvent sous utilisés. La plupart des organisations de santé utilisent la sécurité des terminaux, les flux de renseignement sur les menaces et des programmes structurés de threat hunting, mais seule une minorité exploite réellement tout le potentiel de ces outils.L'optimisation de capacités avancées, telles que des indicateurs de compromission (IOC) personnalisés ou des plateformes de renseignement sur les menaces, reste particulièrement limitée. Pour parvenir à une cyber résilience mature, il est essentiel d'intégrer ces outils dans une boucle de renseignement continue qui améliore la visibilité, la détection et la réponse.

LES ENTREPRISES SONT SUSCEPTIBLES D'ÊTRE RÉINFECTÉES

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

56 % Faire des simulations annuelles de bout en bout impliquant une équipe transversale composée de parties prenantes des services techniques, juridiques, stratégiques, exécutifs et de communication.

54 % Identifier et corriger les failles des contrôles de sécurité avant de restaurer les systèmes en production

53 % Créer un référentiel en ligne et sécurisé des systèmes et informations critiques pour soutenir la réponse aux incidents et la restauration

36 % Utiliser un environnement isolé pour enquêter sur les incidents, les corriger et restaurer de manière sécurisée

36 % Garantir l'immuabilité de toutes les données de sauvegarde

L'approche des entreprises françaises en matière de résilience des applications progresse, mais des lacunes subsistent. Plus de la moitié identifient les lacunes des contrôles de sécurité avant de restaurer les systèmes et organisent des exercices annuels de restauration. Une proportion similaire maintient des dépôts en ligne sécurisés (coffre-fort) pour soutenir la réponse et la restauration. Moins d'organisations utilisent des environnements isolés pour une investigation et une restauration sécurisées ou appliquent l'immuabilité à l'ensemble des données de sauvegarde. Cela rend 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 CONFORMITÉ PROGRESSE, LA SAUVEGARDE RESTE À LA TRAÎNE

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 ?

60 %

En cas de cyberattaque, nous utilisons la classification des données de sauvegarde pour déterminer les obligations de conformité liées aux données impactées

59 %

Identifier et corriger les violations de confidentialité et de sécurité des sauvegardes afin d'assurer la conformité

53 %

Définir et comprendre l'importance d'une cyberattaque avant qu'un incident ne survienne

52 %

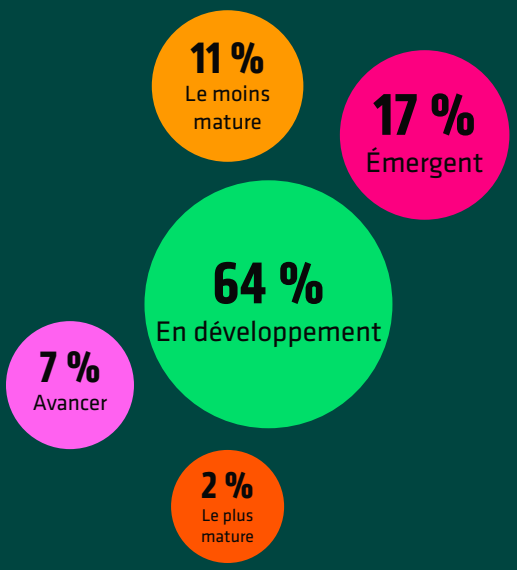
Identifier et hiérarchiser les systèmes pour la sauvegarde

Les organisations de santé utilisent la découverte et la classification des données de manière plus stratégique pour la conformité, la réponse et la restauration. Six sur dix utilisent la classification pour guider la conformité lors d'une attaque, tandis qu'une proportion proche traite les violations de la vie privée et de la sécurité. Un peu moins définissent la matérialité avant un incident ou priorisent les sauvegardes en fonction du risque. Ces lacunes suggèrent que l'utilisation de la classification fondée sur le risque est encore en évolution. Une cyber-résilience mature transforme la classification en une capacité systématique qui optimise la posture de risque des données et renforce la protection, la réponse et la 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 françaises construisent (ou peinent à construire) leur résilience dans la pratique. Si la majorité des entreprises en sont encore au stade du développement, seules 2 % d'entre elles possèdent les capacités intégrées les plus matures qui caractérisent les entreprises préparées aux risques.

LA COURBE DE MATURITÉ DE LA CYBER-RÉSILIENCE (FRANCE)



Le moins mature (11 %) : Les sauvegardes, les stratégies et les mesures de sécurité sont souvent 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.

Émergent (17 %) : 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. Des efforts sont faits en matière de renseignement sur les menaces et de conformité, mais ils restent immatures et fragmentés.

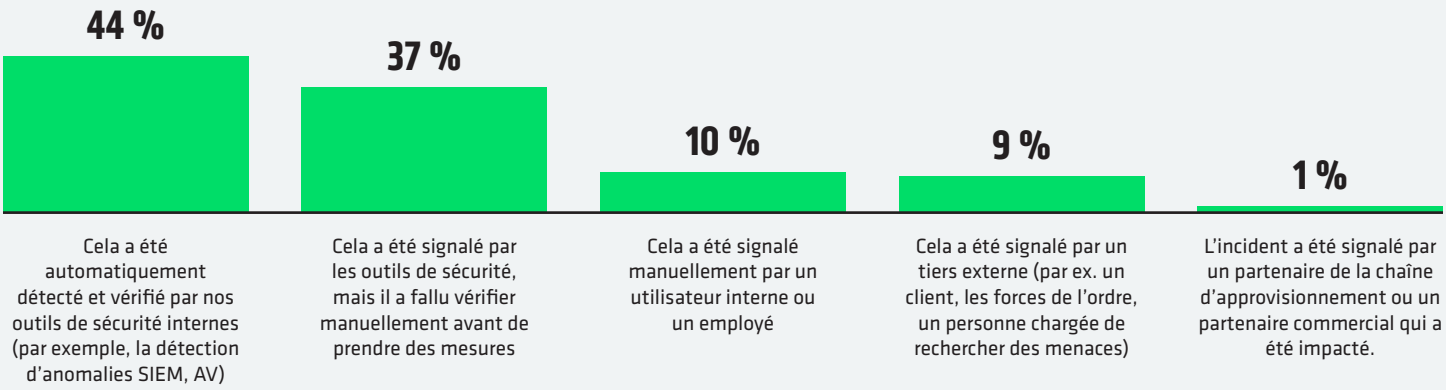
En cours de développement (64 %) : Les pratiques fondamentales, notamment les sauvegardes, les contrôles administrateurs et les renseignement sur les menaces, sont plus courantes, mais restent inégales. Les environnements de restauration, les contrôles de conformité et la correction des failles de sécurité sont appliqués de manière sporadique, ce qui limite l'efficacité des efforts en matière de résilience.

Avancé (7 %) : La plupart des pratiques clés sont systématiquement appliquées, notamment les stratégies de sauvegarde globales, les approbations des administrateurs et la correction avant la restauration. Les renseignements sur les menaces sont utilisés, mais ne sont pas pleinement optimisés, et il subsiste certaines lacunes en matière de restauration isolée et de couverture complète de la conformité.

Le plus mature (2 %) : La résilience est systématique et complète. Les données sensibles sont sauvegardées à l'échelle mondiale, la MFA et les contrôles administrateurs sont standard, les renseignement sur les menaces sont optimisés, la restauration est sécurisée grâce à la correction et les mesures de conformité sont systématiquement respectées.

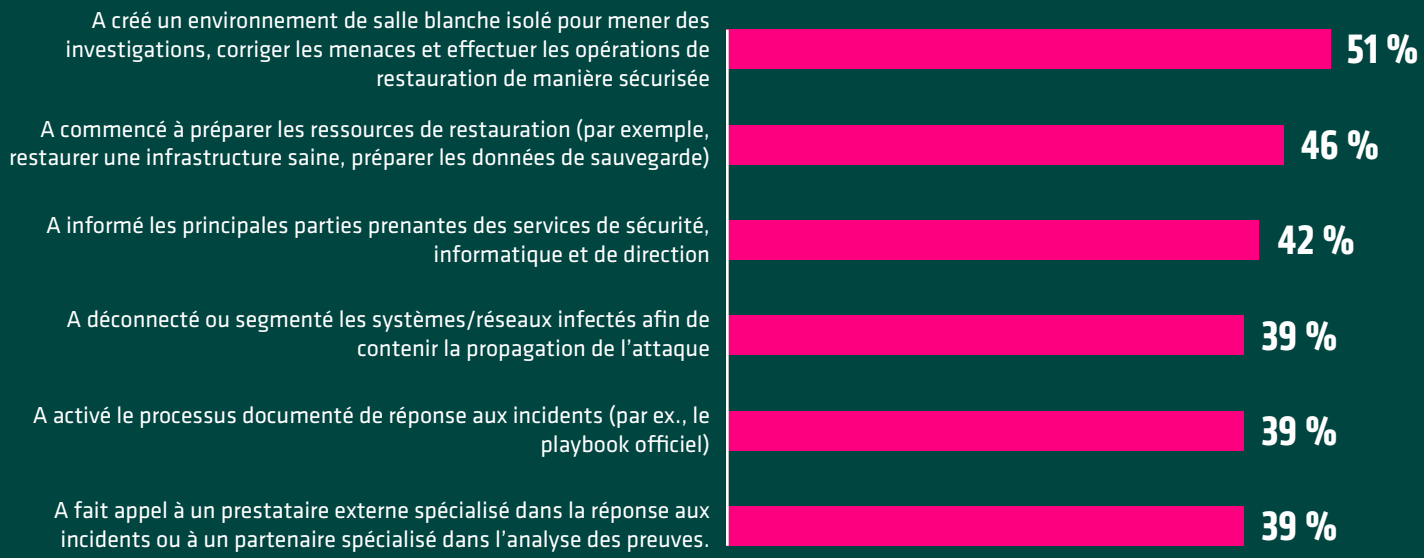
LA RÉSILIENCE DANS L'ADVERSITÉ

COMMENT LES ÉQUIPES ONT IDENTIFIÉ L'ATTAQUE



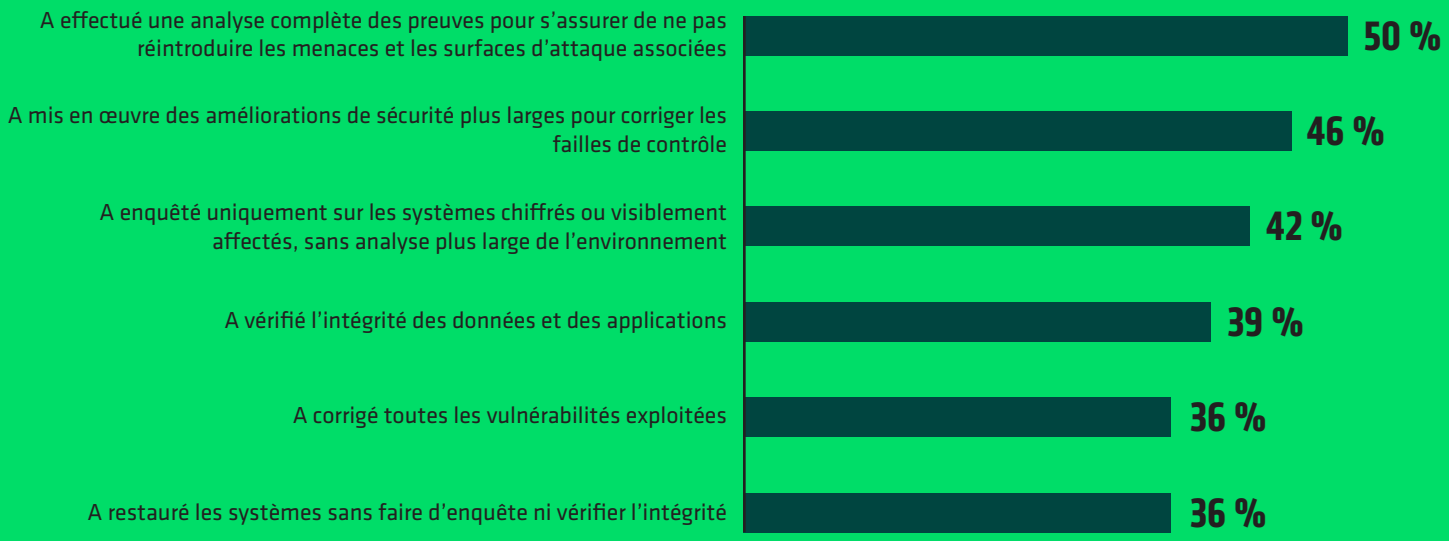
En cas de cyberattaque, près de la moitié des organisations de santé ont indiqué que les attaques étaient automatiquement identifiées et vérifiées par leurs propres outils de sécurité, tandis que plus d'un tiers ont signalé qu'elles étaient détectées par des outils mais nécessitaient une vérification manuelle avant toute action. Les alertes provenant de tiers étaient beaucoup moins fréquentes. La détection semble principalement interne, mais toujours dépendante d'une confirmation humaine.

MESURES PRISES PAR LES ÉQUIPES APRÈS CONFIRMATION DE L'ATTAQUE



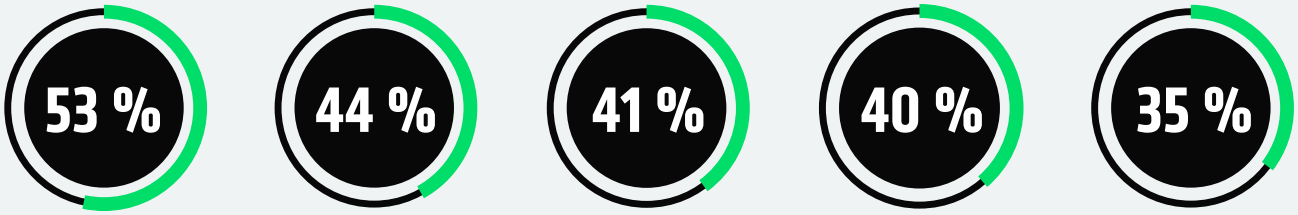
Après confirmation d'une attaque, les organisations de santé ont entrepris diverses actions pour soutenir la restauration. Un peu moins de la moitié ont commencé à restaurer une infrastructure propre ou à préparer les données de sauvegarde. Plus de la moitié ont mis en place des environnements de salle blanche isolés pour une investigation et une restauration sécurisées. Environ quatre sur dix ont notifié les parties prenantes clés, contenu les systèmes infectés, activé des plans formels de réponse ou fait appel à des experts externes en réponse à incident ou en investigation forensique. Ces variations indiquent que les actions de réponse ne sont pas encore pleinement standardisées pour les étapes critiques.

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



Avant de remettre les systèmes en ligne, les organisations de santé ont entrepris un mélange d'actions forensiques et correctives. La moitié ont réalisé une analyse des preuves complète, tandis qu'un peu moins de la moitié ont mis en œuvre des améliorations de sécurité plus larges. Moins d'organisations ont vérifié l'intégrité des données et des applications, corrigé les vulnérabilités exploitées ou enquêté au-delà des systèmes visiblement affectés. Plus d'un tiers ont restauré les systèmes sans investigation complète ni vérification d'intégrité, laissant des failles propices à la réinfection et à des risques résiduels.

DIFFICULTÉS RENCONTRÉES PAR LES ÉQUIPES PENDANT L'ATTAQUE



Les équipes ont signalé d'importants défis tout au long du processus. Beaucoup ont rencontré des difficultés de communication ou de coordination pendant que les systèmes critiques étaient hors ligne. Près de la moitié ont subi une pression pour restaurer les opérations avant la fin des mesures correctives. L'évasion des outils de sécurité, la réinfection et l'absence de points de reprise propres ont aggravé les difficultés, soulignant la nécessité de mesures de résilience plus robustes.

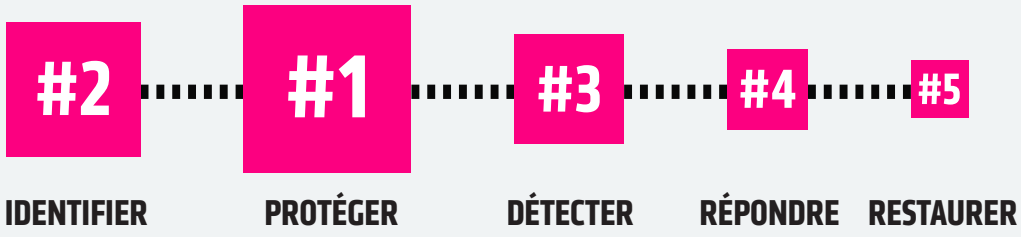
LES LACUNES PERSISTANTES DES INVESTISSEMENTS DANS LA RÉSILIENCE

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 organisations de santé 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 françaises 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 la GenAI les plus récents, capables de traiter des requêtes de menaces en langage naturel et d'effectuer des analyses contextuelles, gagnent en popularité car ils permettent de simplifier et d'accélérer la prise de décision. 61 % des organisations de santé ayant subi une cyberattaque ont indiqué avoir appris qu'il était essentiel de renforcer l'automatisation des processus de détection, de réponse et de restauration. Cela reflète la demande croissante pour des plateformes intégrées d'automatisation et d'orchestration, sur lesquelles l'IA agit comme un multiplicateur de force, améliorant l'efficacité, la cohérence et la performance de l'ensemble 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. Près de la moitié (54%) anticipent que l'IA soutiendra la prise de décision humaine, améliorant l'analyse et les recommandations tout en laissant aux humains le contrôle des actions finales. 37 % s'attendent à ce que l'IA devienne un élément central de la détection et de la 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 organisations de santé réalisent des progrès mesurables en matière de cyber résilience, beaucoup disposent encore d'une marge de progression pour améliorer leur réponse, leur restauration et la validation de leur niveau de préparation après une attaque. La cyber résilience représente un avantage concurrentiel majeur. L'avenir appartient aux organisations qui investissent dans les personnes, les produits et les processus nécessaires pour se rétablir plus rapidement, préserver la confiance de leurs patients et partenaires, et maintenir leur activité lorsque d'autres n'y parviennent pas. Lorsqu'une perturbation devient quasiment inévitable, la résilience n'est plus seulement une forme de protection : c'est un véritable levier de performance.

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

- Réservez un atelier sur la résilience face aux ransomwares.
- Passez au niveau supérieur grâce à un plan d'action en cinq étapes pour renforcer votre cyber-résilience
- En savoir plus sur les solutions de cyber-résilience de Cohesity

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.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000075-001-FR 4-2026