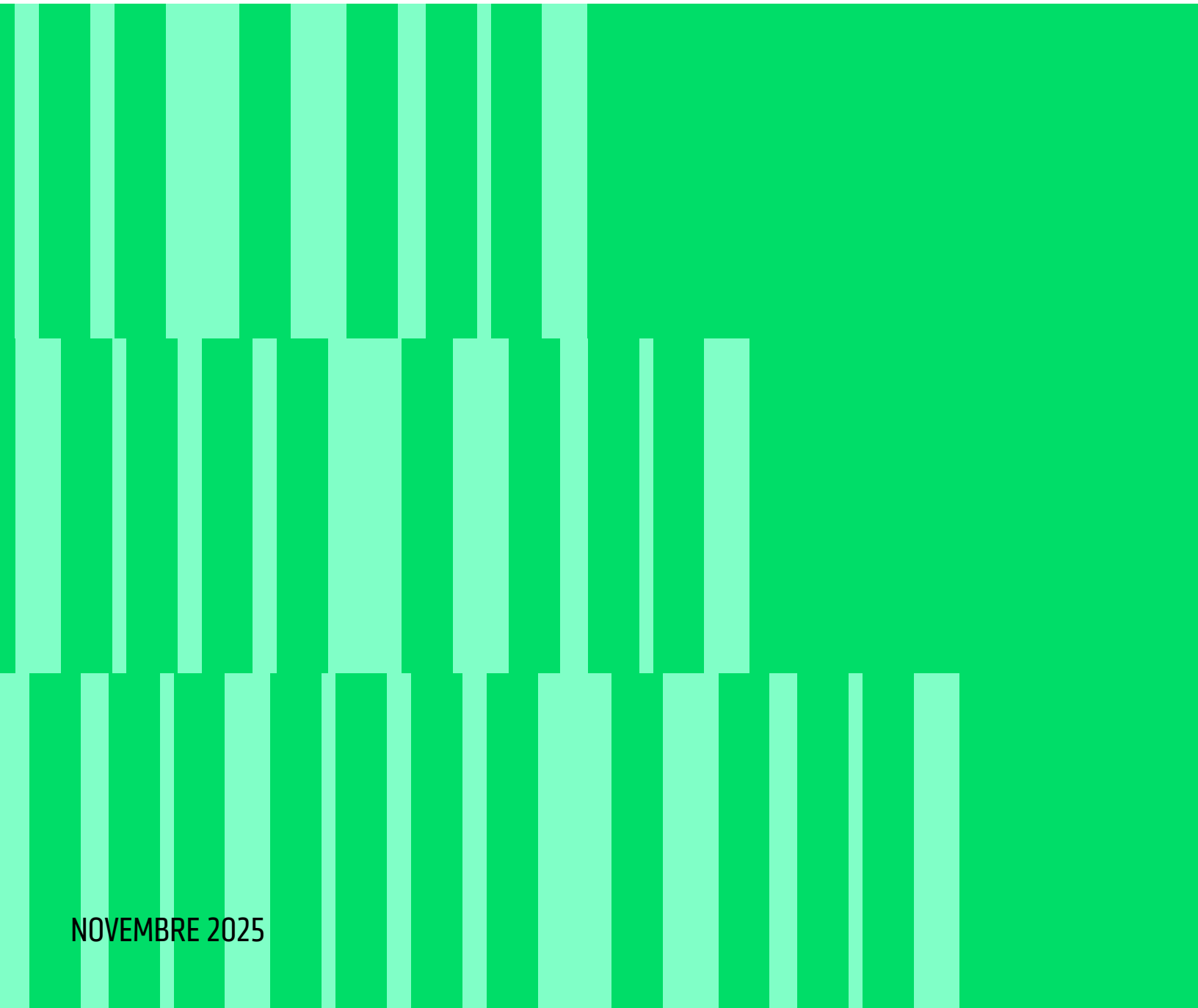
COHESITY

RAPPORT SUR LA CYBER-RÉSILIENCE

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



NOVEMBRE 2025

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 400 responsables d'équipes chargées des opérations informatiques et de la sécurité opérationnelle en France afin de comprendre pourquoi, et de découvrir ce qui distingue les entreprises résilientes de celles qui rencontrent toujours des difficultés. Les résultats révèlent que le fossé en matière de résilience se creuse : les entreprises préparées aux risques sont capables de restaurer rapidement et en toute confiance, tandis que celles qui y sont exposées restent vulnérables aux perturbations prolongées et aux dommages financiers qui en découlent.

Notre étude examine les impacts concrets des cyberattaques majeures, la manière dont les entreprises françaises 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.

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

Tous les cyber incidents ne se valent pas. De nombreuses entreprises gèrent quasiquotidiennement des tentatives de phishing, des scans de logiciels malveillants ou des pannes système. Mais les cyberattaques majeures sont différentes. Elles paralysent les opérations, entraînent des pertes financières, nuisent à la réputation et attirent l'attention des conseils d'administration, des auditeurs et des organismes de réglementation tels que l'Autorité des marchés financiers (AMF), la Commission nationale de l'informatique et des libertés (CNIL) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

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

76 %

des entreprises françaises ont subi au moins une cyberattaque majeure.

56 %

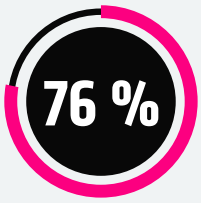
en ont subi une au cours des 12 derniers mois.

28 %

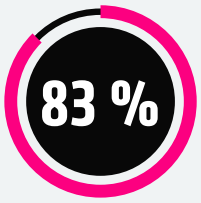
ont subi plusieurs incidents sur cette période de 12 mois.

LE VÉRITABLE COÛT DES CYBERATTAQUES MAJEURES

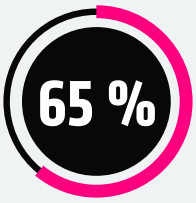
LES ENTREPRISES FRANÇAISES QUE NOUS AVONS INTERROGÉES ONT TOUTES FAIT ÉTAT DE PRESSIONS FINANCIÈRES ET RÉGLEMENTAIRES :



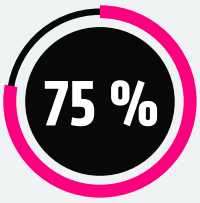
ont déclaré avoir perdu des revenus



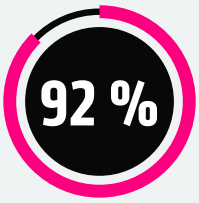
des entreprises françaises cotées en bourse ont déclaré avoir révisé leurs prévisions financières[1]



des entreprises françaises privées ont réaffecté des budgets initialement destinés à des initiatives de croissance



ont payé une rançon, d'un montant moyen de 1,2 million d'euros par incident



ont fait face à des conséquences juridiques ou réglementaires, notamment des sanctions financières (41 %) et des actions légales collectives ou représentatives (38 %)

[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

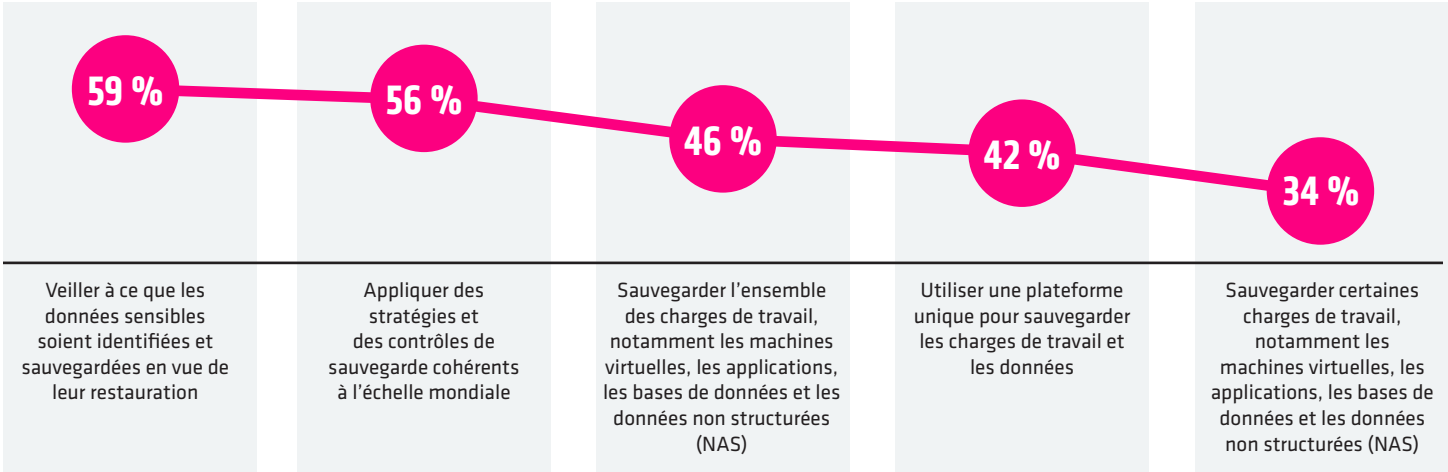
Compte tenu de l'ampleur des répercussions financières et opérationnelles révélées par notre étude, on pourrait s'attendre à ce que la résilience organisationnelle soit un sujet de préoccupation très répandu. Près de la moitié des personnes interrogées (47 %) se sont dites totalement convaincues que 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'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 ?



La majorité des entreprises françaises veillent à identifier et à sauvegarder leurs données sensibles afin de pouvoir les restaurer, et plus de la moitié d'entre elles appliquent des stratégies de sauvegarde cohérentes à l'échelle mondiale. Pourtant, la protection des données reste fragmentée. Moins de la moitié sauvegardent l'ensemble de leurs charges de travail, et seulement 42 % utilisent une plateforme unique, tandis qu'environ un tiers sauvegardent uniquement certaines charges de travail. Cette approche fragmentée limite la visibilité, augmente l'exposition et complique la restauration. Une cyberrésilience 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

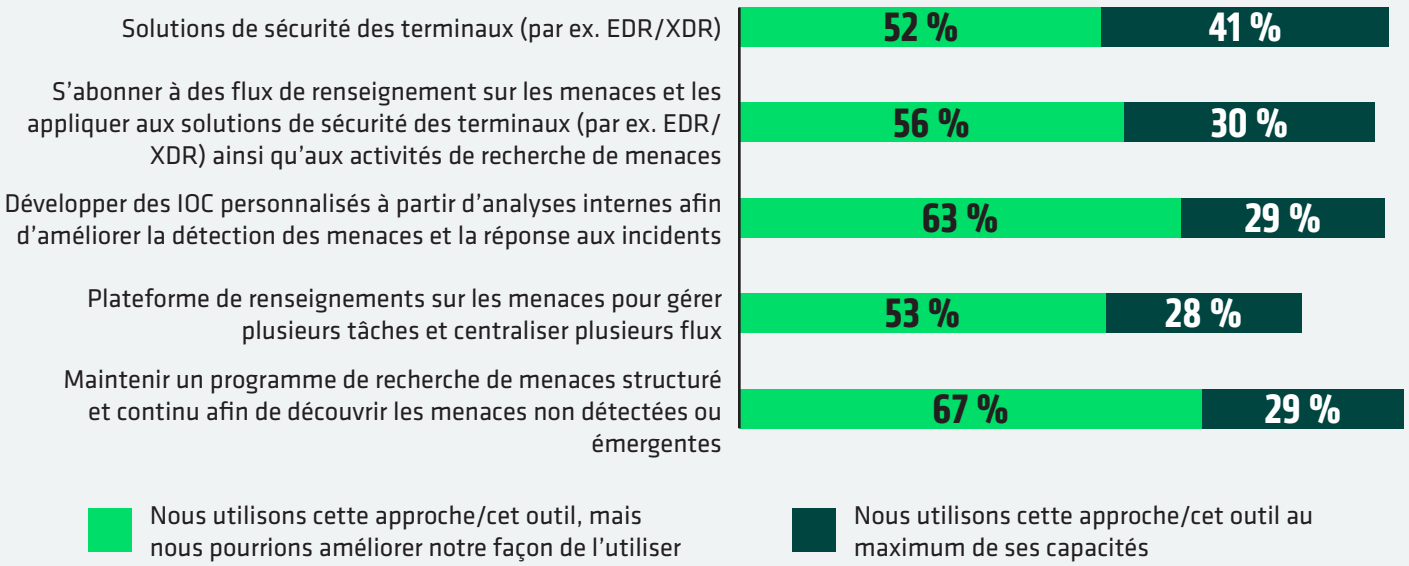
Que fait votre entreprise pour garantir la capacité de récupération de ses données ?

55 %	Exiger une autorisation supplémentaire pour les tâches administratives à risque élevé associées aux solutions de sauvegarde et de restauration
55 %	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)
52 %	Authentification multifacteur sur notre solution de sauvegarde
45 %	Appliquer le principe du moindre privilège aux charges de travail sauvegardées
37 %	Protéger les données critiques grâce à l'immuabilité

De nombreuses entreprises françaises ont renforcé les contrôles d'accès à leurs environnements de sauvegarde. Un peu plus de la moitié exigent une autorisation administrative supplémentaire pour les tâches à risque élevé et imposent une authentification multifacteur. Une proportion similaire suit la règle de sauvegarde 3-2-1. Pourtant, moins de la moitié appliquent le principe du moindre privilège ou protègent leurs données avec l'immuabilité. 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 adoptés, mais pas pleinement utilisés. La plupart des entreprises investissent dans la sécurité des terminaux, les flux de renseignement sur les menaces et les programmes structurés de recherche de menaces, mais seulement un tiers d'entre elles exploitent ces outils à leur plein potentiel. Pour parvenir à une cyber-résilience mature, il faut les intégrer 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 ?

61 % Identifier et corriger les failles des contrôles de sécurité avant de restaurer les systèmes en production

58 % 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 % Créer un référentiel en ligne et sécurisé des systèmes et informations critiques pour soutenir la réponse aux incidents et la restauration

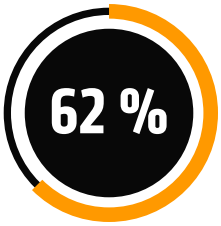
49 % Utiliser un environnement isolé pour enquêter sur les incidents, les corriger et restaurer de manière sécurisée

35 % 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. La plupart simulent des exercices de restauration et corrigent les faiblesses de contrôle avant de restaurer les systèmes, et plus de la moitié conservent les référentiels des systèmes critiques dans un coffre-fort pour faciliter la réponse et la restauration. Pourtant, moins de la moitié utilisent des environnements isolés pour mener des investigations sécurisées ou appliquent l'immuabilité à l'ensemble de leurs 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

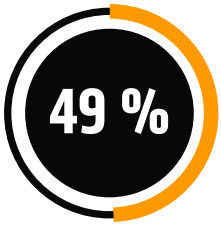
Comment votre entreprise utilise-t-elle les approches/outils de découverte et de classification des données pour minimiser l'exposition aux risques liés aux données dans l'ensemble de son patrimoine de données ?



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

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

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



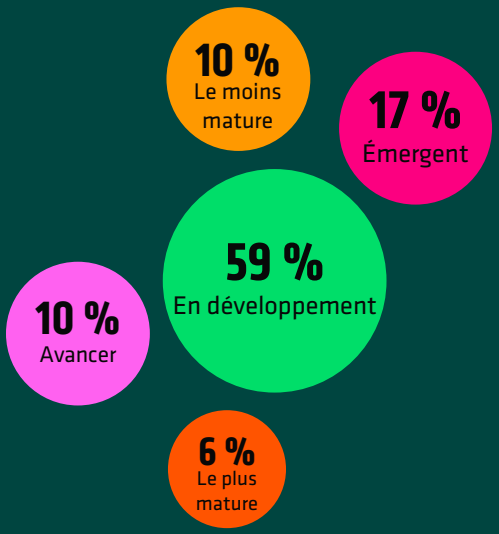
Identifier et hiérarchiser les systèmes pour la sauvegarde

Les entreprises françaises utilisent la découverte et la classification des données de manière plus stratégique pour la conformité, la réponse et la restauration. La majorité d'entre elles traitent les violations de confidentialité et de sécurité et utilisent la classification pour orienter les obligations de conformité en cas d'attaque, tandis qu'une minorité définit l'importance ou hiérarchise les sauvegardes en fonction des risques. 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 6 % 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 (10 %) : 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.

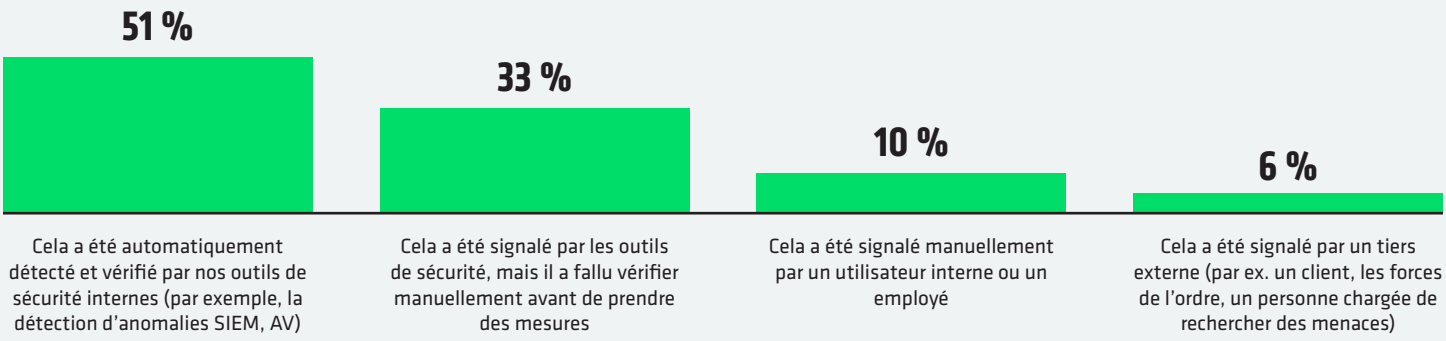
En cours de développement (59 %) : Les pratiques fondamentales, notamment les sauvegardes, les contrôles administrateurs et les renseignement sur les menaces, sont plus courantes, mais restent inégales. Les environnements de restauration, les contrôles de conformité et la correction des failles de sécurité sont appliqués de manière sporadique, ce qui limite l'efficacité des efforts en matière de résilience.

Avancé (10 %) : 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 (6 %) : 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.

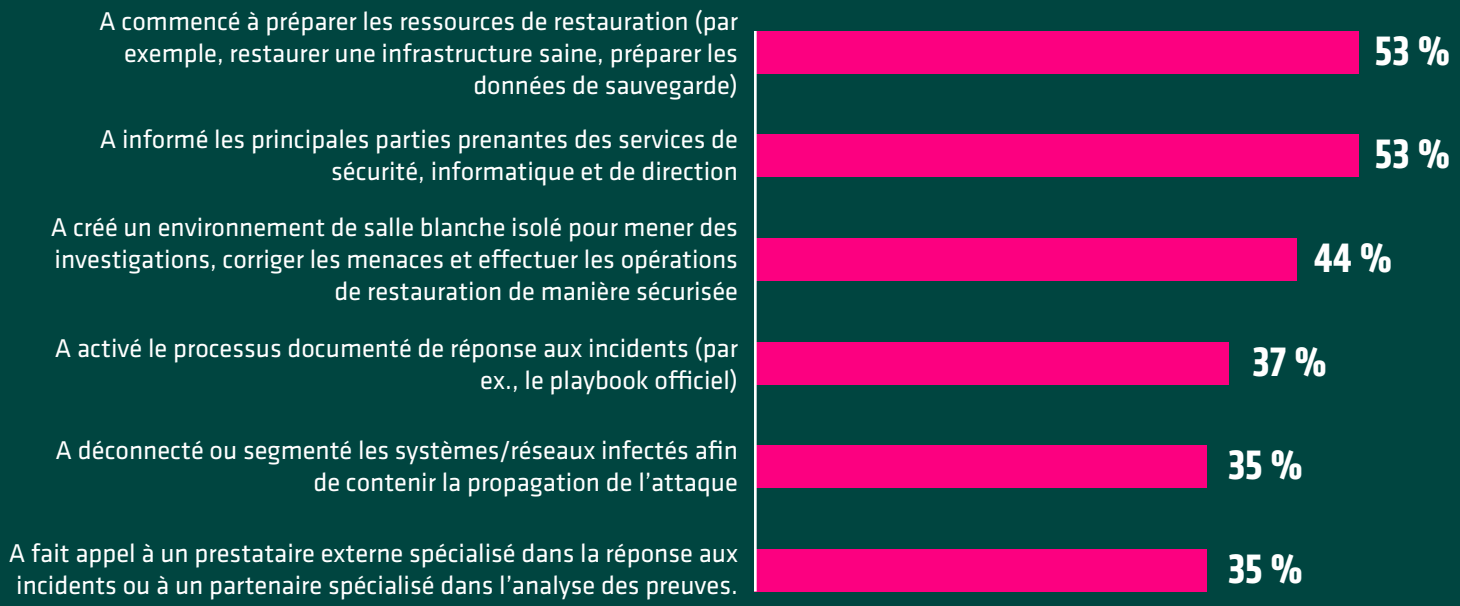
LA RÉSILIENCE DANS L'ADVERSITÉ

COMMENT LES ÉQUIPES ONT IDENTIFIÉ L'ATTAQUE



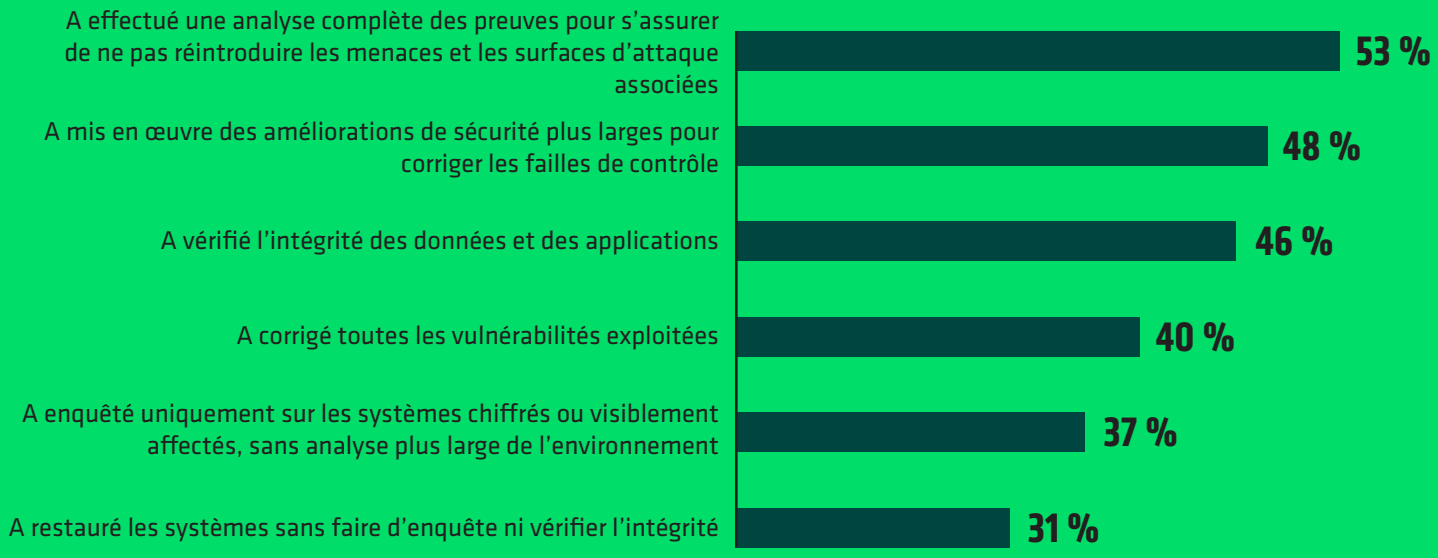
La plupart des entreprises françaises qui sont victimes d'une cyberattaque détectent les incidents via leurs dispositifs internes. Un peu plus de la moitié des attaques ont été identifiées et vérifiées automatiquement par les outils de sécurité en place. Un autre tiers des cas a nécessité une vérification manuelle suite au déclenchement d'alertes. Seule une faible proportion des incidents a été signalée par des rapports d'employés ou de tiers. Ainsi, la détection repose principalement sur des dispositifs internes, mais nécessite toujours une confirmation humaine.

MESURES PRISES PAR LES ÉQUIPES APRÈS CONFIRMATION DE L'ATTAQUE



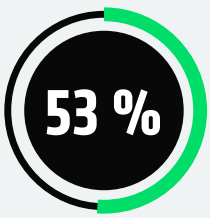
Une fois les attaques confirmées, les entreprises françaises ont rapidement commencé à préparer la restauration. Plus de la moitié d'entre elles ont commencé à restaurer une infrastructure saine et à préparer les données de sauvegarde, et une proportion équivalente a informé les parties prenantes chargées de la sécurité, de l'informatique et de la direction. Moins de la moitié ont mis en place des environnements de salles blanches isolés pour mener des investigations et prendre des mesures de correction en toute sécurité, et seulement un tiers ont suivi un playbook officiel ou fait appel à des experts externes. Cela montre que les actions de réponse restent inégales à toutes les étapes critiques.

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



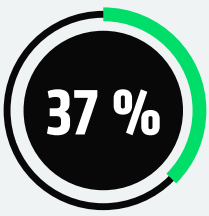
La plupart des équipes ont effectué au moins une partie de l'analyse des preuves et de la correction avant de remettre les systèmes en ligne. Un peu plus de la moitié ont fait une analyse complète des preuves pour s'assurer que les menaces étaient éliminées, moins de la moitié ont renforcé les contrôles ou vérifié l'intégrité des données, et seulement quatre équipes sur dix ont corrigé les vulnérabilités. Près d'un tiers ont restauré les systèmes sans les avoir entièrement validés : il existe donc une possibilité de réinfection et un risque résiduel.

DIFFICULTÉS RENCONTRÉES PAR LES ÉQUIPES PENDANT L'ATTAQUE

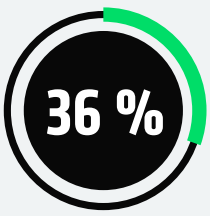


Incapacité à communiquer ou à se coordonner au sein de notre équipe en raison de la panne des systèmes critiques (par ex., e-mail, applications collaboratives, système de tickets)

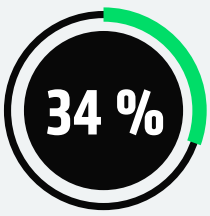
Pression de la direction pour restaurer les systèmes avant que l'attaque ne soit corrigée



Manque d'accès à des points de restauration sains et validés



Nous avons restauré, mais avons ensuite été réinfectés, car les menaces n'étaient pas entièrement éliminées



Les outils de sécurité ont été contournés et les sauvegardes ont été attaquées

Les équipes ont signalé d'importants défis tout au long du processus. Beaucoup ont eu du mal à communiquer ou à se coordonner pendant que les systèmes critiques étaient hors service. D'autres ont subi des pressions de la part de la direction pour restaurer les opérations avant d'avoir fini de corriger les problèmes. Le contournement des outils de sécurité, la réinfection et l'absence de points de restauration sains ont aggravé les difficultés.

LES LACUNES PERSISTANTES DES INVESTISSEMENTS DANS LA RÉSILIENCE

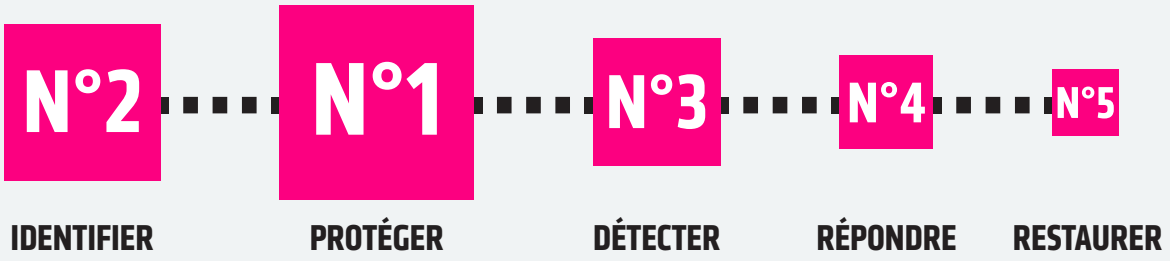
Même les entreprises bien préparées peinent à maintenir leur résilience en cas d'attaque. Plus la pression opérationnelle augmente, plus les failles de coordination, les corrections incomplètes et les risques de réinfection révèlent à quel point la restauration peut être fragile sans processus unifiés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

Ces faiblesses se reflètent dans la manière dont les entreprises françaises allouent aujourd'hui leurs budgets de cyber-résilience. Si la plupart s'alignent sur les normes nationales et les recommandations de l'ANSSI et de la norme ISO/IEC 27001, beaucoup se réfèrent également au cadre de cybersécurité du NIST pour faire un benchmark de leur maturité par rapport à ses cinq fonctions essentielles : identifier, protéger, détecter, répondre et restaurer.

Lorsqu'on leur demande comment ils répartissent les budgets entre ces domaines, la plupart continuent de concentrer leurs investissements dans la prévention, la protection et la détection, et consacrent relativement moins de ressources à la réponse et à une restauration vérifiée. La courbe de maturité reste donc davantage axée sur la défense que sur la restauration, et il est possible 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 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. 58 % des entreprises françaises 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. Près de la moitié (45 %) 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. 39 % 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 entreprises françaises fassent des progrès notables en matière de cyberrésilience, 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 :

- 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

2000065-001 FR 11-2025