veeam Insights

PRIVAL

Du risque à la résilience

Les tendances des ransomwares et les stratégies proactives en 2025

Résumé :

Évaluation des menaces et des défenses contre les ransomwares en 2025

Les attaques par ransomware évoluent, se développent plus rapidement et sont plus sophistiquées que jamais. Une chose est sûre : **la menace omniprésente des ransomwares continuera de frapper les entreprises en 2025 et au-delà.** Que ces attaques proviennent de groupes bien établis ou d'un nombre croissant de cybercriminels « loups solitaires », une absence de préparation minutieuse peut coûter beaucoup de temps et d'argent à une organisation, ainsi que la confiance des parties prenantes.

Pour les aider à contrer ces cybermenaces persistantes, notre rapport « Du risque à la résilience » en 2025 présente plusieurs mesures concrètes que les entreprises peuvent prendre pour limiter les risques et se rétablir plus rapidement après une attaque. **Nous avons interrogé 1 300 entreprises dans le monde** pour évaluer comment les responsables de la sécurité des systèmes d'information (RSSI), les professionnels de la sécurité et les responsables informatiques se rétablissent après une cyberattaque.

Les stratégies testées sur le terrain par des entreprises qui se remettent plus vite d'une attaque reflètent un ensemble de meilleures pratiques de cyber-résilience que toutes les organisations devraient envisager de mettre en œuvre.

Il y a de bonnes nouvelles. Par rapport à notre étude de 2024,[1] **le pourcentage d'entreprises ayant subi au moins une attaque par ransomware ayant entraîné un chiffrement ou une exfiltration de données a légèrement diminué, passant de 75 % à 69 %.** Cette diminution s'explique probablement par l'amélioration continue des pratiques de préparation et de résilience par les entreprises, ainsi que par la collaboration accrue entre les équipes IT et de sécurité. Les gouvernements ont également fait équipe pour éliminer les principaux groupes de ransomware, ce qui a incité les acteurs de la menace à s'adapter et à modifier la dynamique d'attaque au sens large.

Notre analyse révèle **six tendances clés qui façonnent le paysage des menaces de ransomware en 2025** et les informations étayées par les données qui peuvent aider les entreprises à renforcer leur résilience. Des tactiques d'usure à l'augmentation des taux d'exfiltration, jusqu'à la baisse des paiements de rançon et la collaboration accrue entre les parties prenantes, nous examinons le paysage des menaces persistantes et la manière dont les entreprises qui réussissent réduisent les risques et leur impact liés aux ransomwares.

1 300

entreprises du monde entier ont été interrogées par Veeam

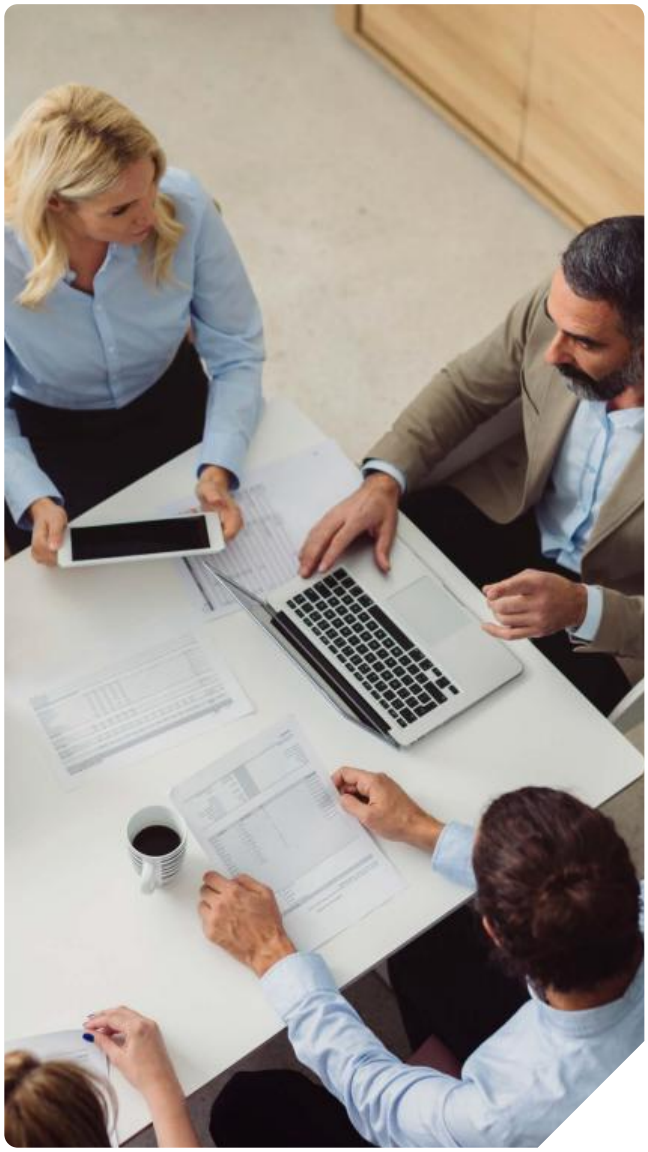
6 %

moins d'entreprises touchées par au moins une attaque par ransomware

Pour relever les défis des ransomwares, les entreprises doivent passer d'une sécurité réactive à des **stratégies de cyber-résilience** proactives, en s'appuyant sur la préparation, la rapidité de réponse et les mesures de récupération sécurisées destinées à réduire les risques.

Les 6 principales tendances des ransomwares à surveiller en 2025

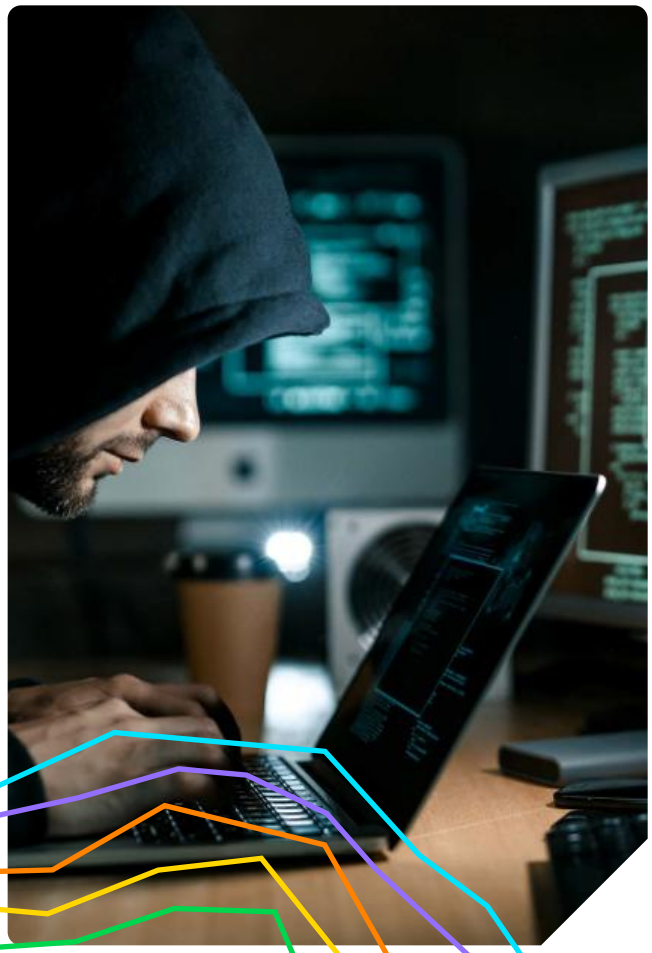
1. **Les forces de l'ordre obligent les acteurs malveillants à s'adapter**
2. **Les attaques d'exfiltration de données se multiplient**
3. **Les paiements liés aux ransomwares diminuent**
4. **Nouvelles conséquences juridiques du paiement de rançons**
5. **La collaboration renforce la résilience contre les ransomwares**
6. **Les budgets augmentent pour la sécurité et la restauration, mais davantage sont nécessaires**



Les forces de l'ordre obligent les acteurs malveillants à s'adapter

TREND# 1

En 2024, les autorités ont lancé avec succès plusieurs opérations visant à démanteler d'importants groupes de cybermenaces. L'élimination de ces groupes plus importants est évidemment une évolution positive pour la défense contre les menaces. Cependant, **le nombre de petits groupes et de « loups solitaires » qui propagent desattaques a augmenté.** Certains groupes ont également déplacé leur objectif en aval, en évitant les infrastructures critiques pour réduire la surveillance des forces de l'ordre et en ciblant les petites et moyennes entreprises (PME) qui ont souvent des cyberdéfenses plus faibles.



Voici quelques-uns des plus grands groupes qui ont été fermés, qui ont disparu ou qui ont cessé leurs activités :

- **LockBit**, un groupe de ransomware en tant que service (RaaS), éliminé par les efforts des forces de l'ordre menées par la National Crime Agency du Royaume-Uni en collaboration avec le FBI et Europol.[2]
- **BlackCat**, un groupe RaaS, que le FBI avait déjà démantelé en 2023,[3] a mis fin à ses opérations en mars 2024 à la suite de son attaque réussie ciblant Change Healthcare – et d'une rançon d'une valeur de plus de 22 millions de dollars américains[4]
- **Black Basta**, qui a semblé cesser ses activités en 2025 après la divulgation de journaux de discussion, révélant des inquiétudes quant à la surveillance par les forces de l'ordre après une attaque contre le système de santé américain Ascension, qui comprenait 140 hôpitaux dans 19 États.[5]

Les attaques d'exfiltration de données se multiplient

TREND# 2

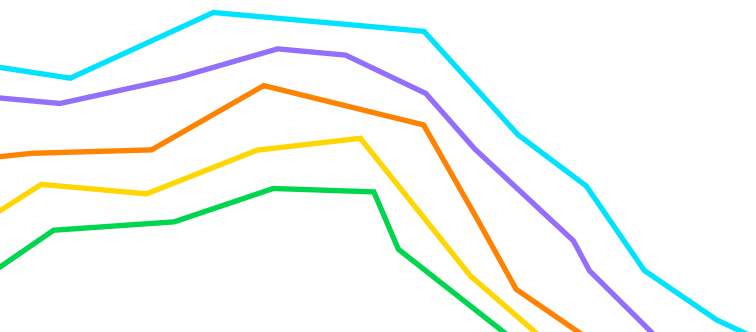
À mesure que le paysage des menaces évolue, les acteurs malveillants continuent de changer de tactique. Il convient de noter que si les techniques d'exfiltration sont généralement utilisées conjointement avec le chiffrement des données, le nombre de victimes uniquement d'exfiltration ayant payé une rançon a augmenté au cours du quatrième trimestre.[6]

L'exfiltration reflète une approche de type « smash and grab » courante dans les attaques par ransomware traditionnelles précédant le chiffrement. Il en va de même pour les applications et les infrastructures cloud mal sécurisées. Outre cette évolution vers l'exfiltration des données et la double extorsion qui combine le chiffrement pour restreindre l'accès et la publication des données sensibles exfiltrées, **on constate une réduction du temps de séjour, c'est-à-dire le temps qui s'écoule entre la compromission et le lancement de l'attaque, avec de nombreuses attaques survenant en quelques heures seulement.**

Au deuxième trimestre 2024, Coveware by Veeam a constaté que deux des trois principaux adversaires de ransomware de ce trimestre présentaient un temps de présence moyen inférieur à 24 heures.[7] Il s'agit d'une baisse marquée par rapport aux trimestres précédents, et la tendance s'est poursuivie au quatrième trimestre.

Lorsque les auteurs de menace accèdent aux réseaux de leurs victimes, ils ont tendance à utiliser des techniques de mouvement latéral. Ils cherchent à faciliter l'exfiltration ou à atteindre un objectif précis (la compromission des hyperviseurs VMware ESXi, par exemple) afin de contraindre les victimes à payer la rançon. Ces stratégies efficaces et bien rodées se traduisent souvent par des attaques plus rapides qui peuvent être difficiles à détecter et à contenir.

Trop souvent, les entreprises dont la cybersécurité est faible et dont l'architecture réseau est complexe sont particulièrement vulnérables à l'exfiltration de données et aux cybermenaces qui y sont associées.



Les paiements liés aux ransomwares diminuent

TREND# 3

Heureusement, la valeur totale des paiements liés aux ransomwares a diminué en 2024 par rapport à 2023.[8] Plus d'un tiers des organisations victimes d'une attaque par ransomware (36 %) n'ont pas payé de rançon et 25 % n'ont pas payé, mais ont quand même pu restaurer leurs données.

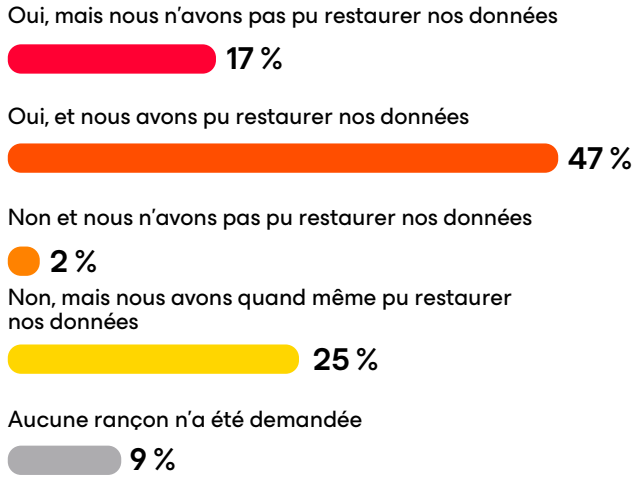
Parmi celles qui ont payé, 82 % ont payé moins que la rançon initiale et 60 % ont payé moins de la moitié de cette somme. Ces données concordent également avec ce que Coveware by Veeam a constaté de première main lors de son intervention auprès des entreprises impactées en 2024, lorsque le **paiement médian a diminué de 45 % au quatrième trimestre** pour atteindre environ 110 000 $, un niveau historiquement bas.

Seules 25 % des entreprises ayant recours à l'expertise de réponse aux incidents de Coveware by Veeam ont payé une rançon. Cela constitue une « étape importante dans la lutte contre les ransomwares ».[9]

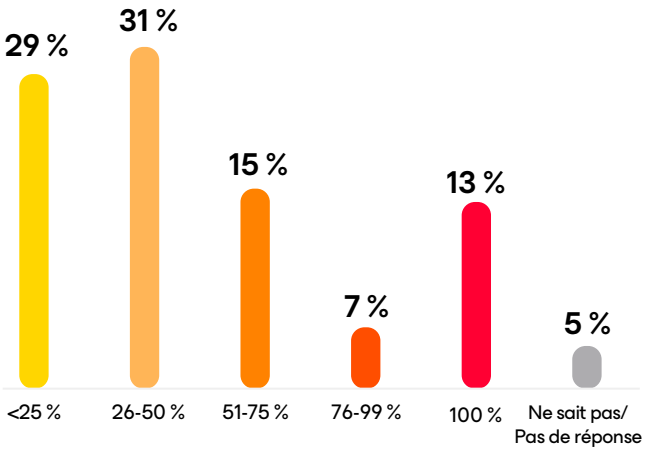
Comparativement aux entreprises ayant recours aux services de réponse aux incidents de Coveware by Veeam, les autres entreprises étaient 156 % plus susceptibles de payer une rançon. Ces données suggèrent que **le recours à des tiers expérimentés pour répondre aux incidents se traduit par une diminution des rançons payées, des montants de rançon plus faibles et des pratiques globalement plus résilientes.**

Les victimes hésitent de plus en plus à payer la rançon, car elles ne peuvent pas faire confiance aux attaquants pour restituer leurs données. Les entreprises ont également amélioré de manière proactive leurs propres plans de réponse aux incidents, notamment en utilisant des sauvegardes inaltérables.

Votre entreprise a-t-elle payé une rançon pour restaurer ses données ?



Pourcentage de la rançon versée



Nouvelles conséquences juridiques du paiement de rançons

TREND#4

Le paiement d'une rançon peut s'avérer très coûteux, car cela incite les attaquants et confirme qu'une entreprise vulnérable est prête à payer. En fait, **parmi celles qui ont payé une rançon, 69 % ont été attaquées plus d'une fois.** Les entreprises qui ne prennent pas de mesures pour renforcer leur capacité de défense et de réponse se retrouvent avec moins d'options lorsqu'une attaque se produit.

69 %

des entreprises ayant payé une rançon ont été attaquées plusieurs fois

L'évolution des initiatives en matière de réglementation et de signalement, ainsi que l'application coordonnée de la loi par les autorités dans l'ensemble des juridictions, ont également contribué à la baisse des rançons. Notamment, l'International Counter Ransomware Initiative (CRI), lancée par le gouvernement américain en 2021, et son groupe de travail affilié rassemblent 68 pays dans le but de perturber l'écosystème des ransomwares et de développer des approches politiques communes.[10]

En 2023, 40 membres de la CRI ont signé un engagement gouvernemental commun visant à « décourager fortement quiconque de payer une demande de ransomware ».[11] Certains pays ont également proposé des lois interdisant aux organisations du secteur public de payer des rançons, comme le Royaume-Uni en janvier 2025[12] , et deux États américains (Floride et Caroline du Nord) ont adopté de telles lois.[13]

Le FBI décourage les organisations de payer des rançons,[14] et le département du Trésor des États-Unis informe qu'il peut y avoir des risques de sanctions associés aux paiements effectués à des entités bloquées par l'Office of Foreign Asset Control (OFAC).[15] Les entreprises internationales doivent également tenir compte d'autres risques de paiement et exigences de conformité.

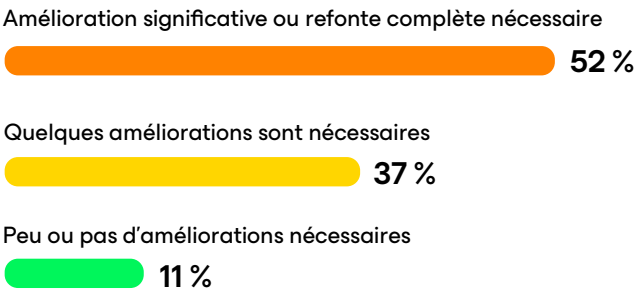
La collaboration renforce la résilience contre les ransomwares

TREND# 5

L'amélioration de la collaboration et de la communication entre les équipes chargées des opérations informatiques et de la sécurité a également aidé les organisations à renforcer leur cyber-résilience. Cependant, la majorité des personnes interrogées (52 %) ont déclaré qu'une amélioration significative ou une refonte complète était nécessaire pour aligner ces équipes. Et seulement 11 % ont déclaré que peu ou pas d'amélioration était nécessaire.

Simultanément, des acteurs de plateformes et des technologies s'associent pour agréger les informations sur les ransomwares et fournir des services qui aident les entreprises à améliorer leurs défenses. Le signalement des ransomwares et autres cyberattaques aux autorités régulatrices, ainsi qu'aux réseaux de partenaires émergents et aux échanges d'informations sectorielles, renforce les défenses collectives.

Alignement des équipes d'exploitation informatique et de sécurité



> « Nous avons un objectif commun de sécurité, et nous devons le faire ensemble. Donc, je ne pense pas qu'il y ait moyen d'arriver à un avenir cyber-sécurisé sans que les entités publiques et privées, et leurs propositions de valeur, ne se réunissent pour trouver des solutions. »[16]

Sue Gordon

ancienne directrice adjointe principale du renseignement national des États-Unis

Regardez l'interview complète de Sue Gordon avec Gil Vega, RSSI de Veeam, ici

Les budgets augmentent pour la sécurité et la restauration, mais davantage sont nécessaires

TREND# 6

Surtout, ils permettent aux fournisseurs et aux agences de fournir des indicateurs de compromission et des stratégies d'atténuation aux autres membres de l'écosystème.

Si de nombreuses techniques de défense contre les ransomwares montrent des signes d'amélioration, **certaines entreprises n'augmentent pas assez rapidement leurs budgets de sécurité et de restauration** pour suivre le rythme de l'évolution des menaces. Les équipes de sécurité sont également dispersées en raison de la diversité des ransomwares et autres vecteurs d'attaque auxquels elles sont confrontées.

Dans l'ensemble, les entreprises ont tendance à consacrer un peu plus de ressources à la sécurité (31 % du budget IT en moyenne) qu'à la restauration (28 % en moyenne), ce qui laisse entrevoir une vulnérabilité potentielle au moment de mettre en place une résilience proactive. Les directeurs informatiques (DSI) et les RSSI doivent trouver l'équilibre approprié en fonction des besoins de leur organisation lors de l'allocation du budget pour chaque domaine. Les résultats de l'étude indiquent que **des investissements insuffisants dans la sécurité ou la restauration peuvent affaiblir la capacité des entreprises à se prémunir et à répondre aux attaques par ransomware.** L'absence d'attention portée à la restauration, en particulier, peut provoquer des pertes de temps et de ressources précieuses, surtout lorsque des acteurs malveillants visent les cibles de sauvegarde.

Du côté positif, **94 % des entreprises ont augmenté leur budget de restauration pour 2025 et 95 % l'ont augmenté pour la prévention**, ce qui indique une priorité croissante pour renforcer la cyber-résilience.

Questions posées par votre conseil d'administration après une attaque par ransomware

Comment l'attaque a-t-elle eu lieu ?
Décrivez en détail la cause, la portée et l'impact.

Qu'a-t-on fait pour éliminer cette menace ?
Indiquez si une rançon a été payée (si oui, comment) et les mesures prises pour écarter la menace et restaurer.

Quels systèmes, données et opérations ont été touchés ?
Décrivez les impacts de l'attaque, y compris les conséquences financières et réputationnelles.

Quelles mesures ont été prises pour améliorer la cyber-résilience et prévenir de futures attaques ?
Identifiez les mesures prises pour renforcer la sécurité et la restauration, comme les changements de mesures de gouvernance ou les priorités d'investissement dans la cybersécurité.

94 %
des entreprises ont augmenté leur budget de restauration en 2025

95 %
des entreprises ont augmenté leur budget de restauration consacré à la prévention

Facteurs clés de succès :

Ce que les entreprises ayant de meilleurs résultats ont en commun

Face à la soudaine attaque par ransomware, les entreprises doivent agir immédiatement et de manière coordonnée. Le temps presse. Il est donc essentiel d'évaluer l'ampleur de la violation, de contenir la menace et de lancer votre réponse à l'incident en quelques minutes.

L'analyse des caractéristiques communes des entreprises qui ont obtenu plus ou moins de résultats après une attaque par ransomware peut vous aider à renforcer vos cyberdéfenses.

Cet écart important de réussite soulève la question suivante :

Pourquoi tant d'entreprises ont-elles eu du mal à faire face à une cybermenace aussi répandue ?

À la lumière des résultats de l'étude, plusieurs lacunes sont corrélées à une résilience moindre face aux ransomwares. De plus, en examinant les leçons apprises par les entreprises au cours de l'année écoulée après avoir subi une attaque, plusieurs modèles se dégagent pour améliorer la protection et la restauration face aux ransomwares.

Une entreprise était considérée comme plus performante si cinq des neuf critères suivants étaient remplis.

- ✔ Aucune rançon n'a été payée par l'entreprise qui a pu restaurer ses données.
- ✔ L'entreprise n'a pas été attaquée plusieurs fois.
- ✔ L'entreprise n'a pas subi d'impact significatif.
- ✔ Les données de production de l'entreprise n'étaient pas chiffrées.
- ✔ L'entreprise a été jugée prête ou entièrement préparée après l'attaque.
- ✔ L'entreprise a restauré des fonctionnalités sur plus de 80 % de ses serveurs.
- ✔ Plus de 90 % des données affectées de l'entreprise ont été restaurées.
- ✔ Moins de 20 % des plateformes de production de l'entreprise ont été touchées.
- ✔ Moins de 10 % des cibles de sauvegarde ont été modifiées ou supprimées lors de la tentative de l'acteur malveillant.

Les guides de stratégie ransomware améliorent la préparation aux attaques

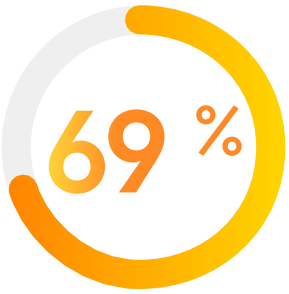
La confiance avant l'attaque ne correspond pas toujours à la réalité : **69 % des victimes de ransomware ont déclaré qu'elles pensaient être préparées avant d'être attaquées, mais cette confiance diminue de plus de 20 % après l'attaque,** mettant en évidence de graves lacunes dans la planification.

L'écart entre la perception de l'état de préparation et la réalité était également plus important pour certains rôles. En particulier, l'indice de préparation des DSI a diminué de 30 % après une attaque, contre une baisse de 15 % pour les RSSI, ce qui indique que ceux-ci ont une compréhension plus précise de la posture de sécurité de leur organisation.

Dans l'ensemble, il est essentiel de favoriser l'alignement organisationnel autour de la cyber-résilience, des mesures de préparation et des procédures de réponse aux incidents. Cela devrait inclure des formations et des exercices dans tous les groupes concernés afin de soutenir une réponse cohérente et coordonnée pendant et après une attaque.

Alors que 98 % des personnes interrogées disposaient d'un guide de stratégie ransomware, **moins de la moitié des entreprises disposaient d'éléments techniques clés** tels que des vérifications et la fréquence des sauvegardes (44 %), des copies de sauvegarde et l'assurance de l'intégrité (44 %), des dispositions alternatives en matière d'infrastructure (37 %), des plans de confinement ou d'isolation (32 %) et une voie hiérarchique prédéfinie (30 %).

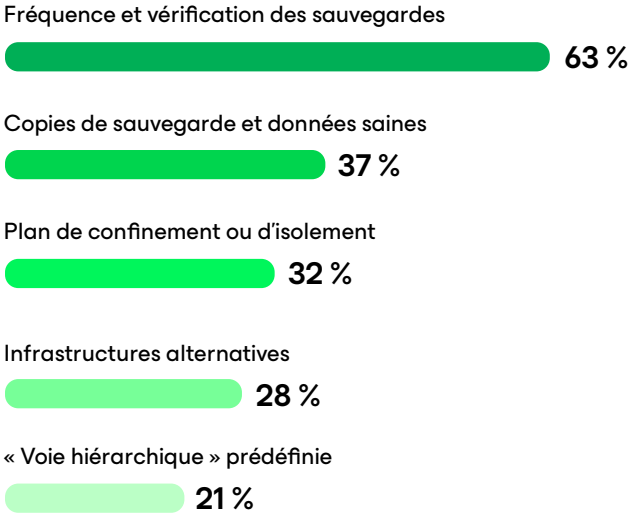
Les entreprises ayant **obtenu de meilleurs résultats ont eu une fréquence beaucoup plus élevée d'inclusion de ces cinq éléments techniques clés dans leurs guides.**



étaient confiants dans leur préparation face à une attaque par ransomware

ont montré une baisse de confiance dans la préparation de leur entreprise après une attaque

Éléments clés du guide stratégique pour les entreprises ayant connu de meilleurs résultats



Sauvegarde proactive et restauration pour renforcer la résilience

La restauration sécurisée de sauvegarde est essentielle, mais elle s'avère plus difficile que beaucoup ne l'imaginent. En fait, **89 % des entreprises ont vu leurs cibles de sauvegarde visées par les acteurs malveillants.**

Pire encore, 34 % en moyenne de leurs cibles de sauvegarde ont été modifiées ou supprimées. Moins de 10 % d'entre elles ont réussi à restaurer plus de 90 % de leurs serveurs dans la limite des attentes, et seulement 51 % ont restauré la majorité de leurs serveurs.

La planification de la restauration est essentielle et comporte plusieurs étapes. Les équipes IT et de sécurité doivent contenir ou supprimer la cybermenace, puis remédier aux accès à l'aide d'outils tels que la gestion des identités et des accès et d'autres solutions de cybersécurité, avant de restaurer définitivement les données dans un environnement sécurisé.

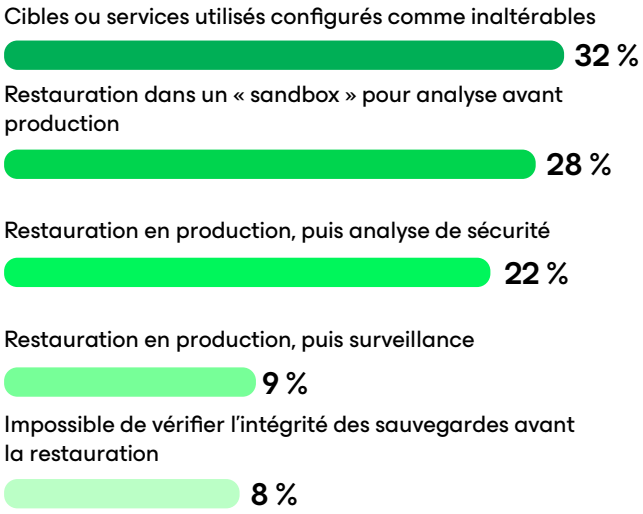
Les sauvegardes sécurisées ont également été sous-utilisées en tant que mesure proactive. **Seuls 32 % des personnes interrogées ont utilisé des cibles ou des services configurés comme inaltérables,** alors que 28 % seulement ont restauré les données dans un environnement de type sandbox et en ont analysé l'intégrité. **Pas moins de 39 % des répondants ont dû restaurer leurs données directement dans l'environnement de production, et 8 % n'ont pas pu vérifier l'intégrité de la sauvegarde avant de les restaurer.**

Pour limiter les risques d'entreprise, les dirigeants et les responsables IT doivent s'assurer que les données et les sauvegardes sont analysées et exemptes de tout logiciel malveillant avant de les restaurer en production. Dans le cas contraire, ils s'exposent à toute une série de conséquences graves, notamment : réinfection rapide, mouvement latéral, mécanismes de persistance, détonation retardée, interruption d'activité prolongée, violation de la conformité et plus encore.

89 %

des entreprises ont vu leurs cibles de sauvegarde visées par les acteurs malveillants

Méthode de vérification de l'intégrité des sauvegardes



Le pouvoir de « l'humain » dans la résilience face aux ransomwares

Alors que ces aspects techniques de la restauration sont essentiels, trop d'entreprises négligent les éléments « humains » cruciaux dans leurs guides anti-ransomware.

Seulement 26 % des entreprises avaient mis en place un processus de décision concernant le paiement de la rançon, afin de guider une réponse rapide aux demandes de paiement en fonction de l'impact potentiel. Bon nombre d'entre elles ne disposent pas non plus de procédures permettant d'informer les forces de l'ordre, ce qui pourrait faciliter la restauration et la conformité.

Plus d'un tiers des entreprises ont fait appel à des membres de leur équipe interne pour communiquer avec les auteurs de menace. Les autres comptent sur des tiers pour les assister, notamment des spécialistes de la réponse aux incidents et de la négociation des rançons. Ces spécialistes sont indispensables pour orienter l'engagement en fonction d'une compréhension détaillée du comportement des acteurs de la menace, ce qui permet d'obtenir de meilleurs résultats. Le fait que des membres de l'équipe interne communiquent avec des auteurs de menace peut également exposer par inadvertance une organisation à des risques et à des menaces supplémentaires.

Enfin, seulement 30 % des entreprises disposent d'une voie hiérarchique prédéfinie pour faire face aux attaques. La voie hiérarchique contribue à assurer des échelles d'autorisation et d'approbation adéquates pour prendre des décisions cruciales pendant la réponse à l'incident, y compris la prise de contact avec les acteurs malveillants ou le paiement d'une rançon.

Quel que soit le jour ou l'heure, c'est toujours un mauvais moment pour subir une attaque par ransomware. C'est pourquoi il est si important de disposer d'une feuille de route pour répondre à ces menaces stressantes et urgentes.

26 %

des entreprises avaient un processus décisionnel concernant le paiement d'une rançon

Rassembler tous les éléments

Considérées ensemble, ces mesures mettent en évidence une différence de mentalité essentielle entre les entreprises qui ont fait preuve de résilience face aux attaques par ransomware au cours de l'année écoulée et celles qui ne l'ont pas fait :

Les entreprises qui réussissent intègrent la cyber-résilience à leur discipline quotidienne. Elles intègrent des stratégies proactives dans l'ensemble de leurs opérations informatiques quotidiennes.

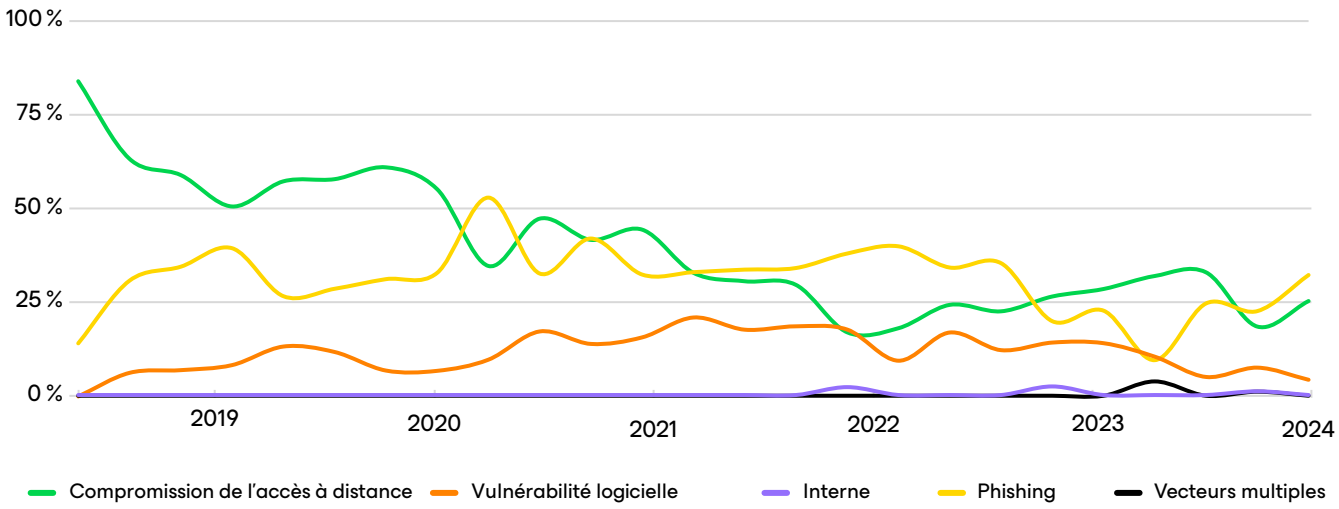
Après une attaque, les entreprises les plus performantes étaient également plus susceptibles de renforcer les programmes de formation et de sensibilisation des employés, ce qui peut contribuer à atténuer les attaques d'ingénierie sociale telles que le phishing. Les stratégies de mise à jour logicielle sont également généralement renforcées après une attaque afin de se prémunir contre l'exploitation continue des vulnérabilités logicielles. Notamment, **nombre d'entreprises ont déployé des solutions de sauvegarde et de restauration plus récentes et sont passées au cloud ou à des services gérés après une attaque.** Ces mesures permettent de se prémunir contre les vecteurs d'attaque courants et d'améliorer la résilience.

Les entreprises qui réussissent ont mis en œuvre des éléments de restauration plus proactifs après une attaque que les entreprises moins performantes.

Ces pratiques de défense proactive permettent également de faire face aux vecteurs d'accès initiaux les plus courants détectés par Coveware by Veeam au cours de son travail au quatrième trimestre, notamment la compromission d'accès à distance, le phishing, les vulnérabilités logicielles, etc.

Une défense efficace contre les attaques par ransomware ne peut pas être simplement invoquée en cas d'attaque. Ils doivent faire partie intégrante du fonctionnement quotidien de l'entreprise.

Vecteurs d'attaques par ransomware



Source : Coveware by Veeam, « Le succès des forces de l'ordre contre les ransomwares se poursuivra-t-il en 2025 ? »

Faire le point et passer à l'action

Les attaques par ransomware peuvent nuire à la réputation d'une entreprise et saper la confiance de ses clients et utilisateurs finaux. Les coûts liés à une attaque peuvent également avoir un impact financier sévère : temps d'arrêt opérationnel, perte de productivité et amendes ou procédures judiciaires éventuelles.

En cas d'attaque, les entreprises doivent mettre l'accent sur le travail d'équipe, la collaboration et la communication, en restant calmes et posées tout en mettant en œuvre les stratégies de réponse définies dans leur guide de réponse aux attaques par ransomware. Au lendemain d'une attaque, les entreprises doivent faire le point, s'attaquer aux causes premières de l'attaque et prendre les mesures nécessaires pour renforcer leur résilience afin d'éviter que ce type de sinistre ne se reproduise.

Les entreprises ayant réalisé les restaurations les plus réussies ont suivi les meilleures pratiques suivantes :

- ✔ Élaborez des plans robustes de réponse aux incidents avec des rôles et des responsabilités clairement définis.
- ✔ Concevez une stratégie de sauvegarde et restauration. Suivez la règle de résilience des données 3-2-1-1-0 pour configurer les cibles comme inaltérables ou protégées d'une autre façon et vous assurer que les sauvegardes sont exemptes de logiciels malveillants avant la restauration.[2]
- ✔ Mettez en œuvre des mesures et des processus de sécurité proactifs tels qu'une architecture Zero Trust, une gestion des identités et des accès, des politiques de mise à jour logicielle, des solutions de détection et de réponse plus récentes, ainsi que des services cloud ou gérés.
- ✔ Augmentez les dépenses en outils de détection des menaces pour la prévention et en solutions de sauvegarde pour la restauration. Les plateformes de résilience des données intégrées aux outils de sécurité et dotées de fonctionnalités permettant de prévenir ou de détecter les menaces, comme la Veeam Data Platform[3], contribuent considérablement à améliorer la cybersécurité et la résilience.
- ✔ Organisez des programmes de formation à la sécurité et sensibilisez l'ensemble des collaborateurs.

À propos du rapport

Pour rédiger le rapport sur les ransomwares de cette année, 1 300 entreprises ont été interrogées dont 900 ont subi au moins une attaque par ransomware ayant entraîné le chiffrement ou l'exfiltration au cours des 12 mois écoulés. Les personnes interrogées étaient des responsables de la sécurité des systèmes d'information (RSSI) ou des cadres ayant des responsabilités similaires, ainsi que des professionnels de la sécurité et des responsables informatiques des Amériques, en Europe et en Australie.

Visitez notre page d'accueil pour en savoir plus sur les solutions de sécurité susceptibles d'améliorer votre posture de cybersécurité en vue d'accélérer la restauration ou pour parler avec l'un de nos experts Veeam.

Les stratégies de cyberdéfense sont une question qui concerne le conseil d'administration . N'attendez pas qu'une cyberattaque se produise. Prenez les mesures nécessaires pour minimiser les risques et maintenir la résilience.

Sources

1 https://go.veeam.com/ransomware-trends-executive-summary-2024-us

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

4 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

5 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

6 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

7 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

8 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

9 https://www.coveware.com/blog/2025/1/31/q4-report

10 https://counter-ransomware.org/aboutus

11 https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

12 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

13 https://www.databreachtoday.com/blogs/as-states-ban-ransom-payments-what-could-possibly-go-wrong-p-3273

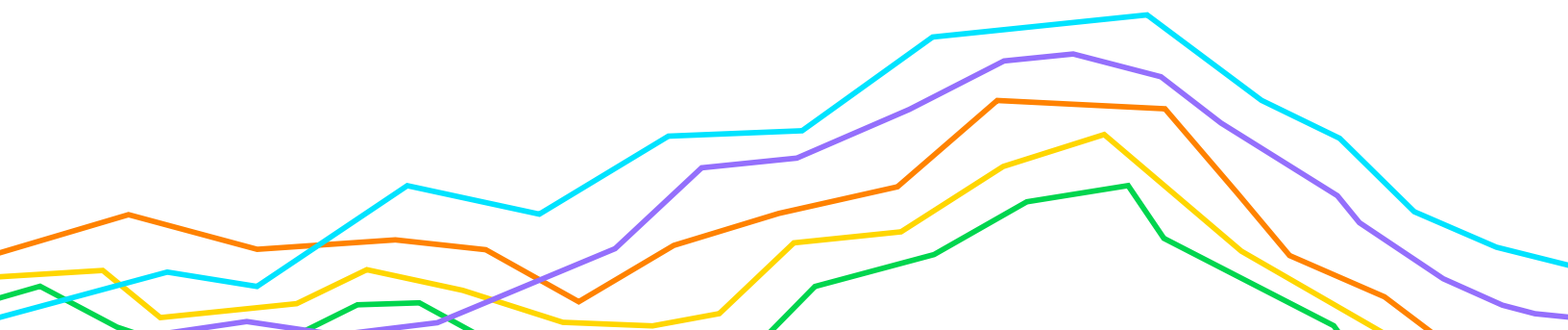
14 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

15 https://ofac.treasury.gov/media/912981/download?inline

16 https://www.youtube.com/watch?v=Fs2xq0pb7YQ

17 https://www.veeam.com/blog/fr/321-backup-rule.html

18 https://www.veeam.com/fr/products/veeam-data-platform.html



veeam Insights