DELL Technologies

# Ransomware : renforcer la cybersécurité et la résilience avec Dell Technologies

## Qu’est-ce qu’un ransomware ?

Un ransomware (ou ransomware) est un type de logiciel malveillant qui bloque l’accès à un système informatique ou à des données en attendant le paiement d’une rançon. Il s’agit de l’un des types de cyberattaques qui provoquent le plus de perturbations. 50 % des organisations du monde entier ont été touchées par un ransomware au moins une fois au cours de l’année écoulée, et le temps d’arrêt moyen consécutif à une attaque par ransomware est de trois semaines, entraînant des interruptions d’activité importantes.

## La menace croissante du ransomware

Un ransomware (ou ransomware) est un type de logiciel malveillant qui bloque l’accès à un système informatique ou à des données en attendant le paiement d’une rançon. Il s’agit de l’un des types de cyberattaques qui provoquent le plus de perturbations. 50 % des organisations du monde entier ont été touchées par un ransomware au moins une fois au cours de l’année écoulée, et le temps d’arrêt moyen consécutif à une attaque par ransomware est de trois semaines, entraînant des interruptions d’activité importantes.

## Principe de fonctionnement d’un ransomware

Le ransomware infecte généralement les organisations lorsqu’un utilisateur clique sur un lien malveillant, ouvre une pièce jointe infectée ou se rend sur un site Web compromis. Il s’introduit alors dans les systèmes pour chiffrer les fichiers et les rendre illisibles. Généralement, le programme de ransomware affiche un message exigeant un paiement (souvent en cryptomonnaie) en échange d’une clé de déchiffrement. Si la victime refuse de payer la rançon, le hacker peut menacer de supprimer des données ou de les divulguer publiquement. L’attaque WannaCry, survenue en 2017, est un exemple bien connu de ransomware ; l’attaque s’est répandue rapidement dans le monde entier, touchant des établissements hospitaliers, des entreprises et des organismes gouvernementaux, et a eu des répercussions financières considérables. Avec plus de 200 000 systèmes affectés dans 150 pays en seulement quelques jours, le virus WannaCry a eu un impact économique mondial de l’ordre de 4 à 8 milliards de dollars selon Cyber Risk Management (CyRiM) et Lloyds of London.

Parmi les entreprises touchées figuraient deux grandes multinationales : FedEx, qui a déclaré une perte de 300 millions de dollars à la suite d’une interruption de service et d’un nettoyage de données, et Renault-Nissan, qui a dû interrompre temporairement sa production dans plusieurs usines. Les coûts cachés d’une attaque par ransomware peuvent être nombreux :

- paralysie de l’entreprise et perte de productivité ;
- atteinte à la réputation ;
- coûts du rétablissement du système et de l’application des correctifs ;
- amendes légales et sanctions réglementaires.

Face à une attaque par ransomware, il est important que les entreprises suivent ces quelques conseils :

- ne payer que si cela est absolument nécessaire : rien ne garantit que les pirates rétabliront l’accès aux données ;
- restaurer les données à partir d’une sauvegarde, si possible ;
- signaler l’attaque aux autorités ;
- renforcer leurs défenses pour prévenir toute infection future (par exemple, maintenir les logiciels à jour, former le personnel, protéger les points de terminaison).

## Combattre les attaques par ransomware avec Dell Technologies

Dell Technologies met entre les mains des entreprises des outils complets et avant-gardistes conçus pour déjouer les risques de ransomware avant qu'ils ne causent préjudice.

### Sécurité renforcée des points de terminaison avec Dell Trusted Device

Les terminaux sont souvent les principaux points d'entrée des attaques par ransomware, ce qui fait de la sécurité des points de terminaison une priorité essentielle. Les appareils Dell Trusted Device intègrent des fonctions de sécurité matérielles qui protègent les systèmes sans compromettre les performances. Des solutions telles que Dell SafeBIOS et SafeID protègent les terminaux contre les accès non autorisés, tandis que Dell SafeData chiffre les données pour protéger les informations sensibles, même en dehors du pare-feu de l'entreprise. En intégrant la sécurité directement dans les appareils, les entreprises assurent une protection au niveau du matériel, ce qui réduit les opportunités d'attaque pour les pirates.

### Détection proactive avec CrowdStrike

Les attaques par ransomware peuvent être évitées si les entreprises utilisent les outils appropriés pour détecter les menaces et réagir en temps réel. Proposé dans le cadre de la gamme de solutions Dell, CrowdStrike fournit une plateforme de protection des points de terminaison de nouvelle génération, optimisée par l'IA et l'analytique comportementale. Cette technologie identifie et neutralise les activités suspectes avant qu'elles ne deviennent une véritable attaque. En s'intégrant de manière transparente à l'infrastructure Dell, CrowdStrike offre aux équipes IT une excellente visibilité sur l'ensemble de leur environnement pour leur permettre de réagir immédiatement et efficacement face aux menaces.

### Protection complète des données avec Dell PowerProtect

Les solutions Dell PowerProtect constituent le pilier de la résilience face aux ransomwares. Ces outils avancés de protection des données sont conçus pour protéger les données d'entreprise contre les menaces internes et externes. Certaines fonctionnalités, comme les sauvegardes immuables, empêchent les ransomwares de modifier, supprimer ou chiffrer vos données, formant un filet de sécurité fiable même face à des attaques avancées. Dell PowerProtect Cyber Recovery Vault, par exemple, isole les données critiques du réseau à l'aide d'une technologie d'isolement. Vos données restent ainsi intactes, même au cours des violations les plus sophistiquées. Grâce à une détection automatisée des anomalies et à des workflows intelligents, les organisations sont en mesure de détecter rapidement les activités malveillantes et de réagir avant que le ransomware ne se propage.

### Sécurité réseau avancée et microsegmentation avec Dell PowerSwitch Networking et SmartFabric OS

Protège contre les attaques « Zero-Day » en fournissant une segmentation avancée du réseau, des contrôles d'accès stricts et une analyse du trafic en temps réel sur l'ensemble de votre infrastructure.

### Restauration à grande échelle avec les Services de protection des données Dell

Bien que la prévention soit essentielle, la récupération est un aspect tout aussi important de la préparation aux ransomwares. Dell l'a bien compris. Les Services de protection des données Dell fournissent non seulement des solutions automatisées de sauvegarde et de restauration, mais également des conseils d'experts pour garantir aux entreprises une reprise d'activité rapide et minimiser les interruptions de service. Les services de récupération des données à distance et de réponse aux incidents, par exemple, apportent aux entreprises le soutien dont elles ont besoin dans les moments de crise les plus critiques. Cette approche complète permet de préserver l'intégrité des données et de réduire les délais de reprise, pour éviter les interruptions opérationnelles.

Ce ne sont là que quelques exemples de solutions Dell qui peuvent vous aider à contrer les menaces internes malveillantes.

## Une force bâtie autour de partenariats

L'approche collaborative de Dell étend sa protection au-delà de ses technologies propriétaires. À travers ses partenariats avec des entreprises spécialisées dans la cybersécurité aussi réputées que CrowdStrike et SecureWorks, Dell propose un écosystème de solutions intégrées qui abordent tous les vecteurs d'attaque possibles. Ensemble, ces solutions offrent une couverture de sécurité de bout en bout, permettant aux entreprises de créer des défenses multicouches adaptées à leurs propres profils de risque.

## Pourquoi choisir Dell ?

Bien plus qu'un simple fournisseur de technologie, Dell Technologies est un partenaire de confiance dans la lutte contre les ransomwares. En combinant innovation, expertise et engagement à donner aux entreprises les moyens d'agir, Dell procure aux organisations les outils et la confiance dont elles ont besoin pour faire face aux menaces en constante évolution. Qu'il s'agisse de sécuriser les points de terminaison, de protéger les données critiques ou de se relever rapidement d'une attaque, les produits et services Dell garantissent la continuité opérationnelle et la tranquillité d'esprit.

## Construire un avenir tourné vers la résilience

Les attaques par ransomware ne cessent d'évoluer, mais avec Dell Technologies, les entreprises sont en mesure de garder une longueur d'avance. En utilisant du matériel, des logiciels et des services à la pointe de la technologie, les organisations ont les moyens de créer un cadre de cybersécurité à la fois résilient, adaptable et fiable. Sécurisez vos données, protégez vos opérations et pérennisez votre activité dès aujourd'hui grâce aux solutions complètes de Dell contre les ransomwares.

Pour garantir la résilience de votre entreprise, il est essentiel de comprendre le paysage actuel des menaces et de se tenir au fait des menaces émergentes. Les experts en cybersécurité de Dell Technologies surveillent en permanence les nouveaux vecteurs d'attaque (y compris ceux qui n'ont pas encore de nom) et s'efforcent de traiter de manière proactive les vulnérabilités potentielles de nos produits et services. Cette approche nous permet de vous apporter la protection la plus à jour contre les menaces de ransomware en constante évolution.

En plus de se tenir informées, les entreprises doivent également adopter une approche de sécurité à plusieurs niveaux. Cela implique de déployer tout un arsenal de mesures de sécurité, telles que des pare-feux, des logiciels de protection contre les programmes malveillants, des systèmes de détection des intrusions et des sauvegardes de données. En diversifiant vos stratégies de défense, vous pouvez minimiser l'impact d'une attaque et maintenir votre entreprise à flot même si une tentative de ransomware passe entre les mailles du filet.

Il est également important de tester et de mettre à jour régulièrement vos mesures de sécurité (appliquer des correctifs à vos systèmes et mettre à jour vos stratégies). Les pirates cherchent constamment de nouveaux moyens de contourner les mesures de sécurité traditionnelles. Il est donc essentiel que les entreprises conservent une longueur d'avance en testant régulièrement leurs défenses et en les mettant à jour si nécessaire. Cela suppose notamment d'entreprendre régulièrement des analyses de vulnérabilités, d'effectuer des tests de pénétration et de gérer les correctifs.

Pour protéger votre entreprise contre les ransomwares, vous devez également sensibiliser vos employés aux pratiques d'excellence en matière de cybersécurité. De nombreuses attaques par ransomware sont lancées via des tactiques d'ingénierie sociale, et notamment des e-mails de phishing ou des liens malveillants. En expliquant à vos employés comment détecter et éviter ces menaces, vous pouvez réduire considérablement les perspectives de réussite d'une attaque.

En outre, la mise en place d'un plan de reprise après sinistre peut considérablement atténuer l'impact d'une attaque par ransomware. Ce plan doit inclure des sauvegardes régulières des données et systèmes stratégiques, ainsi qu'une procédure claire pour répondre à une attaque et organiser la reprise d'activité.

En plus de ces mesures proactives, il est également important de mettre en place un plan solide de réponse aux incidents. Ce plan consiste notamment à définir clairement les rôles et les responsabilités associés à la gestion d'une attaque par ransomware, et à employer des protocoles de communication pour informer les parties prenantes et limiter les dommages.

Enfin, pour garder une longueur d'avance sur les menaces potentielles, il est important de se tenir informé des dernières tendances et des développements récents en matière d'attaques par ransomware. En examinant régulièrement les rapports rédigés par des professionnels du secteur et les mises à jour des experts de sécurité, vous pouvez mettre en œuvre de nouvelles mesures de sécurité en amont afin de protéger votre entreprise.

N'oubliez pas qu'aucune entreprise n'est à l'abri des attaques par ransomware ; cependant, en adoptant les bonnes stratégies et en déployant les outils appropriés, vous pouvez minimiser les risques et l'impact de telles attaques. En adoptant une approche proactive de la cybersécurité, vous ne faites pas que protéger votre entreprise : vous établissez également un climat de confiance avec vos clients et les parties prenantes.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **Dell.com/SecuritySolutions**

---

En savoir plus
sur les solutions Dell

Contacter un
expert Dell Technologies

Consulter d'autres
ressources

Prenez part à la discussion
avec #hashtag



DELL Technologies