Synology

Protégez votre entreprise contre les rançongiciels

On s'attend à ce que les attaques par rançongiciel coûtent un total de 8 milliards de dollars américains aux entreprises rien que pour l'année 2023[1]. Les plans de protection des données avec options de restauration rapide sont essentiels pour réduire l'impact des rançongiciels et autres formes de cybercriminalité.

Date 13 oct. 2023

Sauvegardes : la dernière ligne de défense en cas de sinistre

En cas de perte de données suite à une suppression ou à une modification malveillante, les sauvegardes vous permettent de restaurer des données critiques et d'éviter des interruptions de service coûteuses. Tirez parti des solutions de protection des données de Synology pour concevoir une stratégie de sauvegarde pour l'ensemble de votre infrastructure informatique.

Protection complète

Protégez les points de terminaison, ainsi que les sauvegardes principales pour créer plusieurs réseaux de sécurité pour vos données.

Restauration rapide

Réduisez au minimum les interruptions de service en cas de sinistre grâce aux options de restauration instantanée.

Stockage immuable

Empêchez toute modification non autorisée apportée aux données et aux instantanés.

Sauvegardes sans licence

Sauvegardez autant de données que votre stockage le permet, sans limitation ni frais cachés.

Protection centralisée contre les rançongiciels

Consolidez les sauvegardes des flottes de postes de travail, de serveurs, de machines virtuelles et d'applications cloud. Optimisez la consommation de stockage et évitez les goulots d'étranglement de la bande passante grâce à la déduplication des données et aux technologies de sauvegarde incrémentielle. https://www.synology.com/dsm/solution/infrastructure

Charges de travail physiques

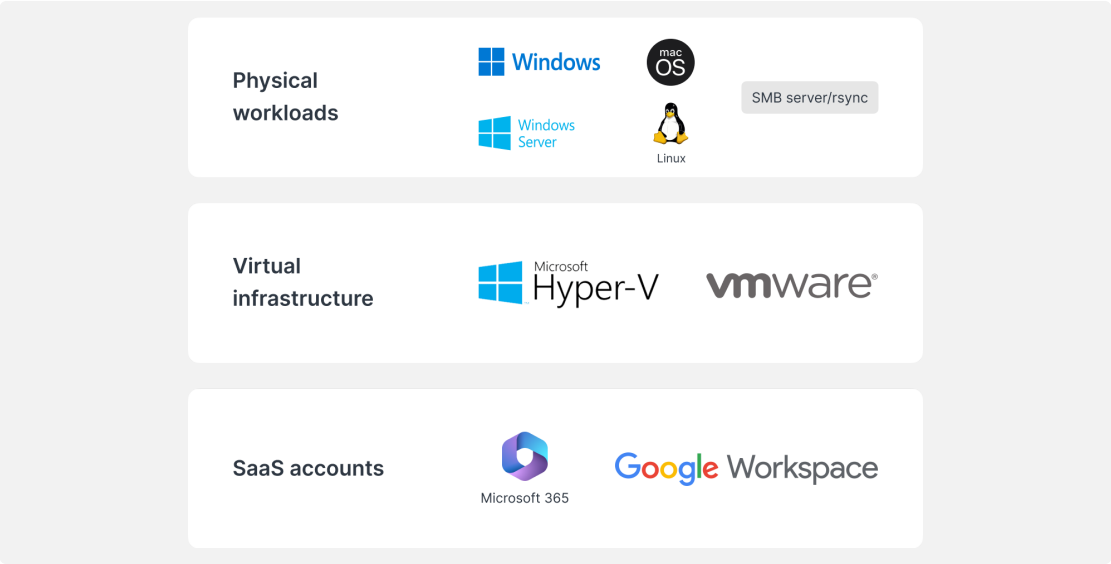
Protégez vos points de terminaison en cas d'attaques malveillantes grâce à une sauvegarde sans système d'exploitation complète et à une restauration flexible au niveau des fichiers.

Infrastructure virtuelle

Sauvegardez les machines virtuelles VMware® vSphere™, Microsoft® Hyper-V® et les LUN grâce à de puissantes technologies de réduction des données.

Comptes SaaS

Activez la protection continue des données stockées sur le cloud, avec détection automatique des nouveaux comptes ajoutés.



Restauration efficace

Réduisez les temps d'arrêt des systèmes de production critiques en restaurant rapidement les sauvegardes à partir d'un système Synology local ou hors site.

RTO proche de zéro

Montez des images de sauvegarde sur VMware®, Hyper-V® ou Synology Virtual Machine Manager pour reprendre le travail le plus rapidement possible. Restaurez les machines virtuelles sur un autre hyperviseur pour éviter toute interruption de service.

RPO minimal

Configurez la fréquence de sauvegarde en fonction de vos besoins, en réduisant la quantité de données potentiellement affectées lors d'une attaque. Protégez rapidement vos systèmes grâce aux sauvegardes incrémentielles et à la technologie de déduplication.

Fonctionnement intuitif

Laissez les employés parcourir et prévisualiser les e-mails, les contacts et les fichiers depuis un portail pratique avant de les restaurer, offrant ainsi une expérience plus conviviale et réduisant la charge de travail des équipes informatiques.

Ajoutez une couche de protection supplémentaire

Respectez la stratégie de sauvegarde 3-2-1 en stockant un troisième ensemble de données hors site ou dans le cloud, protégeant ainsi vos données contre les incendies, les catastrophes naturelles ou le vol.

Sur des serveurs hors site

Stockez vos sauvegardes sur un serveur Synology se trouvant sur un site secondaire pour vous protéger contre les catastrophes physiques et répliquez les instantanés immuables pour une protection supplémentaire contre les rançongiciels.

Sur le cloud

Sauvegardez vos données auprès de n'importe quel fournisseur de stockage dans le cloud, en les protégeant contre tout accès non autorisé grâce au chiffrement AES-256 côté client. https://c2.synology.com/storage/nas

Fiable dans différents secteurs

« Synology [...] nous a permis de réduire nos dépenses en matériel pour notre serveur [...], tout en simplifiant considérablement les sauvegardes d'infrastructure et de postes de travail, la journalisation du système et la gestion des fichiers. »
https://www.synology.com/company/case_study/Investortools

« Grâce à Active Backup for Business, toutes nos sauvegardes sont désormais centralisées et disponibles 24 h/24 et 7 j/7, ce qui nous permet de réduire les interruptions de service et de rester en conformité avec les réglementations FERPA. »
https://www.synology.com/company/case_study/University_of_Washington

« [...] Active Backup for Business dispose de vitesses de sauvegarde étonnantes et fonctionne à merveille pour supprimer les données en double : il n'occupe que 28 To sur les 58 To du serveur. [...] »
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

« [...] Active Backup for Business nous permet de centraliser et de gérer toutes les tâches de sauvegarde à partir d'une seule console. La restauration rapide et fiable garantit également la continuité des opérations. »
https://www.synology.com/company/case_study/UNESCO

Foire aux questions

Qu'est-ce qu'un rançongiciel ?

Le rançongiciel est un type de logiciel malveillant qui crypte les fichiers des victimes. Les attaquants demandent ensuite une rançon pour restaurer l'accès aux données, menaçant souvent de détruire définitivement les données si aucune rançon n'est versée. Les attaques par rançongiciel peuvent être dévastatrices et peuvent entraîner des pertes financières importantes pour les individus et les organisations. Il est important de vous protéger, vous et vos appareils, contre les rançongiciels, par exemple en maintenant vos logiciels à jour et en sauvegardant régulièrement vos fichiers.

Quels types de rançongiciels existe-t-il ?

Il existe de nombreux types de rançongiciels et de nouvelles versions sont constamment développées. Voici quelques-uns des types de rançongiciels les plus courants :

- **Rançongiciel de chiffrement** : le type de rançongiciel le plus courant chiffre les fichiers de la victime afin qu'elle ne puisse pas y accéder sans la clé de déchiffrement. Les attaquants demandent ensuite le paiement d'une rançon en échange de la clé
- **Rançongiciel verrouilleur d'ordinateur** : un type de rançongiciel qui empêche aux victimes d'accéder à leur ordinateur en modifiant leurs identifiants de connexion ou en affichant un message qui les empêche d'accéder à leur système. Les attaquants demandent ensuite le paiement d'une rançon pour déverrouiller l'ordinateur
- **Rançongiciel-as-a-Service (RaaS)** : un modèle commercial dans lequel les attaquants proposent des rançongiciels à d'autres individus ou groupes qui souhaitent perpétrer des attaques. Les attaquants fournissent généralement le rançongiciel et gèrent les paiements, tandis que l'acquéreur reçoit un pourcentage des paiements de rançon
- **Scareware** : des rançongiciels conçus pour faire peur aux victimes et les pousser à payer la rançon. Il s'agit généralement d'afficher de faux avertissements de sécurité ou de faux messages qui prétendent que l'ordinateur de la victime est infecté par un virus. L'attaquant exigera ensuite une rançon pour éliminer l'infection supposée

Comment les rançongiciels se propagent-ils ?

Les rançongiciels se propagent généralement par le biais d'e-mails d'hameçonnage ou en exploitant les vulnérabilités d'un système informatique. Lors d'une attaque d'hameçonnage, un attaquant envoie un e-mail qui semble provenir d'une source légitime, telle qu'une banque ou une entreprise connue. L'e-mail contient souvent un lien ou une pièce jointe qui, lorsque vous cliquez dessus, installe le rançongiciel sur l'ordinateur de la victime. L'exploitation des vulnérabilités dans un système est similaire, sauf que l'attaquant utilisera un défaut de sécurité du système pour installer le rançongiciel sans que la victime en ait connaissance. Dans les deux cas, une fois le rançongiciel installé, il peut rapidement se propager à d'autres ordinateurs sur le même réseau.

Quel est le processus type d'une attaque par rançongiciel ?

Le processus d'une attaque par rançongiciel suit généralement les étapes suivantes :

1. L'attaquant accède à l'ordinateur d'une victime, soit en envoyant un e-mail d'hameçonnage, soit en exploitant une vulnérabilité dans le système
2. Une fois que l'attaquant a accès à l'ordinateur de la victime, il installera le rançongiciel sur le système
3. Le rançongiciel chiffrera ensuite les fichiers de la victime, ce qui les rendra inaccessibles à l'utilisateur
4. L'attaquant exigera ensuite une rançon de la part de la victime, généralement sous forme de monnaie numérique comme le bitcoin, en échange de la clé de déchiffrement qui déverrouillera les fichiers chiffrés
5. Si la victime paie la rançon, l'attaquant fournira la clé de déchiffrement et la victime pourra à nouveau accéder à ses fichiers. Cependant, il n'y a aucune garantie que l'attaquant fournira réellement la clé et, même si c'est le cas, les fichiers de la victime peuvent être endommagés ou corrompus à la suite du processus de chiffrement

Il est important de noter qu'il existe de nombreuses variations dans ce processus, et que toutes les attaques par rançongiciel ne suivront pas exactement ces étapes. Certaines attaques peuvent ne pas impliquer le chiffrement des fichiers, par exemple, tandis que d'autres peuvent impliquer d'autres formes d'extorsion ou de chantage.

Comment tomber sur un rançongiciel ?

Il existe plusieurs façons de tomber sur un rançongiciel. L'une des méthodes les plus courantes consiste à cliquer sur un lien malveillant ou une pièce jointe dans un e-mail d'hameçonnage. Ce type d'e-mail est conçu pour sembler légitime et semble souvent provenir d'une entreprise ou d'une organisation connue. Lorsque vous cliquez sur le lien ou la pièce jointe, le rançongiciel s'installe sur votre ordinateur. Vous pouvez également tomber sur un rançongiciel en consultant un site Web compromis. Ces sites Web ont été piratés par des attaquants qui ont inséré du code qui installera automatiquement le rançongiciel sur votre ordinateur si vous consultez le site. Vous pouvez également obtenir un rançongiciel en téléchargeant des fichiers infectés depuis Internet. Cela peut se produire si vous téléchargez un fichier à partir d'un site Web suspect ou si vous téléchargez un fichier qui a été partagé par une personne que vous ne connaissez pas. En résumé, il est important de faire preuve de prudence lorsque vous naviguez sur Internet et d'éviter de cliquer sur des liens ou de télécharger des fichiers à partir de sources inconnues. Cela peut vous aider à vous protéger contre les rançongiciels et autres types de programmes malveillants.

Qui sont les cibles des rançongiciels ?

Les attaques par rançongiciel peuvent cibler toute personne utilisant un ordinateur ou un autre périphérique connecté à Internet. Cependant, certains groupes sont plus susceptibles d'être ciblés que d'autres. Par exemple, les attaques par rançongiciel ciblent souvent les entreprises, car elles disposent souvent de données plus précieuses et sont plus disposées à payer une rançon pour les récupérer. Les hôpitaux, les écoles et autres organisations qui fournissent des services essentiels sont également des cibles courantes, car une attaque par rançongiciel peut perturber leurs opérations et mettre en danger la vie des gens. Les individus peuvent également être la cible d'attaques par rançongiciel. Dans ce cas, les attaquants peuvent tenter d'extorquer de l'argent à la victime en menaçant de supprimer ses fichiers personnels ou de publier des informations sensibles, sauf si une rançon est versée. Les cibles des attaques par rançongiciel sont souvent choisies en fonction de la valeur de leurs données et de leur volonté de payer une rançon pour les récupérer.

Quels sont les risques liés au paiement d'un rançongiciel ?

Payer une rançon à un rançongiciel malveillant peut sembler le moyen le plus simple de récupérer vos fichiers, mais cela peut en fait être une décision très risquée. Le paiement d'une rançon comporte plusieurs risques, notamment :

- Rien ne garantit que l'attaquant fournira réellement la clé de déchiffrement. Dans de nombreux cas, les victimes qui paient la rançon ne reçoivent jamais la clé et restent dans l'incapacité d'accéder à leurs fichiers
- Payer la rançon peut encourager les attaquants à poursuivre leur campagne d'attaques. Si les attaquants savent que leurs victimes sont prêtes à payer la rançon, ils sont plus susceptibles de perpétrer davantage d'attaques à l'avenir
- Payer la rançon peut faire de vous une cible pour de futures attaques. Si l'attaquant sait que vous êtes prêt à payer une rançon, vous serez peut-être plus susceptible d'être sa cible à l'avenir
- Payer la rançon peut être illégal. Dans certains cas, le paiement d'une rançon à une organisation criminelle peut être considéré comme une forme de financement du terrorisme ou d'autres activités illégales

Bien que le paiement de la rançon puisse sembler le moyen le plus simple de récupérer vos fichiers, il peut s'agir d'une décision très risquée. Il est important d'examiner attentivement les risques avant de prendre une décision.

Quels sont les coûts des rançongiciels ?

Le coût d'une attaque par rançongiciel peut varier considérablement en fonction d'un certain nombre de facteurs, tels que le type de rançongiciel utilisé, le nombre de fichiers chiffrés et l'efficacité de l'attaque. Dans certains cas, le coût d'une attaque par rançongiciel peut être relativement faible, les attaquants exigeant quelques centaines de dollars de rançon. Dans d'autres cas, le coût peut être beaucoup plus élevé, les attaquants exigeant des milliers de dollars, voire plus, pour restaurer l'accès aux fichiers de la victime. Outre les coûts directs associés au paiement d'une rançon, les attaques par rançongiciel peuvent également avoir des coûts indirects importants. Par exemple, une attaque par rançongiciel peut entraîner des temps d'arrêt et une perte de productivité, ce qui peut entraîner une perte de revenus. Cela peut également nuire à la réputation d'une entreprise et à la confiance des clients, ce qui peut avoir des effets négatifs sur l'activité à long terme. Ces coûts indirects sont souvent bien plus élevés que la rançon elle-même.

Quels sont les symptômes des rançongiciels ?

Les symptômes d'une attaque par rançongiciel peuvent varier en fonction du type spécifique de rançongiciel utilisé. Cependant, voici certains symptômes courants :

- Vos fichiers sont chiffrés et vous ne pouvez pas y accéder
- Vous recevez un message de l'attaquant demandant le paiement d'une rançon en échange de la clé de déchiffrement
- Vous voyez des programmes ou processus inconnus s'exécuter sur votre ordinateur
- Votre ordinateur ralentit ou ne répond plus
- Votre ordinateur affiche des messages d'erreur ou des fenêtres contextuelles inhabituels

Si vous pensez que votre ordinateur a été infecté par un rançongiciel, il est important d'agir rapidement. Déconnectez votre ordinateur d'Internet pour empêcher la propagation du rançongiciel.

Comment empêcher les attaques par rançongiciel ?

Vous pouvez prendre plusieurs mesures pour éviter les attaques par rançongiciel, notamment :

- Utilisez un logiciel antivirus ou de sécurité fiable et maintenez-le à jour. Cela peut vous aider à protéger votre ordinateur contre les rançongiciels et autres types de programmes malveillants
- Soyez prudent lorsque vous ouvrez des pièces jointes ou des liens dans un e-mail. Les rançongiciels sont souvent envoyés par e-mails d'hameçonnage. Il est donc important de faire attention à ce sur quoi vous cliquez.
- Maintenez votre système d'exploitation et les autres logiciels à jour. Les mises à jour logicielles incluent souvent des correctifs de sécurité qui peuvent vous aider à protéger votre ordinateur contre les rançongiciels et autres menaces
- Sauvegardez régulièrement vos fichiers. Cela peut vous aider à protéger vos données si votre ordinateur est infecté par un rançongiciel. Assurez-vous de respecter l'une des stratégies de sauvegarde recommandées, comme la stratégie de sauvegarde 3-2-1
- Soyez conscient des risques liés aux rançongiciels et informez les autres membres de votre entreprise de ces menaces. Cela peut aider à prévenir les attaques par rançongiciel, à les détecter et à y répondre plus facilement si elles se produisent.

La meilleure façon de prévenir les attaques par rançongiciel est de rester vigilant et de prendre des mesures pour protéger votre ordinateur et vos données. Cela peut contribuer à réduire le risque d'attaque par rançongiciel et à faciliter la récupération après une attaque, le cas échéant.

Comment Synology peut-il me protéger contre les rançongiciels ?

Il est essentiel de prendre des mesures préventives pour éviter de subir des attaques par rançongiciel. Utilisez ces solutions Synology en plus du logiciel antivirus que vous avez choisi :

- **Empêchez l'accès** : limitez la propagation des rançongiciels en définissant des autorisations de fichier, d'application et d'accès, et configurez des identifiants de connexion sécurisés à l'aide de Secure SignIn et de C2 Password.
- **Protégez les périphériques** : les systèmes obsolètes sont plus exposés. Mettez tous vos NAS à jour en même temps grâce à Synology Central Management System (CMS) et protégez les autres périphériques à l'aide de stratégies de groupe dans Synology Directory Server et C2 Identity
- **Évitez les fichiers suspects** : les spams et les e-mails d'hameçonnage contenant des fichiers suspects font partie des méthodes les plus couramment employées par les rançongiciels. Synology MailPlus offre une protection efficace contre les programmes malveillants et une prévention contre les courriers indésirables
- **Identifiez les vulnérabilités** : utilisez Synology Security Advisor pour effectuer des analyses de routine permettant de détecter les programmes malveillants, les vulnérabilités et les activités de connexion anormales. Mettez en œuvre les modifications recommandées pour améliorer la sécurité de votre NAS.
  https://www.synology.com/dsm/overview/security

Méthodes supplémentaires pour protéger vos données

Gérez votre flotte

Tirez parti de fonctionnalités étendues pour gérer de manière centralisée les autorisations d'accès aux données, l'état des logiciels, l'intégrité du système, etc.
https://www.synology.com/dsm/overview/administration

Surveillez tous vos systèmes

Identifiez les activités de connexion suspectes, gérez les mises à jour et surveillez l'intégrité des périphériques, quel que soit l'emplacement de vos périphériques.
https://www.synology.com/dsm/feature/active-insight

Protégez vos données

Suivez la règle de sauvegarde 3-2-1 pour protéger vos données contre toute modification ou suppression accidentelle ou malveillante.
https://www.synology.com/dsm/solution/data_backup

Commencer

Nous contacter

Contactez l'équipe commerciale régionale pour plus d'informations.
https://www.synology.com/form/inquiry/sales

Où acheter

Trouvez un partenaire Synology dans votre région
https://www.synology.com/wheretobuy

Remarques:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Protégez votre entreprise contre les rançongiciels

https://www.synology.com/fr-fr/dsm/solution/ransomware

Site web de Synology

https://www.synology.com/

Nous contacter

https://www.synology.com/company/contact_us