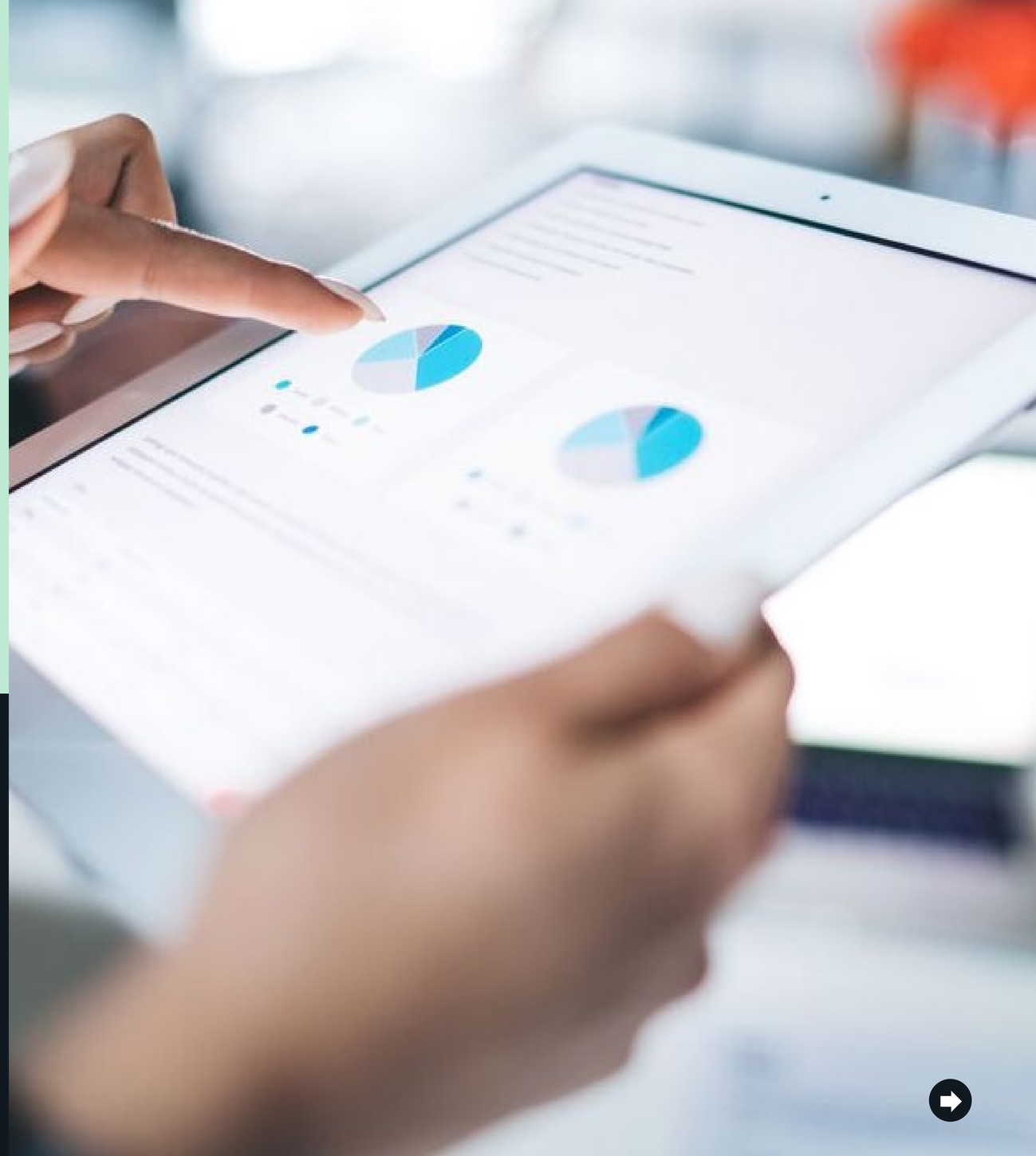
eBOOK

Cyberrésilience : protégez vos données de l'intérieur

NetApp



Overview

Voyage au centre du service IT

Imaginez que vous sortez faire vos courses de la semaine. Vous prenez vos sacs à provisions, vos clés, puis, juste avant de monter dans votre voiture, vous avalez une grosse pilule argentée, votre pilule de super-résistance.

Voilà, maintenant vous pouvez conduire en toute sécurité, car votre corps aura la capacité surhumaine de supporter n'importe quel risque sur le chemin du magasin.

Si l'on pouvait prendre de telles pilules magiques, construire des maisons avec des briques qui éjectent les intrus ou acheter des bijoux qui s'échappent seuls des mains des voleurs, nous n'aurions pas besoin de ceintures de sécurité, de serrures, ni de systèmes d'alarme.

Nouvelle approche de la cybersécurité

Ces protections magiques n'existent peut-être pas dans le monde réel, mais elles commencent à apparaître dans le monde virtuel. Elles convergent avec les équipements de protection existants. Depuis plusieurs dizaines d'années, les professionnels de l'IT utilisent une approche de la cybersécurité de type « ceintures de sécurité et systèmes d'alarme », car c'était la seule disponible.

Aujourd'hui, il existe une approche plus intelligente : ***la cyberrésilience***.

La cyberrésilience associe la protection des données à la sécurité IT classique pour permettre aux entreprises de rebondir suite à une cyberattaque. Même si un intrus franchit le périmètre ou que quelqu'un de l'intérieur commet une action malveillante, les données sont couvertes, car elles bénéficient d'une protection intégrée et non d'une protection après coup.

Pourquoi est-ce important ?
Les mesures de cybersécurité qui adoptent une approche « château et douves » ne suivent pas le rythme de l'évolution constante des tactiques criminelles. Aujourd'hui :

La plupart des stratégies de sécurité consistent à arrêter l'ennemi devant l'entrée principale en fortifiant le périmètre.

Les entreprises ne défendent pas qu'une seule porte. Elles sont responsables de centaines d'entre elles, en raison de la prolifération des terminaux, des politiques de « bring-your-own-device » et de l'essor du télétravail.

Il est désormais plus facile pour les hackers d'infiltrer les entreprises trop submergées pour surveiller en profondeur leurs environnements réseau complexes.

En outre, de nombreuses entreprises oublient que l'objectif n'est pas d'empêcher les intrusions, L'objectif principal est de protéger les ressources les plus précieuses : **vos données**.

Cyberrésilience *nom*

cy·ber ré·si·lience

La capacité d'anticiper, de résister, de se rétablir et de s'adapter à des conditions défavorables, des contraintes, des attaques ou des compromissions qui utilisent ou sont rendues possibles par des cyberressources[1].

Votre stratégie de cyberrésilience commence-t-elle par ce qui compte le plus?

Si les menaces sont partout, par où commencer ?

La stratégie consiste d'abord à organiser la sécurité et la protection autour de vos données, et à en faire des éléments clés de votre plan de cyberrésilience. Dans le paysage moderne des menaces :

- Le **nombre de ransomware a augmenté de 62 % à travers le monde**[2] et le nombre de familles de ransomware de 3,4 %[3]. Ceci est la preuve que les hackers ont réalisé des progrès en matière de prise en otage des données.
- **Environ un tiers des organisations finissent par payer** pour récupérer leurs données chiffrées après avoir subi une attaque par ransomware[4].
- **Le coût moyen pour faire face à une attaque par ransomware en 2021 était de 1,85 million de dollars US**, contre 768 106 dollars US en 2020[5].
- **Les attaques par ransomware à double extorsion sont en hausse.** Ainsi, les entreprises risquent non seulement de perdre leurs données, mais aussi de les voir divulguées au public[6].

Les enjeux sont plus élevés que jamais, et les attaques par ransomware sont devenues une réalité de l'informatique moderne.

Alors n'est-il rien que vous puissiez faire pour vous prémunir efficacement ? Si. Vous pouvez cesser de craindre les ransomware et **activer la cyberrésilience** de l'entreprise en adoptant une approche de la cybersécurité axée sur les données.

Cette approche implique de poser les bases de votre sécurité au plus près des données, plutôt qu'au périmètre.

Tracez votre chemin vers une plus grande cyberrésilience

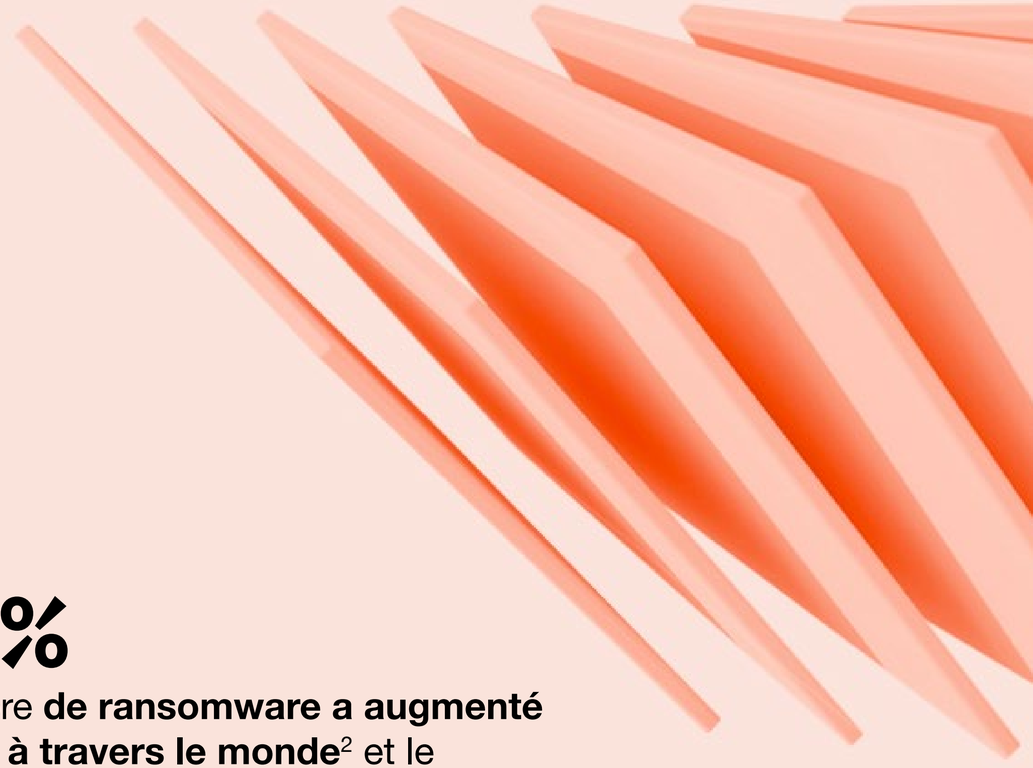
Si vous souhaitez accéder au cœur de votre service IT pour protéger vos données, cela demande quelques efforts. Heureusement, vous n'êtes pas le premier à vous y aventurer et vos prédécesseurs vous ont laissé quelques points de repère utiles :

Identifier **Protéger** **Détecter**

Réagir **Restaurer**

Même si ces jalons sont utiles, la mise en place d'un plan de cyberrésilience complet reste complexe et coûteuse. Votre équipe doit jongler avec des ressources limitées, combler le manque de compétences, respecter les exigences réglementaires, sachant qu'elle n'est pas la seule à avoir des revendications dans l'entreprise[7]. Au vu des efforts qu'elle demande, la cyberrésilience a malheureusement tendance à finir aux oubliettes.

Voici comment aborder chaque étape.



62 %

Le nombre **de ransomware a augmenté de 62 % à travers le monde**[2] et le nombre de familles de ransomware de **3,4 %**[3]. Ceci est la preuve que les hackers ont réalisé des progrès en matière de prise en otage des données.

Identifier :
faites le point sur votre environnement

Identifiez les éléments à protéger et classez-les par ordre d'importance.
Les questions à considérer sont les suivantes :

Savez-vous où résident vos données et quels types de données existent dans votre environnement ?

Pour chaque type de données, sont-elles sensibles et qui a les autorisations d'accès ?

Quels systèmes sont essentiels au maintien des opérations commerciales ?

Quel rôle joue chaque technologie dans vos opérations commerciales, et comment pourrait-elle être exploitée par un acteur malveillant ?

Les flux d'informations sont-ils documentés ?

Comment les rôles et les responsabilités liés aux activités de cybersécurité sont-ils attribués ?

Quel est votre plan pour l'identification des menaces et la gestion des risques ?[7]

Quelles sont vos solutions actuelles de protection et de sécurité des données ?

En d'autres termes, vous devrez évaluer votre système actuel de protection et de sécurité des données. Vous devrez également classer les différents types de données, déterminer leur emplacement et évaluer leurs autorisations.

Défis associés à l'étape d'identification
L'étape d'identification prend beaucoup de temps. Or, les responsables IT ont déjà beaucoup de pain sur la planche, notamment à cause de la gestion quotidienne de l'infrastructure et des données. L'inventaire d'une infrastructure IT complète, surtout si vous n'avez pas d'outils d'automatisation, peut vite devenir chronophage.

En l'absence d'un plan spécifique ou de protocoles de classification normalisés, vous risquez de créer un ensemble de données encore plus confus que vos équipes auront du mal à déchiffrer et à utiliser.

Protéger : dressez vos défenses

L'étape de protection consiste à « se murer ».

Chiffrez vos données, effectuez des sauvegardes régulières, assurez le contrôle des accès, mettez en œuvre des défenses du périmètre, mettez à jour les systèmes d'exploitation et les applications vulnérables et formez les utilisateurs aux bonnes pratiques en matière de cybersécurité[7].

Cette étape vise à bloquer les utilisateurs malveillants, à mettre en quarantaine les données potentiellement corrompues, à empêcher l'ajout de données sur un disque, à créer des copies granulaires immuables impossibles à infecter et à empêcher la suppression de données grâce à des sauvegardes indélébiles.

Défis associés à l'étape de protection
L'étape de protection reflète certains changements récents dans l'approche de la cybersécurité. Bien que les entreprises utilisent des pare-feu et des capteurs d'intrusion réseau depuis des décennies pour protéger leurs environnements IT, la prolifération des données met à mal ces stratégies. Les équipes informatiques doivent répondre à des questions difficiles comme :

- Comment chiffrer de grandes quantités de données générées trop rapidement pour être inventoriées ?
- Comment assurer le contrôle des accès sans nuire gravement à l'expérience de l'utilisateur et entraîner une chute de la productivité ou encourager les solutions de contournement dangereuses ?
- Comment être sûr que votre environnement tout entier est protégé, étant donné le nombre d'angles morts que vous avez découverts ?
- Quels tests réguliers effectuez-vous sur vos technologies de protection des données pour vous assurer qu'en cas de menace, vous pouvez récupérer vos données avec succès ?

Détecter : gardez une longueur d'avance

Il vaut mieux prévenir que guérir. Mettez en place des systèmes qui identifient les activités suspectes avant qu'elles ne se muent en véritables menaces, par exemple :

- Des processus de détection à jour
- Des journaux surveillés régulièrement afin de détecter et bloquer les activités anormales
- Une compréhension approfondie des flux de données réguliers afin de repérer les activités inhabituelles qui pourraient être des tentatives de vol de données
- La capacité non seulement de détecter, mais aussi de mesurer l'impact d'une violation[7]

En d'autres termes, vous devez surveiller le comportement des utilisateurs pour détecter toute activité suspecte et repérer les anomalies dans le comportement des données.

Défis associés à l'étape de détection

Gérer la surcharge d'alertes : le défi majeur lié à l'étape de détection reste sans doute le filtrage du bruit. Les équipes de cybersécurité et les centres de supervision et d'administration de la sécurité (SOC) sont submergés d'alertes de menaces, qu'ils doivent souvent traiter manuellement.

Automatiser le tri des menaces : ils ont besoin d'un moyen d'analyser et d'écarter automatiquement les fausses alertes et les problèmes les moins importants afin de consacrer leur attention sur les cas les plus difficiles.

Augmenter la vitesse de détection : les équipes de cybersécurité ont également besoin d'un moyen d'accélérer la détection de ces menaces afin de réagir avant qu'elles ne causent des dommages graves. Il faut notamment qu'elles soient immédiatement averties en cas d'accès non autorisé à l'aide d'informations d'identification compromises pour empêcher tout intrus de chiffrer d'importantes quantités de données.

Réagir :
soyez prêt à agir en cas de crise

Les menaces évoluent en parallèle des mesures de sécurité. Par conséquent, il est important de mettre régulièrement vos plans à l'épreuve en trois étapes :

1

Tous les membres de l'équipe doivent connaître leurs responsabilités : y compris les bonnes pratiques générales en matière de cybersécurité et leur rôle spécifique en cas d'urgence.

2

Mettez à jour vos plans de défense pour vous adapter à l'évolution des menaces, notamment en appliquant les enseignements tirés des attaques précédentes.

3

Partagez toutes les mises à jour de vos plans avec les autres parties prenantes, tant internes qu'externes, afin que vos actions restent cohérentes en cas d'attaque[7].

Défis associés à l'étape de réaction
Pour réagir efficacement, vous devez disposer d'une vue d'ensemble de vos systèmes qui vous permet de visualiser l'emplacement de vos données, de surveiller le type d'activité qui se produit dans votre environnement et de mettre à jour vos plans en conséquence.

Encore une fois, il s'agit d'une activité chronophage pour les entreprises qui croulent déjà sous les tâches quotidiennes de gestion de l'infrastructure et des données.

En outre, pour être efficace, un plan de réponse doit s'exécuter plus rapidement qu'un plan d'action manuel, même très bien préparé. Les équipes de cybersécurité ont besoin d'outils automatisés qui suivent immédiatement des étapes prédéfinies, comme la prise d'une Snapshot, dès que le système détecte une activité suspecte.

Restaurer :
reprenez votre activité normale en un rien de temps

Si une cyberattaque interrompt vos opérations métier, vous devez être en mesure de reprendre rapidement votre activité normale. Il est impératif de savoir :

- Quelles informations faut-il partager ?
- Qui a besoin de ces informations ?
- Comment s'assurer que ces parties prenantes obtiennent les informations dont elles ont besoin à temps ?
- Comment allez-vous communiquer la violation au public, en informant les personnes dont les informations pourraient avoir été compromises ?
- Quelles mesures doivent être prises pour communiquer avec les organismes de réglementation ?

Au cours de la phase de restauration, vous devrez réduire les interruptions et restaurer les données rapidement, remettre en ligne les applications non compromises et réaliser des analyses de sécurité intelligentes pour identifier la source de l'attaque.

Défis associés à l'étape de récupération
À la suite d'une attaque, l'identification et l'évaluation des dégâts peuvent prendre beaucoup de temps. Or, vous aurez besoin de ces informations rapidement pour gérer à la fois votre plan d'action interne et les communications externes[7].

La solution de cyberrésilience de NetApp® prend en charge les cinq parties de votre plan de cyberrésilience, à savoir l'identification, la protection, la détection, la réaction et la restauration. Malheureusement, de nombreuses entreprises ont investi dans un ensemble d'outils de cybersécurité disparates et peuvent difficilement passer à un autre fournisseur.

Avec NetApp, pas besoin de tout remplacer. Vous pouvez adopter notre solution anti-ransomware soit toute seule, pour protéger toute votre entreprise, soit en complément d'autres outils en place.

Construisez une approche moderne de la cyberrésilience de l'intérieur vers l'extérieur

Jetons un coup d'œil plus approfondi à la mise en place d'une approche moderne de la cyberrésilience pour votre entreprise, y compris les solutions qui peuvent relever les défis communs soulignés ci-dessus. Les approches de cyberrésilience NetApp abordent ces défis de l'intérieur en offrant des solutions de sécurité et de protection conçues autour de vos données.

Le portefeuille de solutions de NetApp comprend une gestion des données puissante et robuste, une surveillance intelligente des données et des utilisateurs, ainsi que des services professionnels pour aider les entreprises à tous les stades de leur préparation et de leur gestion.

En donnant la priorité à vos données, il devient plus facile de répondre à vos besoins en matière de cyberrésilience. La première étape consiste à comprendre votre situation actuelle. Pour ce faire, répondez aux questions suivantes.

Il vaut mieux prévenir que guérir. Mettez en place des systèmes qui identifient les activités suspectes avant qu'elles ne se muent en véritables menaces, par exemple :

- Où se trouvent mes données ? dans le cloud, Sur site ? à la périphérie du réseau. Dans plusieurs régions ?
- Quels types de données ai-je ?
- Quels types d'autorisations mes données possèdent-elles ?
- Comment puis-je identifier et bloquer rapidement les activités malveillantes ?
- Comment puis-je m'assurer que toutes mes données sont en sécurité pendant que je détermine le rayon d'impact d'une attaque ?
- Comment puis-je restaurer mes données et applications en quelques minutes seulement après une attaque ?
- Comment puis-je enquêter sur la source d'une menace afin de disposer des informations nécessaires à contrer les futures tentatives similaires ?
- Comment puis-je intégrer la protection directement à l'intérieur ou autour de mes données afin qu'elles puissent « se défendre » rapidement, tout en identifiant et en bloquant la menace ? Comment puis-je surveiller le comportement des utilisateurs et détecter les activités suspectes sur mon réseau mondial ?

En répondant à toutes ces questions, vous allez créer le squelette d'un plan de cyberrésilience axé sur les données grâce auquel votre entreprise se préparera aux attaques par ransomware.

Si vous êtes inquiet parce que vous avez répondu « Je ne sais pas » à plusieurs questions, sachez que NetApp offre des services professionnels qui vous donnent non seulement des réponses, mais aussi les outils pour exécuter votre nouveau plan de protection contre les ransomware et de restauration.

Un plan de cyberrésilience en action avec NetApp

NetApp propose un portefeuille de solutions conçues pour répondre aux besoins des équipes informatiques et de sécurité afin de mieux protéger et sécuriser les données. Sur la base du logiciel de gestion du stockage ONTAP®, nous superposons des services de données pour améliorer la visibilité, détecter les menaces et automatiser la réponse et la restauration.

Continuez votre lecture pour découvrir la manière dont NetApp ainsi qu'un plan de cyberrésilience basé sur les réponses que vous venez de donner peuvent aider votre équipe à déjouer une attaque par ransomware.

« Nous avons récemment été confrontés à une attaque par ransomware. Quand nous avons eu connaissance de la fonctionnalité de détection Cloud Insights, nous avons tout de suite été convaincus. »

Directeur IT, entreprise de transport

Identifier

Votre équipe doit savoir quel type de données vous possédez, si elles sont sensibles et où elles se trouvent, afin de mieux planifier ce que vous allez protéger et comment. NetApp Cloud Data Sense, une solution SaaS, utilise des algorithmes d'intelligence artificielle (IA) pour la détection, le mappage et la classification des données afin de fournir ces informations.

Pendant ce temps, votre équipe peut exploiter NetApp Cloud Insights, qui offre une visibilité sur toute l'infrastructure de cloud hybride, pour surveiller et sécuriser l'ensemble de votre environnement. Heureusement, car vos défenses sont sur le point d'être mises à l'épreuve...

Protéger

Un matin, votre équipe IT basée à New York arrive au travail et apprend qu'un collègue du bureau de Londres a cliqué sur un lien dans un e-mail frauduleux.

Personne sur place n'a pu réagir directement à l'attaque, mais grâce à la protection des données « zéro confiance » de NetApp FPolicy®, un composant du logiciel de gestion des données NetApp ONTAP, les extensions de fichiers malveillants connues ont été bloquées.

Néanmoins, les hackers insistent. Ils exploitent un compte utilisateur compromis pour infecter des fichiers par le biais d'un malware zero-day. Celui-ci se propage sur d'autres comptes utilisateur compromis et se met à chiffrer des données, lentement, en se faisant discret.

Détecter et répondre

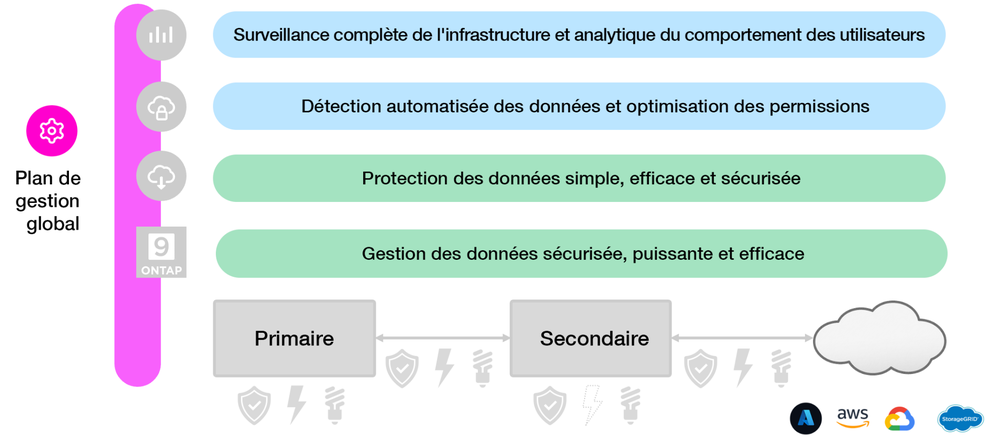
Difficile pour une poignée d'individus de repérer et d'éliminer toutes ces activités malveillantes, surtout s'ils jonglent avec d'autres responsabilités dans plusieurs fuseaux horaires. Heureusement, vous disposez de NetApp Cloud Insights pour surveiller les partages de fichiers en réseau et détecter les comportements anormaux des utilisateurs. Alors même si votre équipe ne remarque pas l'attaque, celle-ci ne peut pas échapper à la vigilance de Cloud Insights qui crée instantanément une copie NetApp Snapshot™ pour protéger les données.

Votre volume primaire est vulnérable au chiffrement, mais vos copies Snapshot sont immuables et, lorsqu'elles sont associées à NetApp Cloud Backup, elles constituent une stratégie de protection des données sûre et efficace.

Cloud Insights peut identifier la source de l'attaque et bloquer automatiquement le compte utilisateur compromis pour éviter d'autres dommages et aider à prévenir l'exfiltration de données.

Et qu'en est-il du malware qui progresse lentement dans votre stockage de fichiers ? Aucun problème. Votre équipe reçoit une alerte du système de protection anti- ransomware autonome intégré avec ONTAP, qui utilise le machine learning pour contrôler l'activité des workloads et l'entropie des données. Cette alerte déclenche également une copie Snapshot automatique, fournissant plusieurs points de restauration.

Les escroqueries par hameçonnage et les pièces jointes aux courriels ne sont pas les seules menaces. Des informations d'identification d'administration compromises, ou pire encore un administrateur véreux, peuvent mettre vos données en grand danger. NetApp ONTAP peut empêcher un seul compte d'administrateur de causer des dommages en exigeant que plus d'un compte d'administrateur approuve des tâches clés, telles que la suppression de copies Snapshot à l'aide de la nouvelle fonction de vérification multiadministrateur.



Restauration

Avec Cloud Data Sense et Cloud Insights, vous pouvez appliquer une analyse intelligente des fichiers pour identifier quelles données ont été touchées et par qui afin de cibler votre restauration de données et de réduire les interruptions.

Votre équipe IT peut ensuite restaurer des téraoctets de données en quelques minutes seulement à l'aide des outils NetApp. Les journaux peuvent être exportés vers les principaux logiciels de gestion des informations et des événements de sécurité (SIEM) pour une analyse plus approfondie.

Et malgré l'intensité dramatique du moment, toute l'équipe peut avoir l'esprit tranquille car la récupération des données n'a jamais été remise en question. En effet, le logiciel NetApp SnapLock® utilise un verrouillage sécurisé des fichiers WORM pour empêcher la suppression des données.

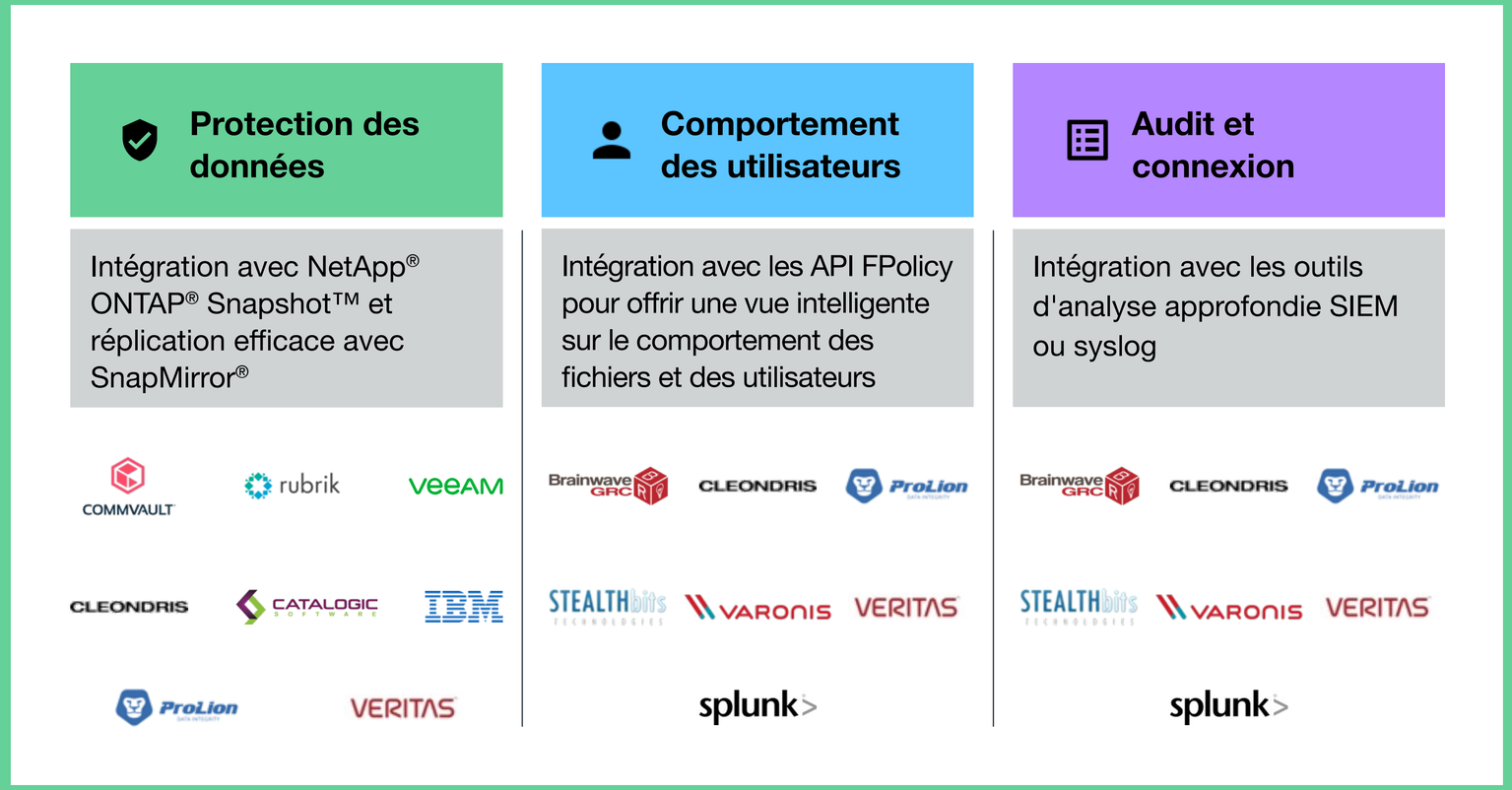
Un plan de cyberrésilience centré sur les données, où qu'elles se trouvent

À ce stade, vous vous demandez peut-être si ce scénario s'applique aussi bien dans le cas où vos données se trouvent sur site, dans le cloud, dans un environnement hybride ou même à la périphérie du réseau. Absolument.

Puisque la cyberrésilience est axée sur les données, celles-ci restent sécurisées, résilientes et disponibles où qu'elles se trouvent, sur site, sur un site distant ou dans le cloud. La solution de cyberrésilience de NetApp couvre le cloud hybride et s'intègre avec tous les principaux clouds publics.

Exploitez pleinement vos systèmes déjà en place

La solution de cyberrésilience axée sur les données de NetApp peut vous aider tout au long des cinq étapes du plan que nous avons décrit plus haut. Mais votre entreprise a peut-être déjà investi dans des outils de cybersécurité. Dans ce cas, les fonctions du logiciel NetApp ONTAP peuvent s'intégrer avec vos solutions afin de combler les lacunes au lieu de partir de zéro.



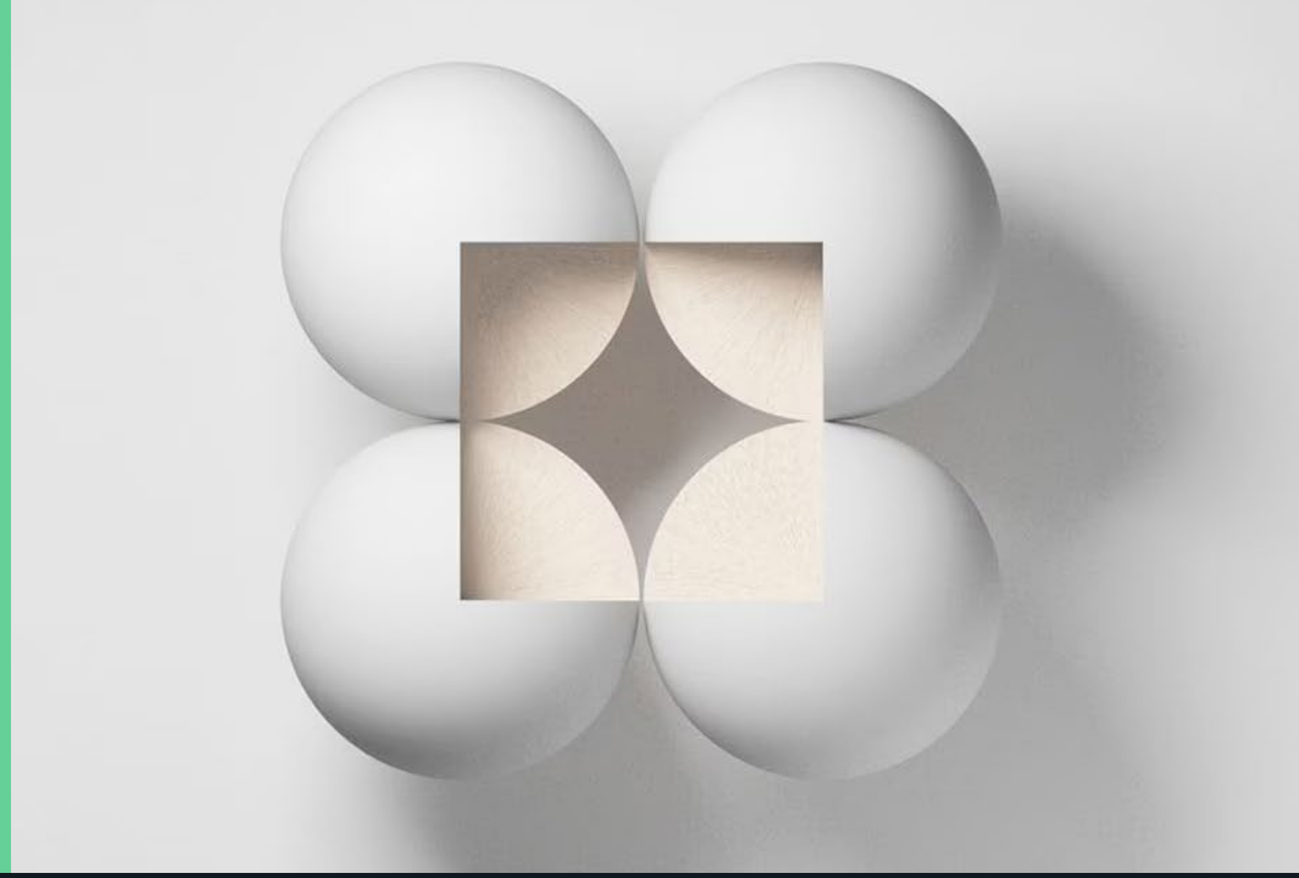
Mettez en place votre plan de cyberrésilience en quelques clics

Nous ne pouvons pas éradiquer la criminalité, mais nous pouvons activer la cyberrésilience de votre entreprise avec les bons outils.

Découvrez comment NetApp peut vous aider à mettre en œuvre votre plan de cyberrésilience axé sur les données.
netapp.com/cyber-resilience/

Cliquez sur les liens ci-dessous pour découvrir les dernières solutions, les blogs et les vidéos sur la cyberrésilience NetApp.

- Solution de cyberrésilience NetApp
- Solutions de protection des données NetApp
- Solutions anti-ransomware de NetApp
- Billets de blog sur la cyberrésilience NetApp
- Vidéos sur la cyberrésilience NetApp.tv



1. National Institute for Standards and Technology, « Developing Cyber-Resilient Systems », décembre 2021.
2. PBS NewsHour, « Why ransomware attacks are on the rise—and what can be done to stop them », 8 juillet 2021.
3. Business Wire, « Ransomware Index Spotlight Report Reveals Steady Increase in Sophistication and Volume of New Ransomware Vulnerabilities and Families in Q3 2021 », 9 novembre 2021.
4. Statista, « Methods of organizations compromised by ransomware to get their encrypted data back as of February 2021 », 2021.
5. Sophos News, « État des ransomware 2021 », 27 avril 2021.
6. Deloitte, « Double extortion incidents », octobre 2020.
7. Infosec, « NIST CSF: Implementing NIST CSF », 19 février 2020.

À propos de Netapp
NetApp est un spécialiste dans un monde de généralistes. Nous nous fixons un seul objectif : aider votre entreprise à valoriser ses données. NetApp migre vers le cloud les services de données haute performance que vous utilisez, et apporte à votre data center la flexibilité du cloud. Nos solutions leaders du secteur fonctionnent dans de nombreux environnements clients et les principaux clouds publics.

En tant qu'entreprise spécialisée dans les logiciels et axée sur le cloud et les données, seul NetApp peut vous aider à créer votre propre Data Fabric, à simplifier et connecter votre cloud, et à fournir les données, les applications et les services adaptés aux personnes appropriées, en tout lieu et à tout moment.

NetApp

+1 877 263 8277