DESCRIPTION DE LA SOLUTION

PROTÉGER, DÉTECTER, RESTAURER. UNE PROTECTION CONTRE LES RANSOMWARES AXÉE SUR LES DONNÉES

Protéger : sécurisez votre environnement.
Détecter : anticipez les menaces.
Restaurer : rebondissez rapidement.

Le challenge
Les attaques par ransomware constituent une menace de plus en plus répandue et sophistiquée pour les entreprises de toute taille. Ces attaques chiffrent les données précieuses et demandent un paiement pour leur restitution, ce qui entraîne souvent des pertes financières importantes et des perturbations opérationnelles.

- Les cyberincidents sont le risque commercial numéro un à l'échelle mondiale.
- Une attaque par ransomware aura lieu toutes les 2 secondes d'ici 2031.
- 59 % des entreprises ont été touchées par les ransomwares l'année dernière.
- Les attaques par ransomware ont augmenté de 73 % de 2022 à 2023.

Bien que de nombreuses entreprises se concentrent sur la sécurité du réseau et des terminaux, il est essentiel de ne pas négliger l'importance de la sécurisation de la couche de stockage où résident les données. En implémentant des mesures de sécurité robustes au niveau du stockage, telles que le chiffrement, les contrôles d'accès et les sauvegardes immuables, vous pouvez créer une ligne de défense supplémentaire contre les ransomwares.

Cette approche contribue à protéger les données à la source, ce qui complique le chiffrement ou la corruption des informations critiques pour les pirates. Les solutions de stockage sécurisé accélèrent les délais de restauration et minimisent les pertes de données en cas d'attaque, soulignant l'importance d'une stratégie de sécurité complète incluant la fortification de l'infrastructure de stockage.

Cyberrésilience NetApp : une approche de la protection contre les ransomwares axée sur les données

La protection contre les cyber-incidents englobe plusieurs couches de défense pour se protéger contre un large éventail de menaces. Une cyber-défense forte commence à la couche de **sécurité de l'identité** qui, avec la couche extérieure, **la sécurité du périmètre**, agit comme la première ligne de défense.

La sécurité réseau s'appuie sur cette base pour protéger les données en transit et détecter les activités anormales au sein du réseau interne. **La sécurité des terminaux** ajoute une couche de défense pour les périphériques individuels connectés au réseau. **La sécurité des applications** est axée sur la protection des applications logicielles contre les vulnérabilités et les attaques.

Enfin, **la sécurité des données** se trouve au cœur de cette stratégie, qui protège la ressource la plus précieuse d'une entreprise : ses données et les ressources les plus stratégiques. Cette couche inclut généralement la protection des données avec des solutions robustes de sauvegarde et de restauration.

Ces couches de sécurité interconnectées créent une stratégie de défense complète conçue pour protéger les ressources numériques de l'entreprise du périmètre au data center et répondre aux menaces à tous les niveaux de l'infrastructure IT.

La protection au niveau de la couche de données des ressources stratégiques est encore plus importante et a des exigences uniques. Pour être efficace, les solutions de cette couche doivent offrir ces quatre attributs essentiels :

- Conception sécurisée pour minimiser les risques d'attaque réussie contre votre entreprise
- Détection et réponse en temps réel pour minimiser l'impact d'une attaque réussie
- Protection WORM (Write Once, Read Many) avec protection air gap pour isoler les sauvegardes de données stratégiques
- Plan de contrôle simple pour une protection complète contre les ransomwares et une restauration rapide

NetApp peut détecter, protéger et restaurer au niveau de la couche de données.

Sécurité dès la conception : protection contre les ransomwares intégrée dans le stockage ONTAP
Le logiciel NetApp ONTAP fournit une protection fiable contre les ransomwares grâce à une approche de sécurité par conception. Les fonctionnalités clés incluent des copies Snapshot immuables et indélébiles, qui permettent aux données de rester inaltérables et ne pouvant pas être supprimées, même par les administrateurs, créant ainsi un point de secours fiable pour la restauration. La fonction ONTAP FPolicy renforce la sécurité en bloquant les fichiers malveillants, empêchant ainsi la propagation des menaces au sein du système.

PRINCIPAUX AVANTAGES

- **Sécurité intégrée.** Protection des données intégrée au niveau de la couche de stockage.
- **Détection et réponse en temps réel.** Une solution de défense contre les ransomware optimisée par l'IA.
- **Cyberarchivage.** Des sauvegardes immuables et indélébiles.
- **Plan de contrôle unifié.** Orchestration intelligente, de la détection à la restauration.
- **Garantie de reprise.** Aucune perte de données grâce aux copies Snapshot NetApp.

Pour renforcer les contrôles d'accès, la vérification multiadministrateur oblige plusieurs administrateurs à approuver des actions stratégiques, ce qui réduit le risque de menaces internes ou d'informations d'identification compromises. En outre, l'authentification multifacteur ajoute une couche de sécurité supplémentaire, ce qui signifie que seul le personnel autorisé peut accéder aux données et aux systèmes sensibles.

Détection et réponse en temps réel
Outre sa protection robuste contre les ransomwares, NetApp fournit une détection en temps réel avec une précision de 99 % et des capacités de réponse quasi instantanée, en exploitant la technologie autonome optimisée par l'IA intégrée directement dans ONTAP. Cette détection avancée surveille en permanence les activités suspectes et les anomalies, identifiant rapidement les attaques par ransomware lors de leur déploiement dans Amazon FSx pour ONTAP. Lorsqu'une menace est détectée, le système peut automatiquement isoler les données affectées et empêcher toute propagation supplémentaire, réduisant ainsi les dommages potentiels.

NetApp Data Infrastructure Insights (DII) offre une couche supplémentaire de protection contre les menaces internes. Ce logiciel détecte les comportements anormaux des utilisateurs et prend des mesures immédiates, par exemple en bloquant l'accès des utilisateurs aux systèmes de stockage et en effectuant des copies Snapshot. En outre, DII fournit un audit et des analyses détaillées. Cette approche globale associe la détection proactive des menaces, des mécanismes de réponse rapide et une surveillance détaillée de l'activité des utilisateurs, offrant ainsi un bouclier à multiples facettes contre les attaques par ransomware externes et les menaces internes.

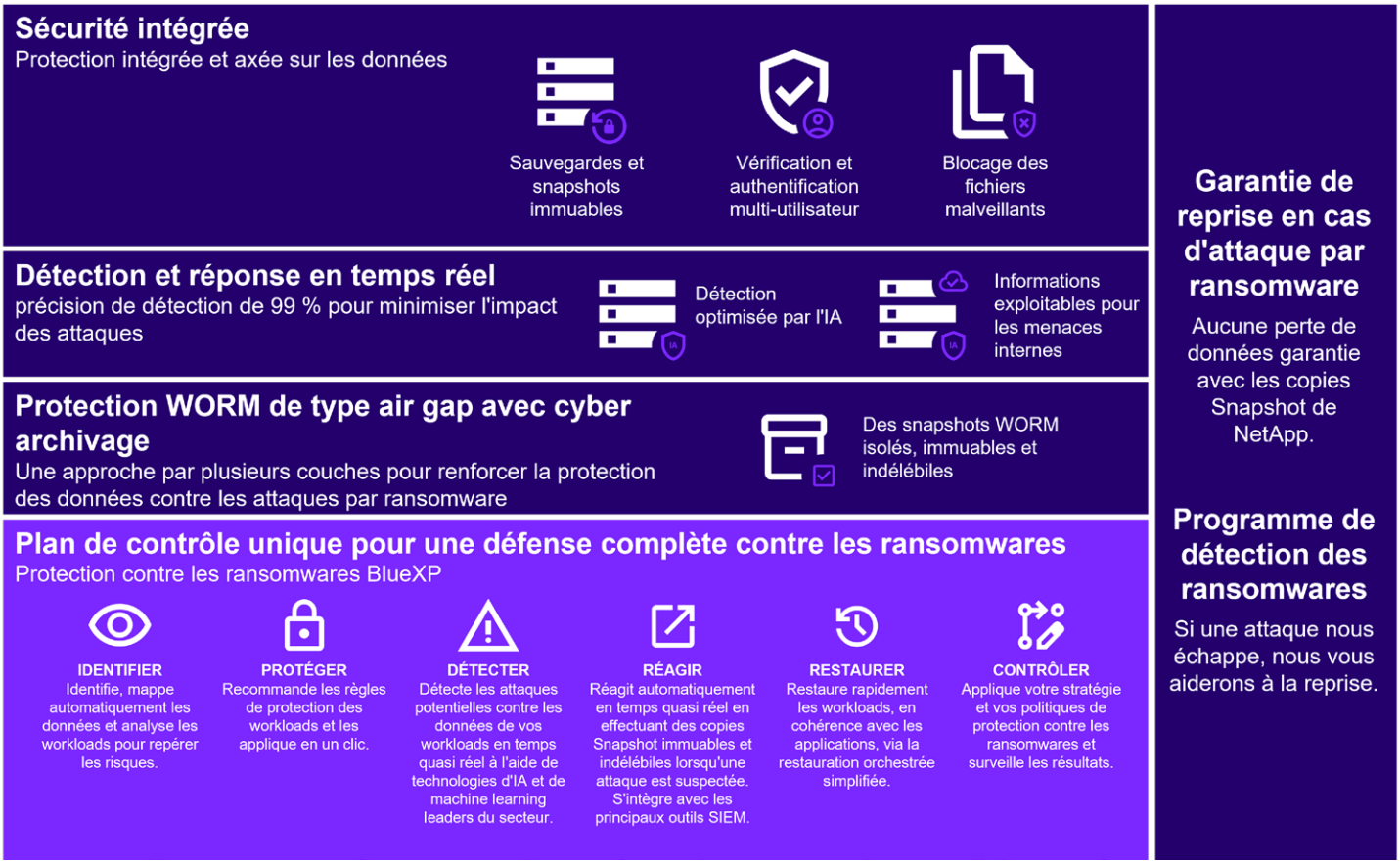

Figure 1 : NetApp propose le stockage des données le plus sécurisé au monde, avec des défenses à plusieurs couches pour protéger intelligemment et efficacement vos données, notamment l'accès aux données via un chiffrement de bout en bout, une authentification multifacteur et un accès basé sur les rôles.

Sauvegardes isolées pour le cyberarchivage
Le cyberarchivage de NetApp, optimisé par le logiciel de conformité SnapLock®, offre aux entreprises une solution complète et flexible pour protéger leurs données les plus stratégiques. L'air gap logique associé à des méthodologies de renforcement robustes pour ONTAP vous permet de créer des environnements de stockage isolés et sécurisés, résilients face aux cybermenaces en constante évolution. Avec NetApp, vous pouvez avoir confiance en la confidentialité, l'intégrité et la disponibilité de vos données, tout en conservant l'agilité et l'efficacité de votre infrastructure de stockage.

Pour renforcer la sécurité, NetApp permet de créer une couche supplémentaire de protection des données :

- Infrastructure de stockage sécurisée et isolée (par exemple, systèmes de stockage à air gap)
- Des copies de sauvegarde de vos données immuables et indélébiles
- Contrôles d'accès stricts et authentification multifacteur
- Fonctionnalités de restauration rapide des données
- En appliquant la technologie WORM, SnapLock empêche le chiffrement et la suppression des données à l'aide de copies de données indestructibles et efficaces

Plan de contrôle robuste et simple
NetApp est le seul fournisseur de stockage à proposer un plan de contrôle unique avec NetApp BlueXP™ pour coordonner et exécuter intelligemment les technologies de défense anti-ransomware de bout en bout axées sur les workloads. Grâce à ces technologies, vous pouvez **identifier et protéger** les données critiques des workloads stratégiques en un clic ; **détecter et répondre** de manière précise et automatique pour limiter l'impact des attaques potentielles ; et **restaurer** des workloads en quelques minutes, et non plus en plusieurs jours ou mois, en protégeant les données de vos workloads stratégiques et en réduisant les coûts liés à la perturbation de l'activité.

L'orchestrateur de protection contre les ransomwares BlueXP fusionne les puissantes fonctionnalités de NetApp ONTAP et les services de données BlueXP. Il inclut des recommandations et des conseils basés sur l'intelligence artificielle et le machine learning, ainsi que des workflows automatisés pour vous aider à :

- **Identifier.** Identifie automatiquement les workloads (VM, partages de fichiers, bases de données) et leurs données dans votre système de stockage NetApp, mappe les données aux workloads, détermine l'importance des workloads et analyse leur risque.
- **Protéger.** Recommande les règles de protection des workloads et les applique en un clic.

- **Détecter.** DÉTECTER : détecte les attaques potentielles contre les données de vos workloads grâce à la détection de pointe basée sur le ML en temps quasi réel.
- **Réagir :** Réagit automatiquement en temps quasi réel en effectuant des copies Snapshot immuables et indélébiles lorsqu'une attaque potentielle est suspectée.
- **Restaurer.** Valide l'intégrité des sauvegardes, identifie le meilleur point de restauration et restaure rapidement les workloads et leurs données associées grâce à une reprise orchestrée, simplifiée et cohérente au niveau des applications.

« 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

L'orchestrateur de protection contre les ransomwares BlueXP élimine la charge et l'anxiété liées à la défense des workloads contre les interruptions et les pertes de données liées aux ransomwares en fournissant une solution complète qui vous aide à vous préparer pour faire face aux attaques par ransomware, répond aux attaques et vous guide tout au long de la restauration. Seul NetApp vous assure que, en cas d'attaque, vous serez immédiatement alerté et vos données de workloads stratégiques seront protégées. La restauration sera plus simple et plus rapide pour minimiser les interruptions d'activité.

La protection contre les ransomwares de NetApp vous aide à identifier et à protéger les données où elles se trouvent, à détecter et à répondre de manière précise et automatique pour limiter l'impact des attaques potentielles et à restaurer les données en quelques minutes, au lieu de plusieurs jours ou mois. Cette fonctionnalité contribue à préserver vos données importantes et à minimiser les perturbations coûteuses pour la cyberrésilience.

Les ransomwares peuvent affaiblir des entreprises qui ne les prennent pas au sérieux. Seule l'approche de cyberrésilience axée sur les données de NetApp offre une sécurité et une protection complètes et intégrées pour les données primaires et secondaires avec une garantie pour vous aider à restaurer vos données.

En savoir plus sur les solutions anti-ransomware de NetApp

Nous contacter

À propos de NetApp

NetApp est l'entreprise d'infrastructure intelligente de données. NetApp propose une combinaison de stockage unifié, de services de données et de solutions CloudOps, conçue pour aider les organisations à transformer leurs défis en opportunités. Nous développons une infrastructure sans silos, exploitant l'observabilité et l'intelligence artificielle pour une gestion optimale des données. Notre service de stockage haute performance, nativement intégré dans les plus grands clouds, offre une flexibilité sans précédent. Nos services de données renforcent l'avantage compétitif des entreprises, améliorant la cyberrésilience, la gouvernance et l'agilité des applications. Nos solutions CloudOps, grâce à l'observabilité et l'intelligence artificielle, favorisent l'optimisation continue des performances et de l'efficacité. Peu importe le type de données, les workloads ou l'environnement, NetApp aide les entreprises à transformer leur infrastructure de données et à saisir les opportunités commerciales. **www.netapp.com/fr**

NetApp

SB-4219-0425-frFR