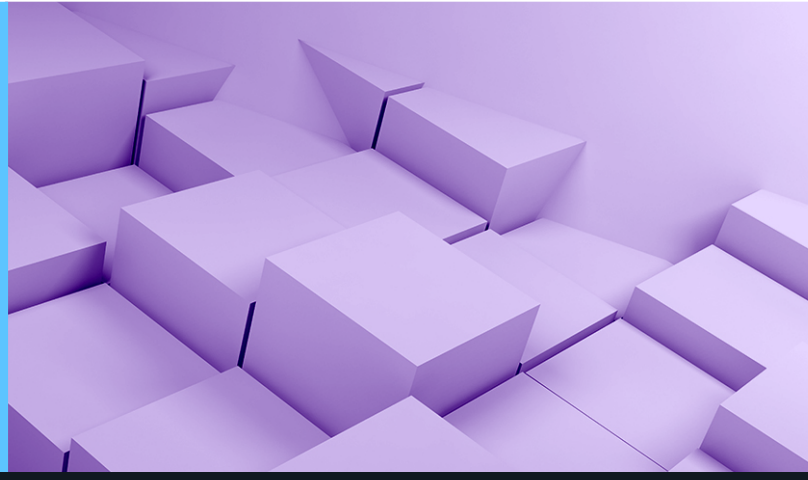
10 RAISONS

De choisir NetApp pour la protection contre les ransomware



01

Air gap logique

Créez un air gap logique pour sécuriser le verrouillage fichier et objet. NetApp® SnapLock® Compliance et NetApp StorageGRID® S3 Object Lock vous offrent des capacités WORM (write once, read many) natives pour empêcher la suppression des données pendant la période de conservation, même par des comptes d'administrateur compromis.

02

Restauration rapide

L'aspect le plus coûteux d'une attaque par ransomware est le temps d'interruption. Remettez vos données en ligne rapidement en utilisant les copies Snapshot immuables NetApp, et restaurez des téraoctets de données quelques secondes, contre plusieurs heures auparavant.

03

Protection anti-ransomware autonome

Découvrez et corrigez rapidement les cybermenaces à l'aide de la technologie de machine learning. Intégrée au logiciel NetApp ONTAP®, cette technologie contrôle le système de fichiers à la recherche d'anomalies qui pourraient indiquer la présence de malware à évolution lente. Utilisez aussi le blocage intégré des extensions de fichiers anti-malware pour détecter et empêcher la propagation des malware connus.

04

Détection des anomalies dans le comportement des utilisateurs

Détectez les anomalies en temps réel afin d'identifier les comptes d'utilisateurs compromis ou les éventuels comportements malveillants en utilisant la fonctionnalité Cloud Secure de NetApp Cloud Insights. Associée au composant NetApp FPolicy d'ONTAP, elle vous permet de créer automatiquement des points de restauration des données et de bloquer l'accès à d'autres comptes pour empêcher le vol ou la suppression massive de données.

05

Approche « zéro confiance »

Adoptez une approche Zéro confiance en matière de sécurité avec des contrôles tels que l'authentification multifacteur, l'accès basé sur des rôles, la journalisation complète et l'audit pour vous protéger contre les attaques auxiliaires.

06

Prévention contre les administrateurs malveillants

Empêchez les dommages causés par des comptes administrateur compromis en utilisant la vérification multiadministrateur ONTAP native. Cette fonctionnalité impose que plusieurs administrateurs autorisent les actions de stockage critiques telles que la suppression de volumes et de copies Snapshot.

07

Gestion avancée des copies

Améliorez la sauvegarde et la reprise d'activité. Utilisez NetApp SnapMirror® et le service NetApp Cloud Backup pour répliquer efficacement vos copies Snapshot vers un autre système ONTAP ou un stockage objet de votre choix, sur site ou dans le cloud.

08

Réduction des risques

Obtenez plus de visibilité sur la sécurité de vos données. Identifiez les données sensibles et leur emplacement en utilisant NetApp Cloud Data Sense. Suivez les autorisations des dossiers et proposez des options pour atténuer les risques comme l'exfiltration de données.

09

Surveillance centralisée

Surveillez votre infrastructure de cloud hybride grâce à une interface utilisateur simple. Identifiez les menaces et commencez à y remédier grâce au tableau de bord de protection contre les ransomware disponible dans NetApp Cloud Manager.

10

Analyse approfondie

Utilisez les solutions éprouvées de NetApp pour effectuer l'analyse des événements pré et post-ransomware. Collectez les informations dont vous avez besoin pour comprendre, gérer et fermer les chemins suivis par les attaques.

NetApp