

# Service de protection contre les ransomwares et de restauration NetApp



## **Planifiez, déployez et gérez une infrastructure de données de cloud hybride protégée contre les ransomwares, sécurisée, disponible, fiable et récupérable**

Face au nombre croissant d'attaques par ransomwares, vous avez besoin de bien plus qu'une assurance cybersécurité pour couvrir les coûts et les pertes de données. Mieux vaut prévenir que guérir : anticipez les attaques en assurant une sécurité adéquate et en protégeant vos données. L'identification des étapes à suivre pour mettre en place un environnement résilient aux ransomwares peut s'avérer complexe.

Vous avez besoin d'identifier clairement les données menacées et les mesures à mettre en place pour anticiper les risques. Définissez et déployez de bonnes pratiques et les outils adéquats pour répondre aux besoins spécifiques de votre entreprise. Et en cas d'attaque, ressources et expertise sont nécessaires pour identifier immédiatement les données affectées et la façon de les restaurer rapidement pour éviter toute perte critique.

### **Service de protection contre les ransomwares et de restauration NetApp**

Accélérez la résilience aux ransomwares et la capacité de survie de vos données avec l'aide des experts des services professionnels de NetApp®. Le service de protection contre les ransomwares et de restauration NetApp fournit l'expertise dont vous avez besoin pour planifier, déployer et gérer une infrastructure de données de cloud hybride protégée contre les ransomwares qui préservera la sécurité, la disponibilité, la fiabilité et la restauration des données stratégiques de votre entreprise.

Nous avons conçu une approche complète pour vous aider à mettre en place un environnement de stockage protégé contre les ransomwares qui minimise les temps d'arrêt, les coûts et les pertes de données en cas d'attaque. Pour adapter la protection à vos besoins, les experts des services professionnels de NetApp proposent un service en trois phases :

- **Découverte.** Nous évaluons votre environnement actuel, identifions les failles de sécurité, et votre plan de restauration des données (si disponible), et nous vous proposons des recommandations pour optimiser la mise en place de la suite logicielle contre les ransomwares de NetApp.
- **Implémentation.** Nos experts implémentent et configurent les outils de sécurité de NetApp adaptés à votre environnement de cloud hybride.
- **Gestion.** L'association d'un service géré par les experts NetApp au modèle d'abonnement vous permet de surveiller et de gérer votre environnement 24 h/24, 7 j/7, toute l'année.

### **Protection contre les attaques**

Pour vous préparer contre les ransomwares vous devez identifier les risques et les failles de sécurité, et définir les solutions appropriées. Nos experts évaluent intégralement votre environnement de données NetApp pour identifier les risques qui affectent la continuité de votre activité, identifier les failles de sécurité de vos solutions logicielles natives NetApp, détecter les volumes de stockage critiques

### **Principaux avantages**

**Détection et résolution des risques de sécurité avant une attaque par ransomware**

**Amélioration de la préparation contre les ransomwares et de la protection des données avec un service professionnel basé sur un modèle d'abonnement et personnalisé :**

- Implémentation et configuration des outils de protection contre les ransomwares NetApp leaders du secteur
  - Surveillance, résolution des problèmes et gestion des logiciels 24 h/24, 7 j/7, toute l'année
- Récupération des données en cas d'attaque par ransomware grâce à la restauration rapide des données**

sur lesquels les données ne sont pas protégées et évaluer votre capacité à restaurer les données après une attaque. Ces données nous permettent de vous fournir des recommandations exploitables pour rectifier rapidement les problèmes de sécurité et les risques avant toute attaque par ransomware. Nos experts vous aident également à détecter et à corriger toute faille au niveau de la protection des données et des règles de conservation des données pour que vous puissiez respecter les objectifs de délais de restauration et de points de récupération.

### **Protection de votre environnement contre les ransomwares**

Pour créer un environnement de données protégé contre les menaces cybernétiques, il ne suffit d'acheter un ensemble d'outils de sécurité. Grâce à ce service personnalisé basé sur l'abonnement, les experts de nos services professionnels déploient des bonnes pratiques à l'efficacité prouvée pour protéger vos systèmes de stockage de données. Ils vous aident à réduire les vulnérabilités en implémentant et en configurant le logiciel et les outils NetApp adaptés pour renforcer rapidement votre protection contre les attaques par ransomwares.

Nos spécialistes suivent des objectifs de niveau de service stricts pour vous aider à restaurer vos données en cas d'attaque par ransomware. Pour cela, ils appliquent un chiffrement avancé des données et testent et valident leur restauration. Ce service vous aide également à répondre aux enquêtes destinées aux assurances cybersécurité et à obtenir un score assurant votre éligibilité pour ce type d'assurance.

Nos spécialistes gèrent ensuite vos solutions NetApp de protection contre les ransomwares (NetApp Cloud Secure, FPolicy, SnapLock®, SnapCenter® et SnapMirror®) et assurent la surveillance via un système d'alertes, la résolution des problèmes et la gestion pour votre environnement, 24 h/24, 7 j/7, toute l'année. Ce service inclut le reporting et le conseil continu pour vous aider à respecter les exigences de sécurité, et permettre à votre équipe IT de se concentrer sur d'autres tâches en vous assurant que vos données sont sécurisées et récupérables.

### Récupération plus rapide après une attaque par ransomware

En cas d'attaque, la préservation de vos données dépend de la rapidité de restauration, de la continuité de votre activité et de l'intégrité des données. Les experts des services professionnels de NetApp vous aident à récupérer facilement votre activité après une attaque par ransomware sans perdre de données critiques. Grâce à la récupération dans SnapCenter à partir d'un archivage de données immuable, notre équipe des services NetApp s'assure que vos données stratégiques sont entièrement récupérables et intactes tout en évitant la propagation des ransomwares.

### Services professionnels supplémentaires recommandés

- **Services gérés flexibles.** La flexibilité de ces services vous aide à préserver votre environnement de cloud hybride NetApp ONTAP® en utilisant uniquement les modules de services qui sont nécessaires.
- **Authentification multifacteur (MFA).** Pour renforcer la protection, les experts NetApp appliquent l'authentification multifacteur aux systèmes primaires, secondaires et SnapLock.

### Commencez dès aujourd'hui

Pour en savoir plus sur le service de protection contre les ransomwares et de récupération NetApp, contactez votre ingénieur commercial NetApp local ou rendez-vous sur le site [www.netapp.com/fr](http://www.netapp.com/fr).

### À propos des services NetApp

Valorisez vos investissements. Pour planifier votre data center nouvelle génération, rechercher un savoir-faire spécialisé pour le déploiement du stockage à grande échelle ou optimiser l'efficacité opérationnelle de votre infrastructure, les services NetApp sont là pour vous accompagner.

### 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, au bon moment et en toute sécurité.