NETAPP RANSOMWARE RECOVERY

Détectez les attaques de ransomware en temps réel, évitez la perte de données, assurez une restauration rapide et minimisez l'impact sur votre entreprise

Êtes-vous préparé contre les attaques par ransomware ?
Un aspect essentiel de la préparation à une attaque de ransomware est la protection de vos données de charge de travail au niveau de la couche de stockage, la dernière ligne de défense. Les attaques devenant de plus en plus sophistiquées, automatisées et coûteuses, il est irréaliste d'empêcher une attaque par ransomware. Vous devez être prêt lorsque des attaquants entrent.

Les sauvegardes seules ne suffisent pas. Vous devez être en mesure d'évaluer les risques pesant sur vos données de charge de travail critiques et de détecter les menaces et d'y réagir en temps réel. Vous avez également besoin de plans de récupération en place qui peuvent être exécutés rapidement et facilement. Cependant, obtenir une résilience efficace contre une attaque de ransomware représente un fardeau opérationnel, avec de nombreuses tâches manuelles sujettes aux erreurs et trop peu de personnel possédant l'expertise nécessaire.

Si vous n'avez pas de programme en place, les attaques sur vos charges de travail ne seront pas détectées et vos réponses seront retardées. La reprise de la charge de travail sera complexe et prendra en moyenne 7 jours.[1] —et vos données pourraient même ne pas être entièrement récupérées. C'est trop peu, trop tard.

Profitez d'une protection complète au niveau de la dernière ligne de défense
Le service NetApp® Ransomware Resilience vous permet d'exécuter rapidement et facilement votre programme, de la prévention à la détection, en passant par la réponse aux attaques et la reprise d'activité.

Ransomware Resilience fournit une interface unique pour orchestrer intelligemment votre défense contre les ransomwares centrée sur la charge de travail. En quelques clics, vous pouvez identifier et protéger vos données de charge de travail critiques à risque. Le service détecte et répond également avec précision et automatiquement aux attaques potentielles et limite leur impact. Et vous pouvez récupérer des charges de travail, sans logiciels malveillants, en quelques minutes, en protégeant vos précieuses données et en minimisant les dommages et le coût des perturbations pour votre entreprise.

Ransomware Resilience fusionne les puissantes fonctionnalités du logiciel NetApp ONTAP® avec les services de données NetApp, ajoutant des recommandations et des conseils intelligents avec des flux de travail automatisés pour :

- **Identifier.** Identifiez automatiquement les charges de travail (machines virtuelles, partages de fichiers, bases de données populaires) et leurs données dans votre stockage NetApp, mappez les données à la charge de travail et déterminez la sensibilité, l'importance et le risque des données.
- **Protection.** Obtenez des recommandations pour les politiques de protection de la charge de travail et appliquez-les en un clic.
- **Détection.** Détectez en temps réel les fichiers suspects et les activités de comportement des utilisateurs qui pourraient signaler des tentatives potentielles d'exfiltration de données, ainsi que des tentatives de cryptage de fichiers et de suppression massive.
- **Répondre aux attaques.** Protégez les charges de travail en créant automatiquement des copies NetApp Snapshot™ et en bloquant les utilisateurs lorsqu'une attaque potentielle est suspectée. Le service s'intègre également aux solutions de gestion des informations et des événements de sécurité (SIEM) de pointe.
- **Restauration.** Restaurez rapidement les charges de travail et leurs données associées grâce à un processus de récupération simple et orchestré. Et en utilisant l'environnement de récupération isolé, vous obtenez une restauration propre et sans malware de vos données.
- **Gouverner votre infrastructure.** Appliquez votre stratégie et vos politiques de protection contre les ransomware et surveillez les résultats.

Préparez-vous à une attaque : gagnez du temps et améliorez votre efficacité

Ransomware Resilience identifie automatiquement les types de données dans votre stockage NetApp, mappe les données à des charges de travail spécifiques, évalue la sensibilité et la criticité des données et analyse les risques. Ce processus réduit votre dépendance à l'égard d'analyses manuelles complexes, d'outils tiers supplémentaires et d'une expertise spécialisée.

PRINCIPAUX AVANTAGES

Bénéficiez d'une protection complète et orchestrée en dernière ligne de défense :

- Obtenez une visibilité complète sur votre posture de protection de la charge de travail.
- Détectez une attaque à un stade précoce et évitez la perte de données.
- Récupérez rapidement l'intégralité des charges de travail et sans logiciel malveillant afin de minimiser les interruptions, les coûts, les pertes de revenus et les dommages commerciaux.
- Obtenez des données pour une analyse approfondie et des recommandations pour améliorer votre posture de sécurité.

Ransomware Resilience propose ensuite des politiques de protection intelligentes utilisant les fonctionnalités ONTAP, notamment a détection d'anomalies de la protection autonome contre les ransomwares optimisée par l'IA (ARP/AI) de NetApp, le blocage des extensions malveillantes FPolicy et les copies Snapshot inviolables. Ransomware Resilience adapte également les recommandations de protection à la sensibilité et à la criticité de vos actifs de données.

En un seul clic, vous appliquez les règles de protection de manière transparente et cohérente aux données de vos workloads. Ransomware Resilience fonctionne en arrière-plan pour configurer les fonctionnalités d'ONTAP et les services de données NetApp, et pour orchestrer les flux de travail de protection sur chaque volume de données, réduisant ainsi le besoin de tâches manuelles répétitives.

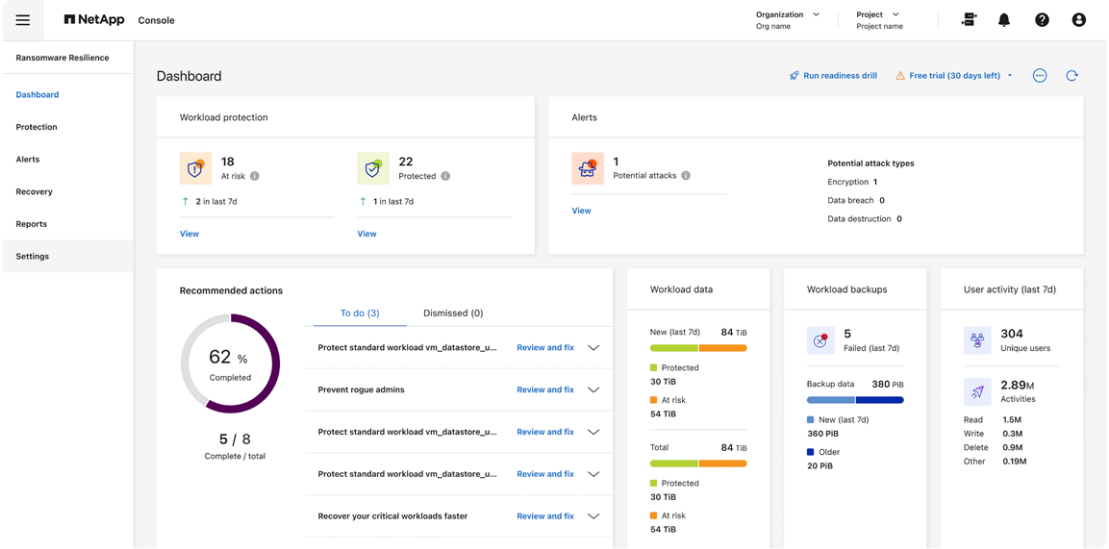
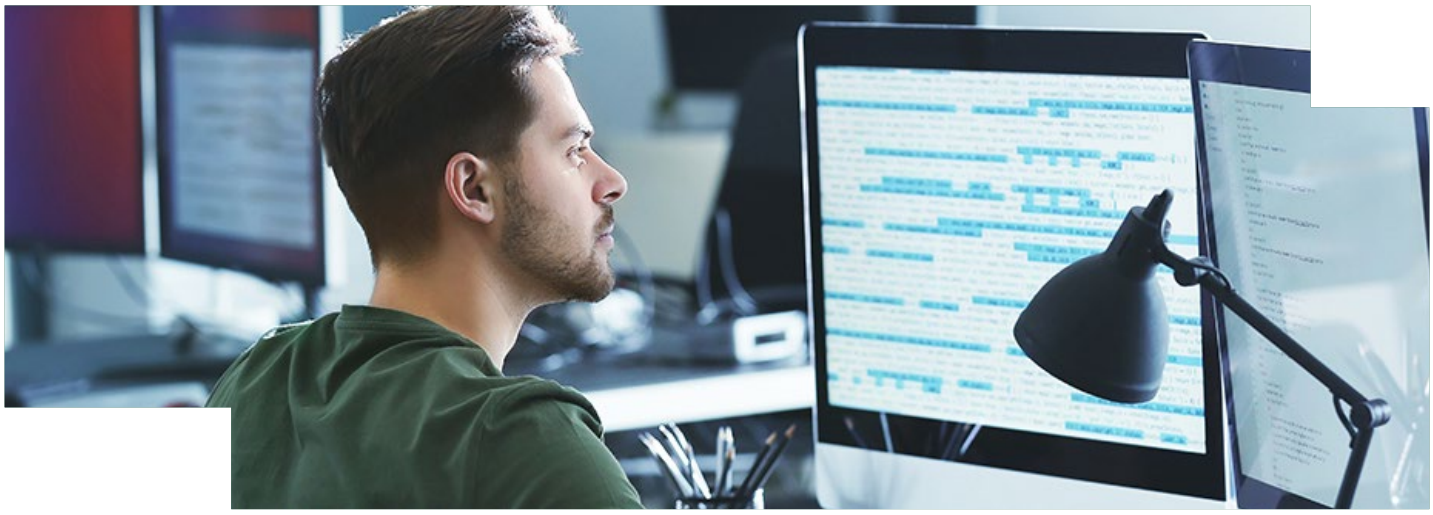


Figure 1 : Le service NetApp Ransomware Resilience offre une défense complète et orchestrée contre les ransomwares centrée sur la charge de travail, de la détection à la récupération via un plan de contrôle unique.



Détecter et répondre aux menaces en temps réel
Ransomware Resilience surveille en permanence les anomalies de fichiers suspects et de comportement des utilisateurs. Il peut détecter les violations de données en identifiant les premiers comportements des utilisateurs qui pourraient signaler des tentatives potentielles d'exfiltration de données, ainsi que des tentatives de cryptage de fichiers et de suppression massive. Lorsqu'une attaque est suspectée, Ransomware Resilience crée une copie Snapshot pour éviter la perte de données et permet de bloquer l'utilisateur qui commet l'attaque pour l'arrêter et empêcher de nouvelles attaques.

Ce service utilise une détection de ransomware innovante et avancée basée sur l'IA sur votre stockage principal. Cette approche signifie que les attaques potentielles peuvent être détectées rapidement et atténuées immédiatement.

Ransomware Resilience fournit des rapports d'incident pour soutenir l'analyse approfondie et s'intègre aux solutions SIEM leaders du secteur.

Récupérez facilement les charges de travail, en quelques minutes
Ransomware Resilience orchestre le flux de travail pour une récupération cohérente des applications de toutes les données de charge de travail associées et vous donne une visibilité sur le processus et l'état en temps réel. Les copies instantanées peuvent être restaurées au niveau de la charge de travail ou de manière plus granulaire au niveau du volume ou du fichier.

Dans le cadre du processus de récupération, Ransomware Resilience fournit un environnement de récupération isolé qui isole les charges de travail infectées, supprime les logiciels malveillants, recommande un point de récupération et guide l'utilisateur tout au long d'un processus de restauration intuitif. Cette approche offre une restauration propre et sans logiciel malveillant et empêche la réinfection de vos données.

Limiter les interruptions de l'activité
Ransomware Resilience élimine le fardeau et l'anxiété liés à la protection de vos charges de travail contre les temps d'arrêt et les pertes de données liés aux ransomwares. Il offre un service complet qui améliore votre préparation, répond aux attaques et vous guide tout au long de la récupération. Seul NetApp vous permet d'avoir l'esprit tranquille en sachant que lorsqu'une attaque se produit, vous serez immédiatement alerté, vos précieuses données de charge de travail seront protégées et la récupération sera rapide et facile, minimisant ainsi les perturbations pour votre entreprise.

Obtenez NetApp Ransomware Resilience dès aujourd'hui

[1] ESG, 2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation, novembre 2023.

Nous contacter

À propos de NetApp
NetApp est une société d'infrastructure de données intelligente, combinant stockage de données unifié, données intégrées, services opérationnels et de charge de travail pour transformer un monde de perturbations en opportunité pour chaque client. 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 services opérationnels et de charge de travail offrent une optimisation continue des performances et de l'efficacité de l'infrastructure et des charges de travail grâce à l'observabilité et à l'IA. Peu importe le type de données, la charge de travail ou l'environnement, NetApp aide les organisations à transformer leur infrastructure de données et à saisir les opportunités commerciales. En savoir plus sur www.netapp.com ou suivez-nous sur X, LinkedIn, Facebook, et Instagram.

SB-4278-0925-frFR