À propos de la protection contre les ransomware de NetApp

ONTAP 9

NetApp
August 31, 2024

Sommaire

À propos de la protection contre les ransomware de NetApp

Attaques par ransomware et portefeuille de solutions de protection de NetApp

Les ransomwares restent l'une des menaces les plus importantes qui ont entraîné des interruptions d'activité pour les entreprises en 2024. D'après le "Sophos : État des ransomware 2024", les attaques par ransomware ont affecté 72 % de leur public interrogé. Les attaques par ransomware ont évolué pour être plus sophistiquées et ciblées : les acteurs de menaces utilisent des techniques avancées, telles que l'intelligence artificielle, pour optimiser leur impact et leurs bénéfices.

Les entreprises doivent regarder l'ensemble de leur posture de sécurité du périmètre, du réseau, de l'identité, des applications et de l'emplacement des données au niveau du stockage, et sécuriser ces couches. L'adoption d'une approche axée sur les données en matière de cybersécurité au niveau de la couche de stockage est cruciale dans le paysage actuel des menaces. Bien qu'aucune solution ne puisse déjouer toutes les attaques, l'utilisation d'un portefeuille de solutions, notamment des partenariats et des tiers, offre une défense multicouche.

Le Gamme de produits NetApp fournit divers outils efficaces pour la visibilité, la détection et la résolution des problèmes, ce qui vous aide à détecter rapidement les ransomware, à prévenir la propagation et à restaurer rapidement, si nécessaire, pour éviter les interruptions coûteuses. Les solutions de défense à plusieurs couches classiques restent répandues, tout comme les solutions tierces et partenaires pour la visibilité et la détection. Une solution efficace reste une partie essentielle de la réponse à toute menace. L'approche unique du secteur qui repose sur la technologie NetApp Snapshot immuable et la solution SnapLock Logical Air Gap est un atout concurrentiel dans le secteur et constitue la bonne pratique du secteur pour la résolution des problèmes par ransomware.

Depuis juillet 2024, le contenu du rapport technique *TR-4572: NetApp ransomware protection*, qui a été publié au format PDF, a été intégré au reste de la documentation produit de ONTAP.

Les données sont la cible principale

Les cybercriminels ciblent de plus en plus directement les données, en reconnaissant leur valeur. Bien que la sécurité du périmètre, du réseau et des applications soit importante, il est possible de les contourner. La couche de stockage, qui se concentre sur la protection des données à la source, constitue une dernière ligne de défense critique. Les attaques par ransomware ont pour objectif d'accéder aux données de production et de les chiffrer ou de les rendre inaccessibles. Pour y parvenir, les attaquants doivent déjà avoir percé les défenses existantes déployées par les entreprises aujourd'hui, du périmètre à la sécurité des applications.

[Couches de sécurité du périmètre à la sécurité des données]

Malheureusement, de nombreuses entreprises ne tirent pas parti des fonctionnalités de sécurité au niveau de la couche de données. C'est là qu'intervient la gamme de solutions NetApp pour la protection contre les ransomwares, pour vous protéger dans votre dernier domaine de défense.

Le vrai coût des ransomwares

Le paiement d'une rançon en elle-même n'a pas le plus grand effet financier sur une entreprise. Bien que le paiement ne soit pas insignifiant, il reste insignifiant comparé au coût des temps d'indisponibilité liés à un incident d'ransomware.

Le paiement d'une rançon n'est qu'un élément du coût de la récupération lorsqu'il s'agit de faire face à des attaques par ransomware. En excluant toute rançon payée, les entreprises ont déclaré en 2024 un coût moyen de restauration suite à une attaque par ransomware de 2,7 millions de dollars, soit une augmentation de près de 1 million de dollars par rapport aux 1,2 million de dollars rapportés en 2023 "2024 Sophos State of ransomware". Les coûts peuvent être 10 fois plus élevés pour les entreprises qui dépendent fortement de la disponibilité INFORMATIQUE, telles que l'e-commerce, les actions boursières et les soins de santé.

Les coûts de la cyberassurance continuent également d'augmenter, étant donné la très réelle probabilité d'une attaque par ransomware sur les entreprises assurées.

Protection contre les ransomware au niveau de la couche de données

NetApp comprend que la sécurité de votre entreprise est vaste et approfondie dans tout le périmètre, jusqu'à l'emplacement des données au niveau de la couche de stockage. Votre pile de sécurité est complexe et doit assurer la sécurité à tous les niveaux de votre pile technologique.

La protection en temps réel au niveau de la couche de données est encore plus importante et a des exigences uniques. Pour être efficace, les solutions de cette couche doivent offrir les attributs critiques suivants :

- **Sécurité par conception** pour minimiser les risques d'attaque réussie
- **Détection et réponse en temps réel** pour minimiser l'impact d'une attaque réussie
- **Protection WORM à air Gap** pour isoler les sauvegardes de données critiques
- **Un seul plan de contrôle** pour une défense complète contre les ransomware

NetApp peut vous offrir tout cela et bien plus encore.

[La gamme de solutions NetApp pour la protection contre les ransomwares qui inclut les attributs stratégiques décrits]

Le portefeuille de solutions NetApp pour la protection contre les ransomwares

NetApp "protection intégrée contre les ransomware"propose une défense à facettes et robuste en temps réel pour vos données stratégiques. Au cœur de ces outils, des algorithmes avancés de détection optimisés par l'IA surveillent en continu les modèles de données, ce qui permet d'identifier rapidement les menaces de ransomware avec une précision de 99 %. En réagissant rapidement aux attaques, notre stockage peut créer rapidement des snapshots de données et sécuriser les copies, assurant ainsi une restauration rapide.

Pour renforcer encore davantage les données, la "cyber-archivage" capacité de NetApp isole les données avec un air Gap logique. En protégeant les données stratégiques, nous assurons une continuité rapide de l'activité.

NetApp "Protection BlueXP contre les ransomware"réduit la charge opérationnelle à l'aide d'un plan de contrôle unique pour coordonner et exécuter intelligemment une défense anti-ransomware de bout en bout axée sur la charge de travail. Vous pouvez ainsi identifier et protéger les données de workloads stratégiques à risque d'un simple clic, détecter et répondre de manière précise et automatique pour limiter l'impact d'une attaque potentielle. Vous pouvez également restaurer vos workloads en quelques minutes au lieu de plusieurs jours, en protégeant vos données de workloads stratégiques et en minimisant les interruptions coûteuses.

En tant que solution ONTAP intégrée native pour protéger les accès non autorisés à vos données, "Vérification multiadministrateur" bénéficiez de fonctionnalités robustes qui assurent l'exécution des opérations telles que la suppression de volumes, la création d'utilisateurs administratifs ou la suppression de copies Snapshot uniquement après approbation d'un second administrateur désigné. Cela empêche les administrateurs compromis, malveillants ou peu expérimentés d'effectuer des modifications ou de supprimer des données indésirables. Vous pouvez configurer autant d'approbateurs administrateurs désignés que vous le souhaitez avant de supprimer une copie snapshot.

NetApp ONTAP répond à la condition requise pour "Authentification multifacteur (MFA)" l'authentification Web dans System Manager et l'authentification via l'interface de ligne de commandes SSH.

Avec la protection contre les ransomwares de NetApp, travaillez sereinement dans un environnement aux menaces qui ne cesse d'évoluer. Son approche globale ne se contente pas de vous défendre contre les variantes actuelles des ransomwares. Elle s'adapte également aux menaces émergentes, assurant ainsi la sécurité à long terme de votre infrastructure de données.

Découvrez les autres options de protection

- "La protection contre les ransomware de Active IQ"
- "Sécurité des workloads de stockage Cloud Insights (CISWS)"
- "FPolicy"
- "SnapLock et copies Snapshot inviolables"

Garantie de restauration contre les ransomwares

NetApp garantit la restauration des données Snapshot en cas d'attaque par ransomware. Notre garantie : si nous ne pouvons pas vous aider à restaurer vos données de snapshot, nous nous engageons à trouver la solution. La garantie est disponible pour tout achat de systèmes AFF A-Series, AFF C-Series, ASA et FAS.

En savoir plus >>

- "Description du service de garantie de récupération"
- "Blog sur la garantie de restauration contre les ransomwares".

Informations associées

- Page des ressources du site de support NetApp http://mysupport.netapp.com/ontap/resources
- Sécurité des produits NetApp https://security.netapp.com/resources/

SnapLock et copies Snapshot inviolables pour la protection contre les ransomwares

SnapLock, l'une des armes essentielles de l'arsenal de NetApp Snap, s'est avéré très efficace pour protéger les données contre les menaces de ransomware. En empêchant la suppression non autorisée des données, SnapLock fournit une couche de sécurité supplémentaire qui garantit l'intégrité et l'accessibilité des données critiques, même en cas d'attaques malveillantes.

Conformité SnapLock

SnapLock Compliance (SLC) assure une protection indélébile de vos données. SLC interdit la suppression de données même lorsqu'un administrateur tente de réinitialiser la baie. Contrairement à d'autres produits concurrents, SnapLock Compliance n'est pas vulnérable aux piratages d'ingénierie sociale par l'intermédiaire des équipes de support de ces produits. Les données protégées par des volumes SnapLock Compliance peuvent être récupérables jusqu'à leur date d'expiration.

Pour activer SnapLock, une "ONTAP One" licence est requise.

En savoir plus >>

- "Documentation SnapLock"

Copies Snapshot inviolables

Les copies Snapshot inviolables constituent un moyen pratique et rapide de protéger vos données contre les actes malveillants. Contrairement à SnapLock Compliance, TPS est généralement utilisé sur les systèmes principaux où l'utilisateur peut protéger les données pendant un temps déterminé et les laisser localement pour des restaurations rapides ou où les données n'ont pas besoin d'être répliquées hors du système principal. TPS utilise les technologies SnapLock pour empêcher la suppression de la copie Snapshot primaire, même par un administrateur ONTAP, pendant la même période d'expiration de la conservation SnapLock. La suppression de copie Snapshot est impossible même si le volume n'est pas activé sur SnapLock, bien que les snapshots ne possèdent pas la même nature indélébile que les volumes SnapLock Compliance.

Pour que les copies Snapshot soient inviolables, une "ONTAP One" licence est requise.

En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware".

Blocage des fichiers FPolicy

FPolicy empêche le stockage des fichiers indésirables sur votre appliance de stockage haute performance. FPolicy vous permet également de bloquer les extensions de fichiers ransomware connues. Un utilisateur dispose toujours des autorisations d'accès complètes au dossier de départ, mais FPolicy ne permet pas à un utilisateur de stocker les fichiers marqués par votre administrateur comme bloqués. Le cas échéant, il n'est pas important que ces fichiers soient des fichiers MP3 ou des extensions de fichiers ransomware connues.

Bloquez les fichiers malveillants avec le mode natif FPolicy

Le mode natif NetApp FPolicy (une évolution du nom, la stratégie de fichiers) est un framework de blocage d'extension de fichiers qui vous permet de bloquer les extensions de fichiers indésirables dans votre environnement. Fait partie de ONTAP depuis plus de dix ans, il est incroyablement utile pour vous protéger contre les ransomware. Ce moteur « zéro confiance » est très utile, car vous bénéficiez de mesures de sécurité supplémentaires qui vont au-delà des autorisations de liste de contrôle d'accès (ACL).

Dans le Gestionnaire système ONTAP et BlueXP , une liste de plus de 3000 extensions de fichier est disponible pour référence.

Certaines extensions peuvent être légitimes dans votre environnement et leur blocage peut entraîner des problèmes inattendus. Créez votre propre liste adaptée à votre environnement avant de configurer FPolicy natif.

Le mode natif FPolicy est inclus dans toutes les licences ONTAP.

En savoir plus >>

- "Blog : lutter contre les ransomware : troisième partie : ONTAP FPolicy, un autre outil puissant et natif (appelé gratuitement)"

Activez l'analyse du comportement des utilisateurs et des entités (UEBA) avec le mode externe FPolicy

Le mode externe FPolicy est un framework de notification et de contrôle de l'activité des fichiers qui offre une visibilité sur l'activité des fichiers et des utilisateurs. Ces notifications peuvent être utilisées par une solution externe pour effectuer des analyses basées sur l'IA afin de détecter les comportements malveillants.

Le mode externe FPolicy peut également être configuré pour attendre l'approbation du serveur FPolicy avant de permettre l'exécution d'activités spécifiques. Vous pouvez configurer plusieurs règles de ce type sur un cluster, ce qui vous apporte une grande flexibilité.

Les serveurs FPolicy doivent répondre aux requêtes FPolicy s'ils sont configurés pour être approuvés. Sinon, les performances du système de stockage risquent d'être affectées.

Le mode externe FPolicy est inclus dans "Toutes les licences ONTAP".

En savoir plus >>

- "Blog : lutter contre les ransomware : quatrième partie — UBA et ONTAP avec le mode externe FPolicy."

Sécurité des workloads de stockage Cloud Insights (CISWS)

La fonction Storage Workload Security (SWS) est une fonctionnalité de NetApp Cloud Insights qui améliore considérablement la sécurité, la capacité de restauration et la responsabilisation d'un environnement ONTAP. SWS adopte une approche axée sur l'utilisateur, en suivant l'activité de tous les fichiers de chaque utilisateur authentifié dans l'environnement. Il utilise des analyses avancées pour établir des modèles d'accès normaux et saisonniers pour chaque utilisateur. Ces modèles sont utilisés pour identifier rapidement les comportements suspects sans avoir besoin de signatures de ransomware.

Lorsque SWS détecte un ransomware, une suppression de données ou une attaque d'exfiltration, il peut prendre des mesures automatiques, telles que :

- Prenez un instantané du volume affecté.
- Bloquez le compte utilisateur et l'adresse IP suspectés d'activité malveillante.
- Envoyez une alerte aux administrateurs.

Comme il peut prendre des mesures automatisées pour arrêter rapidement une menace interne et suivre

chaque activité de fichier, SWS simplifie et accélère la restauration suite à un événement de ransomware. Grâce aux outils avancés d'audit et d'analyse intégrés, les utilisateurs peuvent immédiatement voir quels volumes et fichiers ont été affectés par une attaque, quel compte d'utilisateur l'attaque a été et quelle action malveillante a été exécutée. Les snapshots automatiques atténuent les dommages et accélèrent la restauration des fichiers.

[Résultats de l'attaque sur la sécurité des workloads de stockage Cloud Insights]

Les alertes issues de la protection anti-ransomware autonome (ARP) de ONTAP sont également visibles dans SWS, fournissant une interface unique aux clients qui utilisent à la fois ARP et SWS pour se protéger contre les attaques par ransomware.

En savoir plus >>

- "NetApp Cloud Insights"

Détection et réponse basées sur l'IA intégrées à NetApp ONTAP

Comme les menaces de ransomware sont de plus en plus sophistiquées, vos mécanismes de défense aussi devraient-ils le faire. La protection anti-ransomware autonome (ARP) de NetApp est optimisée par l'IA avec la détection d'anomalies intelligente intégrée à ONTAP. Activez-la pour ajouter une couche de défense supplémentaire à votre cyberrésilience.

ARP et ARP/ai sont configurables via l'interface de gestion intégrée ONTAP, System Manager et activées par volume.

Protection autonome contre les ransomwares (ARP)

La protection anti-ransomware autonome (ARP), une autre solution ONTAP intégrée native depuis 9.10.1, examine l'activité des fichiers de workloads de volume de stockage NAS et l'entropie des données pour détecter automatiquement les ransomwares. ARP fournit aux administrateurs une détection en temps réel, des informations et un point de restauration des données pour une détection intégrée sans précédent des ransomwares.

Pour ONTAP 9.15.1 et les versions antérieures qui prennent en charge ARP, ARP démarre en mode d'apprentissage pour apprendre l'activité typique des données de charge de travail. Cela peut prendre sept jours pour la plupart des environnements. Une fois le mode d'apprentissage terminé, le protocole ARP passe automatiquement en mode actif et commence à rechercher les activités anormales des workloads qui pourraient être des ransomware.

En cas d'activité anormale, une copie Snapshot automatique est immédiatement effectuée, ce qui fournit un point de restauration aussi proche que possible du moment de l'attaque avec un minimum de données infectées. Simultanément, une alerte automatique (configurable) est générée et permet aux administrateurs de voir l'activité anormale des fichiers afin qu'ils puissent déterminer si l'activité est malveillante et prendre les mesures appropriées.

Si l'activité correspond à une charge de travail attendue, les administrateurs peuvent facilement la marquer comme un faux positif. ARP apprend ce changement comme une activité normale de la charge de travail et ne le signale plus comme une attaque potentielle à l'avenir.

Pour activer ARP, une "ONTAP One" licence est requise.

En savoir plus >>

- "Protection autonome contre les ransomwares"

Protection anti-ransomware autonome/IA (ARP/ai)

Présenté en tant que préversion technologique d'ONTAP 9.15.1, ARP/ai va encore plus loin avec la détection en temps réel intégrée des systèmes de stockage NAS. La nouvelle technologie de détection optimisée par l'IA est entraînée sur plus d'un million de fichiers et diverses attaques par ransomware connues. En plus des signaux utilisés dans ARP, ARP/ai détecte également le chiffrement des en-têtes. La puissance ai et les signaux supplémentaires permettent à ARP/ai d'offrir une précision de détection supérieure à 99 %. Ce résultat a été validé par se Labs, un laboratoire de test indépendant qui a donné à ARP/ai son meilleur classement AAA.

L'entraînement des modèles étant effectué en continu dans le cloud, l'ARP/l'IA ne requiert pas de mode d'apprentissage. Elle est active dès sa mise sous tension. La formation continue implique également que l'ARP/l'IA est toujours validée contre les nouveaux types d'attaques par ransomware dès qu'ils surviennent. ARP/ai est également fourni avec des fonctionnalités de mise à jour automatique qui fournissent de nouveaux paramètres à tous les clients pour maintenir la détection des ransomware à jour. Toutes les autres fonctionnalités de détection, d'aperçu et de point de restauration des données d'ARP sont conservées pour ARP/ai.

Pour activer ARP/ai, une "ONTAP One" licence est requise.

En savoir plus >>

- "Blog : la solution NetApp de détection des ransomwares en temps réel basée sur l'IA classe AAA"

Protection WORM protégée par air avec archivage électronique

L'approche de NetApp en matière de cyber-coffre est une architecture de référence dédiée pour un cyber-coffre à air Gap logique. Cette approche tire parti des technologies de renforcement de la sécurité et de conformité, telles que SnapLock, pour permettre des snapshots immuables et indélébiles.

Cyber-archivage avec SnapLock Compliance et un air Gap logique

La tendance est de plus en plus marquée aux pirates informatiques qui détruisent les copies de sauvegarde et, dans certains cas, même les chiffrent. C'est pourquoi beaucoup dans le secteur de la cybersécurité recommandent d'utiliser des sauvegardes « air Gap » dans le cadre d'une stratégie globale de cyberrésilience.

Le problème, c'est que les lacunes traditionnelles (bandes et supports hors ligne) peuvent considérablement augmenter le temps de restauration, augmentant ainsi les temps d'indisponibilité et les coûts globaux associés. Même une approche plus moderne de la solution de l'air Gap peut s'avérer problématique. Par exemple, si le coffre-fort de sauvegarde est temporairement ouvert pour recevoir de nouvelles copies de sauvegarde, puis déconnecte et ferme sa connexion réseau aux données primaires pour être à nouveau « à air Gap », un attaquant pourrait tirer parti de l'ouverture temporaire. Au cours de la connexion, un attaquant pourrait frapper pour compromettre ou détruire les données. Ce type de configuration ajoute également généralement une complexité indésirable. L'air Gap logique est un excellent substitut à un air Gap traditionnel ou moderne car il possède les mêmes principes de protection de sécurité tout en conservant la sauvegarde en ligne. Avec NetApp, simplifiez la gestion des bandes et des disques grâce aux air Gap logiques, que vous pouvez obtenir avec des copies Snapshot immuables et NetApp SnapLock Compliance.

[Air Gap logique avec NetApp Cyber Vault]

NetApp a publié la fonctionnalité SnapLock il y a plus de 10 ans pour répondre aux exigences de conformité des données, telles que la loi HIPAA (Health Insurance Portability and Accountability Act), la loi Sarbanes-Oxley et d'autres règles relatives aux données réglementaires. Vous pouvez également archiver ces copies snapshot primaires dans des volumes SnapLock de façon à ce qu'elles puissent être validées sur WORM, ce qui empêche leur suppression. Il existe deux versions de licence SnapLock : SnapLock Compliance et SnapLock Enterprise. Pour une protection contre les ransomwares, NetApp recommande SnapLock Compliance, car vous pouvez définir une période de conservation spécifique pendant laquelle les copies Snapshot sont verrouillées et ne peuvent pas être supprimées, même par les administrateurs ONTAP ou le support NetApp.

En savoir plus >>

- "Blog : protection multicouche contre les ransomware avec la solution Cyber Vault de NetApp"

Copies Snapshot inviolables

En utilisant SnapLock Compliance comme air Gap logique, vous bénéficiez d'une protection ultime pour empêcher les pirates de supprimer vos copies de sauvegarde, mais vous devez déplacer les copies Snapshot à l'aide de SnapVault vers un volume SnapLock secondaire. Par conséquent, de nombreux clients déploient cette configuration sur un système de stockage secondaire sur le réseau. Cela peut entraîner des temps de restauration plus longs qu'avec la restauration d'une copie Snapshot d'un volume primaire sur un système de stockage primaire.

À partir de la version ONTAP 9.12.1, les copies Snapshot inviolables assurent une protection proche du niveau SnapLock Compliance de vos copies Snapshot sur le stockage primaire et dans les volumes primaires. Il n'est pas nécessaire d'archiver la copie Snapshot à l'aide de SnapVault sur un volume secondaire SnapLocaché. Les copies Snapshot inviolables utilisent la technologie SnapLock pour empêcher la suppression de la copie Snapshot primaire, même si un administrateur ONTAP complet utilise la même période d'expiration de conservation SnapLock. Cela permet d'accélérer les délais de restauration et de sauvegarder un volume FlexClone à l'aide d'une copie Snapshot protégée et inviolable, ce que vous ne pouvez pas faire avec une copie Snapshot classique dans un stockage SnapLock Compliance.

La principale différence entre les copies SnapLock Compliance et les copies Snapshot inviolables est que SnapLock Compliance n'autorise pas l'initialisation et la suppression de la baie ONTAP si des volumes SnapLock Compliance existent avec des copies Snapshot archivées qui n'ont pas encore atteint leur date d'expiration. Pour que les copies Snapshot soient inviolables, vous devez disposer d'une licence SnapLock Compliance.

En savoir plus >>

- "Verrouillez une copie Snapshot pour vous protéger contre les attaques par ransomware"

La protection contre les ransomware de Active IQ

NetApp Active IQ est un conseiller digital qui simplifie le support proactif et l'optimisation du stockage NetApp grâce à des informations exploitables et une gestion des données optimale. Alimenté par les données de télémétrie de notre base installée diversifiée, il emploie des techniques avancées d'intelligence artificielle et de MACHINE LEARNING pour découvrir les opportunités de réduction des risques et d'amélioration des performances et de l'efficacité de votre environnement de stockage.

Non seulement peut "NetApp Active IQ" vous y aider "éliminez les failles de sécurité", mais il fournit également

des informations et des recommandations spécifiques pour vous protéger contre les ransomwares. Une carte d'intégrité dédiée présente les actions nécessaires et les risques résolus. Vous êtes ainsi sûr que vos systèmes respectent ces recommandations en matière de bonnes pratiques.

[Moniteurs d'intégrité dans le tableau de bord NetApp Active IQ]

Les risques et les actions suivis sur la page ransomware Defense Wellness incluent notamment les éléments suivants :

- Le nombre de copies Snapshot des volumes est faible, ce qui réduit la protection potentielle contre les ransomware.
- FPolicy n'est pas activé pour toutes les machines virtuelles de stockage (SVM) configurées pour les protocoles NAS.

Pour voir la protection contre les ransomware de Active IQ en action, consultez "NetApp Active IQ".

Résilience complète avec la protection BlueXP contre les ransomware

Il est important que la détection des ransomwares se produise le plus tôt possible afin d'éviter la propagation des ransomwares et d'éviter des interruptions coûteuses. Toutefois, une stratégie efficace de détection des ransomwares doit inclure plusieurs couches de protection. La protection contre les ransomware de NetApp repose sur une approche complète qui inclut des capacités en temps réel intégrées s'étendant aux services de données via BlueXP et une solution isolée en couches pour la cybercopie.

Protection BlueXP contre les ransomware

BlueXP est un plan de contrôle unique pour orchestrer intelligemment une défense anti-ransomware complète et axée sur les workloads. La protection contre les ransomwares BlueXP réunit les puissantes fonctionnalités de cyberrésilience d'ONTAP, telles que ARP, FPolicy, les copies Snapshot inviolables et les services de données BlueXP , tels que la sauvegarde et la restauration BlueXP . Elle propose également des recommandations et des conseils avec des workflows automatisés pour fournir une défense de bout en bout via une seule interface utilisateur. Il fonctionne au niveau des workloads pour s'assurer que les applications sur lesquelles s'exécute votre entreprise sont protégées et peuvent être restaurées aussi rapidement que possible en cas d'attaque.

[La protection contre les ransomwares BlueXP est une fonctionnalité d'intelligence artificielle qui fournit de l'aide pour minimiser les pertes de données de workloads et permettre une reprise rapide des données. Cette image montre l'interface utilisateur de BlueXP .]

Avantages pour le client :

- La préparation assistée par ransomware réduit la surcharge opérationnelle et améliore l'efficacité
- La détection d'anomalies optimisée par l'IA et le ML améliore la précision et accélère la réponse pour maîtriser les risques
- La restauration guidée cohérente au niveau des applications vous permet de restaurer les workloads plus facilement et en quelques minutes

"Protection BlueXP contre les ransomware" Facilite la réalisation de ces fonctions NIST :

- Automatiquement **découvrir** et hiérarchiser les données dans le stockage NetApp **en mettant l'accent sur les principales charges de travail basées sur les applications**.
- **Protection en un clic** de la sauvegarde des données de la charge de travail la plus importante, immuable, configuration sécurisée, blocage des fichiers malveillants et domaine de sécurité différent.
- **Détectez avec précision** les ransomware au plus vite * en utilisant **la détection d'anomalies basée sur l'IA nouvelle génération.**
- Réponse automatisée et flux de travail et intégration avec les meilleures solutions * SIEM et XDR.*
- Restaurez rapidement les données à l'aide d'une récupération * orchestrée simplifiée* pour accélérer la continuité des applications.
- Mettez en œuvre votre **stratégie** et **politiques** de protection contre les ransomware et **surveillez les résultats**.

Informations sur le copyright

Informations sur les marques commerciales