FICHE PRODUIT

Fonctions de sécurité d'ONTAP

Sécurisation des ressources les plus importantes : les données

Le logiciel de gestion des données NetApp® ONTAP® continue d'évoluer, et la sécurité fait partie intégrante de cette solution. Les dernières versions d'ONTAP comprennent plusieurs nouvelles fonctions de sécurité essentielles pour protéger les données de l'entreprise dans le cloud hybride, éviter les attaques par ransomware et se conformer aux bonnes pratiques du secteur. Ces nouvelles fonctions contribuent également à la transition vers un modèle « zéro confiance. »

Pour en savoir plus sur le renforcement de la sécurité de la solution ONTAP, consultez le rapport technique TR-4569 : Guide sur le renforcement de la sécurité de la solution NetApp ONTAP.

Le challenge

Avec la transformation digitale, les entreprises subissent une pression considérable. Elles sont tenues de gérer efficacement des données distribuées, dynamiques et diversifiées dans leur cloud hybride. Chaque jour, les menaces sont plus sophistiquées et plus dangereuses pour les environnements IT. En tant qu'administrateurs et opérateurs de ressources d'informations et de données, les équipes IT doivent gérer les données de manière sécurisée tout au long de leur cycle de vie.

La solution

Le logiciel NetApp ONTAP joue un rôle clé dans la protection des données et le respect des règles de conformité. Reportez-vous à cette fiche produit et au rapport technique TR-4569 : Guide sur le renforcement de la sécurité de la solution NetApp ONTAP, pour découvrir comment mettre en place une stratégie de sécurité reconnue qui protégera vos ressources les plus précieuses : les données.

Principaux avantages

Amélioration de la confidentialité, de l'intégrité et de la disponibilité des données
Protégez les ressources les plus importantes de votre entreprise, les données, avec les technologies ONTAP de sécurité du cloud hybride.

Renforcement de la stratégie de sécurité de votre entreprise
Assurez un socle sûr et solide pour le cloud hybride de votre entreprise en exploitant des fonctionnalités de visibilité et de sécurité qui créent une infrastructure sécurisée.

Application des bonnes pratiques du secteur et de NetApp en matière de sécurité et de protection contre les ransomware
Mettez en place une culture avancée de la sécurité grâce à l'expertise de NetApp et sa connaissance du secteur.

Respect des exigences de gouvernance et de conformité
Appliquez les bonnes pratiques établies en matière de sécurité pour respecter et promouvoir la réglementation applicable dans votre secteur, ainsi que les règles de sécurité.

Fonctions de sécurité d'ONTAP

Logiciel ou fonctionnalités	Fonction	Impact
Protection anti-ransomware autonome	La protection anti-ransomware autonome est une fonctionnalité intégrée avec une détection préventive contre les attaques grâce au machine learning.	Lors de la détection d'une anomalie, ONTAP fait automatiquement une copie Snapshot puis alerte l'administrateur.
Copies NetApp Snapshot™	Une Snapshot ONTAP est une copie en lecture seule de vos données, efficace et à un point dans le temps. Une Snapshot est une représentation exacte de vos données au moment de sa prise, qu'elle ait eu lieu il y a plusieurs heures, jours, semaines, mois ou même années.	Comme les copies Snapshot sont en lecture seule, elles ne peuvent pas être infectées par des ransomware. En cas d'attaque par ransomware, il vous suffit d'effectuer une restauration à partir d'une Snapshot antérieure à l'événement.
Technologie NetApp SnapLock®	NetApp SnapLock protège les copies Snapshot à l'aide de NetApp SnapVault® au moyen d'une sauvegarde de type « air gap » logique et indélébile.	SnapLock élimine le risque que les copies Snapshot soient supprimées par un administrateur à la suite d'une erreur humaine, par un collaborateur mécontent ou un tiers malveillant disposant d'identifiants volés.
Verrouillage des copies Snapshot	La technologie SnapLock est utilisée pour le verrouillage des copies Snapshot afin de les rendre indélébiles, manuellement ou automatiquement, pendant une durée spécifique.	Les copies Snapshot peuvent être supprimées par un administrateur à la suite d'une erreur humaine, par un collaborateur mécontent ou un tiers malveillant disposant d'identifiants volés.
Technologie NetApp FPolicy	FPolicy est un composant de l'infrastructure ONTAP qui permet à des applications partenaires de surveiller et définir les autorisations d'accès aux fichiers. Les règles peuvent être basées sur le type de fichier. FPolicy détermine la façon dont le système de stockage gère les requêtes de chaque système client pour des opérations telles que les créations, ouvertures, renommages et suppressions. Remarque : dans ONTAP, le système de notification d'accès aux fichiers FPolicy possède des commandes de filtrage et supporte de brèves coupures de réseau.	Le contrôle d'accès est un élément clé dans toute solution de sécurité. Par conséquent, la visibilité des accès aux fichiers et des opérations sur fichiers ainsi que la possibilité d'y réagir sont stratégiques pour maintenir le niveau de sécurité requis. Pour fournir cette visibilité et ce contrôle d'accès aux fichiers, la solution ONTAP utilise la fonction FPolicy. Les serveurs externes FPolicy, y compris NetApp Cloud Insights/Cloud Secure, exploitent l'analytique comportementale des utilisateurs pour identifier les malware et ransomware afin de limiter les conséquences d'une compromission des données à grande échelle.
NetApp Volume Encryption (NVE)	NVE est un mécanisme de chiffrement logiciel qui vous permet de chiffrer des données sur n'importe quel type de disque avec une clé unique par volume.	Le chiffrement des données au repos reste une priorité du secteur. NVE répond à cette priorité tout en assurant une sécurité renforcée dans l'ensemble du cloud hybride.
Suppression sécurisée NVE	Cette fonctionnalité permet la suppression cryptographique des fichiers sur les volumes NVE en migrant les fichiers sains et en éliminant la clé utilisée pour chiffrer les fichiers infectés.	Vous pouvez résoudre les problèmes de fuite de données en ligne alors que le système est en cours d'utilisation. Cette fonctionnalité inclut un mécanisme de suppression de pointe, conforme au Règlement général de l'Union européenne sur la protection des données (RGPD).
NetApp Aggregate Encryption (NAE)	NAE est un mécanisme de chiffrement logiciel qui vous permet de chiffrer des données sur n'importe quel type de disque grâce au partage de clés uniques par agrégat dans les volumes chiffrés.	Comme NVE, NAE permet le chiffrement des données au repos. NAE permet en outre la déduplication dans l'agrégat, car les volumes partagent les clés dans l'ensemble de l'agrégat, ce qui améliore l'efficacité du stockage.

Fonctions de sécurité d'ONTAP

Logiciel ou fonctionnalités	Fonction	Impact
Chiffrement par défaut des données au repos	La fonctionnalité de chiffrement par défaut des données au repos est activée si un gestionnaire de clés externe ou intégré est défini. NVE ou NAE est utilisé comme mécanisme de chiffrement logiciel. Si les disques NSE font partie de la configuration des clusters, le chiffrement des données au repos est en place. Le chiffrement logiciel n'est pas utilisé par défaut.	Le chiffrement par défaut des données au repos simplifie le maintien d'une sécurité renforcée dans l'ensemble du cloud hybride.
NetApp Storage Encryption (NSE)	NSE est l'implémentation par NetApp du chiffrement de disque intégral (FDE) à l'aide de disques autochiffrés FIPS-140-2 de niveau 2. NSE propose un chiffrement sans interruption, compatible avec l'ensemble de la suite de technologies NetApp d'efficacité du stockage.	Le chiffrement des données au repos reste une priorité du secteur. NSE, qui inclut FDE, répond à cette priorité. L'environnement NetApp Data Fabric assure une sécurité renforcée de bout en bout.
Chiffrement SMB utilisant l'accélération Intel AES New Instructions (AES-NI)	Intel AES NI améliore l'algorithme AES et accélère le chiffrement des données pour toute la gamme de processeurs compatibles.	L'accélération des fonctions de sécurité se traduit par un gain d'efficacité. L'utilisation efficace des ressources est déterminante pour obtenir des solutions de sécurité haute performance.
NetApp Cryptographic Security Module (NCSM)	Ce module prend en charge les opérations de chiffrement conformes à la norme FIPS 140-2 pour certains services de gestion SSL. À partir de la version ONTAP 9.11.1, le protocole TLS 1.3 est pris en charge et les opérations sont conformes à la norme FIPS 140-2.	Des modules de sécurité spécialisés améliorent l'efficacité des ressources. En outre, FIPS 140 est la norme reconnue du secteur pour les produits et solutions de cryptographie.
NetApp CryptoMod	Ce module prend en charge les opérations de chiffrement conformes à la norme FIPS 140-2 pour NVE, NAE et le gestionnaire de clés intégré (OKM).	FIPS 140-2 est la norme reconnue du secteur pour les produits et solutions de cryptographie.
Prise en charge de la fonction SHA-2 (SHA-512)	Afin de renforcer la sécurité des mots de passe, ONTAP prend en charge la fonction de hachage SHA-2 et utilise par défaut la fonction SHA-512 pour hacher les nouveaux mots de passe ou les mots de passe modifiés.	La fonction de hachage SHA-2 s'est imposée comme la norme du secteur en raison de sa sécurité grandement améliorée par rapport à la fonction SHA-1 dont les failles ont été maintes fois exploitées.
Transfert de journaux sécurisé (Syslog over TLS [Transport Layer Security])	La fonction de transfert de journaux permet aux administrateurs de provisionner des cibles ou destinations de manière à ce qu'elles puissent recevoir des informations d'audit ou syslog. Compte tenu du caractère sensible de ces informations, ONTAP peut les envoyer de manière sécurisée via TLS à l'aide du paramètre TCP chiffré.	Les informations d'audit et de journalisation sont extrêmement précieuses pour le support et la disponibilité. En outre, les informations figurant dans les journaux (syslog) ainsi que dans les rapports et résultats d'audit sont généralement sensibles. Pour préserver les contrôles et le niveau de sécurité, vous devez gérer les données de journalisation et d'audit de manière sécurisée.
TLS 1.1 et TLS 1.2	ONTAP utilise TLS 1.1 et TLS 1.2 pour sécuriser ses fonctions de communication et d'administration.	NetApp déconseille d'utiliser TLS 1.0, car ses vulnérabilités le rendent incompatible avec certaines normes de conformité telles que PCI-DSS. NetApp privilégie l'utilisation de TLS 1.1 et TLS 1.2 en raison de leur robustesse et de leur intégrité.
Protocole OCSP	Lorsqu'il est activé, le protocole OCSP permet aux applications ONTAP qui utilisent des communications TLS ou LDAP de recevoir le statut du certificat numérique. L'application reçoit une réponse signée indiquant si le certificat demandé est valide, révoqué ou inconnu.	Le protocole OCSP permet de déterminer le statut actuel d'un certificat numérique sans nécessiter de listes de révocation de certificats.
Onboard Key Manager (OKM)	Dans ONTAP, OKM fournit une solution de chiffrement autonome pour les données au repos. Le gestionnaire de clés intégré OKM fonctionne conjointement avec NVE pour fournir un mécanisme de chiffrement logiciel qui vous permet de chiffrer vos données avec n'importe quel type de disque. Il fonctionne également avec NSE pour réaliser un chiffrement de disque intégral (FDE) qui est effectué avec les disques autochiffrés.	OKM assure la gestion des clés pour NSE et NVE. En outre, l'utilisation de cette technologie de chiffrement dans ONTAP vous permet de sécuriser les données au repos, un point essentiel.
Démarrage sécurisé OKM	Cette option permet de demander une phrase secrète pour déverrouiller des disques et déchiffrer les volumes après le redémarrage d'un nœud.	Lorsque NSE et NVE ont recours à OKM, le redémarrage sécurisé protège l'intégralité de la baie de stockage (pas seulement les disques) contre les risques de vol. Cette fonctionnalité sécurise également le transport physique de clusters entiers, ainsi que le retour d'équipement.

Fonctions de sécurité d'ONTAP

Logiciel ou fonctionnalités	Fonction	Impact
Gestion externe des clés	La gestion externe des clés est assurée par un système tiers dans l'environnement de stockage. Celui-ci gère de manière sécurisée les clés d'authentification et de chiffrement utilisées au sein du système de stockage par des fonctionnalités de chiffrement, notamment NSE, NVE ou NAE. Le système de stockage utilise une connexion SSL pour contacter le serveur de gestion externe des clés. Il stocke et récupère les clés d'authentification ou les clés de chiffrement des données de volume au moyen du protocole KMIP (Key Management Interoperability Protocol).	La gestion externe des clés permet de centraliser les fonctions de gestion des clés de l'entreprise tout en veillant à ce que les clés ne soient pas stockées près des ressources, réduisant ainsi le risque pour la sécurité.
Colocation sécurisée	La colocation sécurisée signifie l'utilisation de partitions virtuelles sécurisées au sein d'un environnement de stockage physique partagé pour permettre le partage de cet environnement entre plusieurs locataires distincts. Dans ONTAP, ces partitions sont appelées « machines virtuelles de stockage » (SVM).	La colocation sécurisée permet à ONTAP de devenir une plateforme partagée avec des SVM isolant de manière sécurisée tous les locataires à l'intérieur de la plateforme.
Gestion externe et mutualisée des clés	La gestion externe et mutualisée des clés permet à chaque locataire ou machine virtuelle de stockage (SVM) de gérer ses propres clés via le protocole KMIP pour NVE.	La gestion externe et mutualisée des clés permet de centraliser les fonctions de gestion des clés de votre entreprise par service ou locataire tout en veillant à ce que les clés ne soient pas stockées près des ressources, réduisant ainsi le risque pour la sécurité.
Gestionnaires de clés externes en cluster	La redondance des serveurs KMIP externes est prise en charge par les fonctionnalités de mise en cluster fournies par les partenaires de serveurs de clés de NetApp KMIP. Avant ONTAP 9.11.1, jusqu'à quatre serveurs KMIP externes pouvaient être définis et ONTAP écrivait des clés attribuées à chaque serveur pour assurer la redondance.	Les gestionnaires de clés externes en cluster ont été largement adoptés par les clients ONTAP. La prise en charge d'ONTAP permet à ces clients d'utiliser cette fonctionnalité sans difficulté.
Audit amélioré du système de fichiers	ONTAP génère davantage d'événements d'audit détaillés. Voici les principales informations enregistrées lors de la création d'événements : Fichier Dossier Partage d'accès Fichiers créés, modifiés ou supprimés Fichiers dont l'accès en lecture a abouti Échecs de lecture de champs ou d'écriture de fichiers Modification des autorisations sur les dossiers	Face aux menaces émergentes, les systèmes de fichiers NAS ont étendu leur empreinte. Ainsi, la visibilité qu'offrent les fonctions d'audit demeure donc stratégique, et les fonctionnalités d'audit améliorées d'ONTAP fournissent beaucoup plus de détails qu'auparavant concernant l'audit CIFS.
Signature et chiffrement SMB - CIFS	La signature SMB contribue à sécuriser votre environnement Data Fabric en protégeant le trafic entre les systèmes de stockage et les clients contre les attaques par réexécution ou les attaques de l'homme du milieu. Elle veille également à ce que les messages SMB aient une signature valide. En outre, ONTAP prend en charge le chiffrement SMB.	Le protocole SMB constitue un vecteur de menaces courant pour les systèmes de fichiers et les architectures. La signature et le chiffrement permettent de valider le trafic en plus de sécuriser le transport de données de façon progressive.
Prise en charge de Kerberos 5 et Krb5p	ONTAP prend en charge le chiffrement AES 128 bits et 256 bits pour Kerberos. Le service de confidentialité comprend la vérification de l'intégrité des données reçues, l'authentification utilisateur et le chiffrement des données avant la transmission.	L'authentification Krb5p offre une protection contre la falsification et l'espionnage des données. Elle utilise des checksums pour chiffrer l'ensemble du trafic entre le client et le serveur.
Signature et chiffrement SMB - LDAP (Lightweight Directory Access Protocol)	ONTAP prend en charge la signature et le chiffrement pour sécuriser la session lors de requêtes vers un serveur LDAP.	La signature valide l'intégrité des données LDAP à l'aide d'une technologie à clé secrète. Le chiffrement crypte les données LDAP afin de ne pas transmettre de données sensibles en clair.
Courbes Ed25519 et NIST dans SSH (algorithmes et HMAC mis à jour)	ONTAP fournit des chiffrements et échanges de clés SSH mis à jour, notamment AES, 3DES, SHA-256 et SHA-512.	Les menaces ne cessent de prendre de l'ampleur. C'est pourquoi l'algorithme du protocole, le chiffrement et les échanges de clés doivent être suffisamment robustes pour assurer l'intégrité du protocole et le bon fonctionnement du produit.

Fonctions de sécurité d'ONTAP

Logiciel ou fonctionnalités	Fonction	Impact
Configuration du nombre maximal d'échecs pour les tentatives de connexion SSH	Dans ONTAP, le paramètre parameter-max-authentication-retry-count a été ajouté à la commande security ssh modify pour permettre la configuration du nombre maximal de tentatives de connexion. Le nombre maximal de tentatives de connexion SSH par défaut est de six. Toutefois, NetApp recommande de le limiter à trois.	Cette fonctionnalité vous protège contre les attaques par force brute.
Authentification multifacteur (MFA)	L'authentification multifacteur est activée pour NetApp ONTAP System Manager et NetApp Active IQ® Unified Manager. Elle régit l'accès administratif web via le langage SAML et des fournisseurs d'identité tiers. L'accès administratif par ligne de commande à ONTAP repose sur des méthodes locales d'authentification à deux facteurs qui allient un identifiant utilisateur ou un mot de passe à une clé publique. Vous pouvez utiliser nsswitch avec publickey comme l'un des deux facteurs permettant l'accès administratif SSH par ligne de commande. Il est possible d'utiliser FIDO2 pour l'authentification SSH avec un appareil d'authentification matérielle Yubikey ou d'autres appareils FIDO2 compatibles.	Les identifiants d'administrateur faibles représentent le risque principal pour la sécurité des systèmes. L'authentification multifacteur empêche tout accès administrateur pour les comptes munis uniquement d'un mot de passe.
Technologie NetApp SnapLock avec NSE et NVE	ONTAP prend en charge NSE et NVE avec la fonction SnapLock qui permet d'administrer et de stocker des données WORM (Write Once, Read Many).	La technologie SnapLock crée des volumes spéciaux sur lesquels des fichiers peuvent être stockés dans un état non effaçable et non écrasable. Cet état peut être attribué indéfiniment ou pendant une période de conservation définie, tout en maintenant le niveau de sécurité (chiffrement) des solutions NSE et NVE.
Validation des images lors de la mise à niveau	L'authenticité des images ONTAP est validée au moment de la mise à niveau.	Ce processus de validation permet de détecter l'utilisation d'images corrompues ou falsifiées lors de la mise à niveau.
Démarrage sécurisé UEFI	La validation des images a lieu chaque démarrage du système.	Les images ONTAP signées sont validées par le chargeur de démarrage afin d'empêcher toute falsification des images à chaque démarrage.
Chiffrement des pairs de cluster	Le chiffrement des pairs de cluster exploite TLS 1.2 pour chiffrer toutes les données transférées sur le réseau entre les pairs de cluster et les fonctionnalités ONTAP sous-jacentes qui utilisent le cluster peering pour la réplication des données (NetApp SnapMirror®, SnapVault®, FlexCache®).	Le chiffrement des données à la volée est disponible pour les fonctionnalités ONTAP chargées de la réplication des données. En outre, les clients qui ont recours au chiffrement des données au repos (NVE/NSE) peuvent utiliser le chiffrement de bout en bout entre les clusters ONTAP pour lesquels le chiffrement repose sur les pairs de cluster.
Chiffrement IPsec	IPsec offre le chiffrement de données en transit pour l'ensemble du trafic IP, notamment les protocoles NFS, iSCSI et SMB/CIFS.	IPsec s'assure que les données en transit sont sécurisées et chiffrées en continu. Le trafic du réseau entre le client et ONTAP est protégé grâce à des actions préventives afin d'empêcher les attaques par réexécution ou les attaques de l'homme du milieu.
Contrôle d'accès basé sur des rôles (RBAC)	La fonction RBAC d'ONTAP permet aux administrateurs de limiter l'accès administratif des utilisateurs au niveau correspondant à leur rôle. Les administrateurs peuvent ainsi gérer les utilisateurs par le biais du rôle qui leur a été attribué.	Le contrôle d'accès est un élément fondamental pour obtenir le niveau de sécurité requis. Grâce à des fonctions telles que RBAC, vous avez la possibilité de déterminer qui peut accéder aux données et dans quelle mesure. Cette option réduit les vulnérabilités et les abus, y compris les fuites de données et l'escalade de privilèges.
Vérification multiadministrateur	La vérification multiadministrateur empêche un seul administrateur du cluster d'exécuter des commandes sensibles telles que la « suppression d'une Snapshot de volume » ou une « suppression de volume » sans l'approbation d'un ou plusieurs administrateurs.	La vérification multiadministrateur empêche les administrateurs malveillants ou les comptes administrateur qui représentent un risque de détruire des données précieuses. Cette fonctionnalité d'ONTAP est essentielle pour renforcer l'environnement Zéro confiance centré sur les données.
Connecteur antivirus (analyse antivirus)	L'analyse antivirus est réalisée sur des serveurs Vscan qui abritent à la fois le connecteur antivirus et le logiciel antivirus. Généralement, le système sur lequel s'exécute ONTAP est configuré de manière à analyser les fichiers lorsqu'ils sont lus ou modifiés par un client.	Les vecteurs de menaces et d'attaques ne cessent de se multiplier. Par conséquent, l'analyse antivirus à la volée des fichiers lus ou modifiés protège l'intégrité des fichiers de l'entreprise.

Fonctions de sécurité d'ONTAP

Logiciel ou fonctionnalités	Fonction	Impact
Bannières de connexion et MOTD	Les bannières de connexion sont affichées à l'écran avant l'authentification. Elles permettent à l'entreprise et aux administrateurs de communiquer avec les utilisateurs du système.	Les bannières de connexion permettent à l'entreprise de présenter aux opérateurs, administrateurs, voire aux utilisateurs malveillants, les conditions d'utilisation d'un système. Elles indiquent également qui est autorisé à accéder au système.
Nettoyage de disque	Le nettoyage de disque vous permet de supprimer les données d'un disque ou d'un ensemble de disques de manière à ce qu'elles ne puissent jamais être restaurées.	Les protocoles de sécurité exigent généralement que les données supprimées du disque soient irrécupérables. La fonction de nettoyage de disque offre cette possibilité.