Activez le modèle « zéro confiance »

ONTAP 9

NetApp
July 12, 2024

Sommaire

Activez le modèle « zéro confiance »

NetApp et le modèle « zéro confiance »

La solution « zéro confiance » s'est traditionnellement orientée réseau pour structurer les microsegments et le périmètre (MCAP) afin de protéger les données, les services, les applications ou les ressources grâce à des contrôles appelés « passerelle de segmentation ». NetApp ONTAP adopte une approche « zéro confiance » centrée sur les données, dans laquelle le système de gestion du stockage devient la passerelle de segmentation pour protéger et surveiller l'accès aux données de nos clients. Le moteur « zéro confiance » FPolicy et l'écosystème de partenaires FPolicy deviennent un centre de contrôle pour obtenir une compréhension détaillée des modèles d'accès aux données normaux et aberrants et identifier les menaces internes.

À partir de juillet 2024, le contenu du rapport technique *TR-4015: NetApp et Zero Trust: Activation d'un modèle Zero Trust axé sur les données*, précédemment publié en format PDF, a été intégré au reste de la documentation produit de ONTAP.

Les données constituent les ressources les plus importantes de votre entreprise. Selon le 2022 , les menaces internes sont la cause de 18 % des violations de données "Rapport d'enquête sur les violations de données Verizon". Les entreprises peuvent améliorer leur vigilance en déployant des contrôles « zéro confiance » de pointe sur les données à l'aide du logiciel de gestion des données NetApp ONTAP.

Qu'est-ce que le principe zéro confiance ?

Le modèle « zéro confiance » a d'abord été développé par "John Kindervag" chez Forrester Research. Le service informatique envisage la sécurité du réseau de l'intérieur vers l'extérieur plutôt que de l'extérieur vers l'intérieur. L'approche « zéro confiance » de l'intérieur identifie un micronoyau et un périmètre (MCAP). Le MCAP est une définition intérieure des données, des services, des applications et des ressources à protéger avec un ensemble complet de contrôles. Le concept de périmètre extérieur sécurisé est obsolète. Les entités fiables et autorisées à s'authentifier avec succès via le périmètre peuvent alors rendre l'organisation vulnérable aux attaques. Les initiés, par définition, sont déjà à l'intérieur du périmètre sécurisé. Les employés, les collaborateurs, les collaborateurs et les partenaires sont des initiés, et ils doivent être autorisés à opérer avec des contrôles appropriés pour remplir leurs rôles dans l'infrastructure de votre entreprise.

Zéro confiance a été mentionné comme une technologie qui offre une promesse au DoD en septembre 2019 "FY19-23 Stratégie de modernisation numérique du Département de la Défense des États-Unis". Le modèle « zéro confiance » est défini comme « Une stratégie de cybersécurité qui intègre la sécurité dans l'ensemble de l'architecture dans le but d'enrayer les fuites de données. Ce modèle de sécurité centré sur les données élimine l'idée de réseaux, périphériques, rôles ou processus fiables ou non approuvés, et passe à des niveaux de confiance basés sur plusieurs attributs qui activent des stratégies d'authentification et d'autorisation dans le concept d'accès le moins privilégié. Pour mettre en œuvre la technologie « zéro confiance », il est nécessaire de repenser la façon dont nous utilisons l'infrastructure existante pour mettre en œuvre la sécurité en simplifiant et en améliorant l'efficacité tout en assurant la continuité des opérations. »

En août 2020, le NIST a publié "Architecture Zero Trust Pub 800-207 spéciale" (ZTA). ZTA se concentre sur la protection des ressources, et non des segments de réseau, car l'emplacement du réseau n'est plus considéré comme le composant principal de la posture de sécurité de la ressource. Les ressources sont des données et de l'informatique. Les stratégies ZTA sont destinées aux architectes de réseaux d'entreprise. ZTA présente une nouvelle terminologie issue des concepts originaux de Forrester. Les mécanismes de protection appelés

le point de décision de la politique (PDP) et le point d'application de la politique (PEP) sont analogues à une passerelle de segmentation Forrester. ZTA présente quatre modèles de déploiement :

- Déploiement basé sur un agent ou une passerelle
- Déploiement basé sur l'enclave (un peu similaire au MCAP de Forrester)
- Déploiement sur portail de ressources
- Sandbox d'application de périphérique

Pour les besoins de cette documentation, nous utilisons les concepts et la terminologie de Forrester Research plutôt que le NIST ZTA.

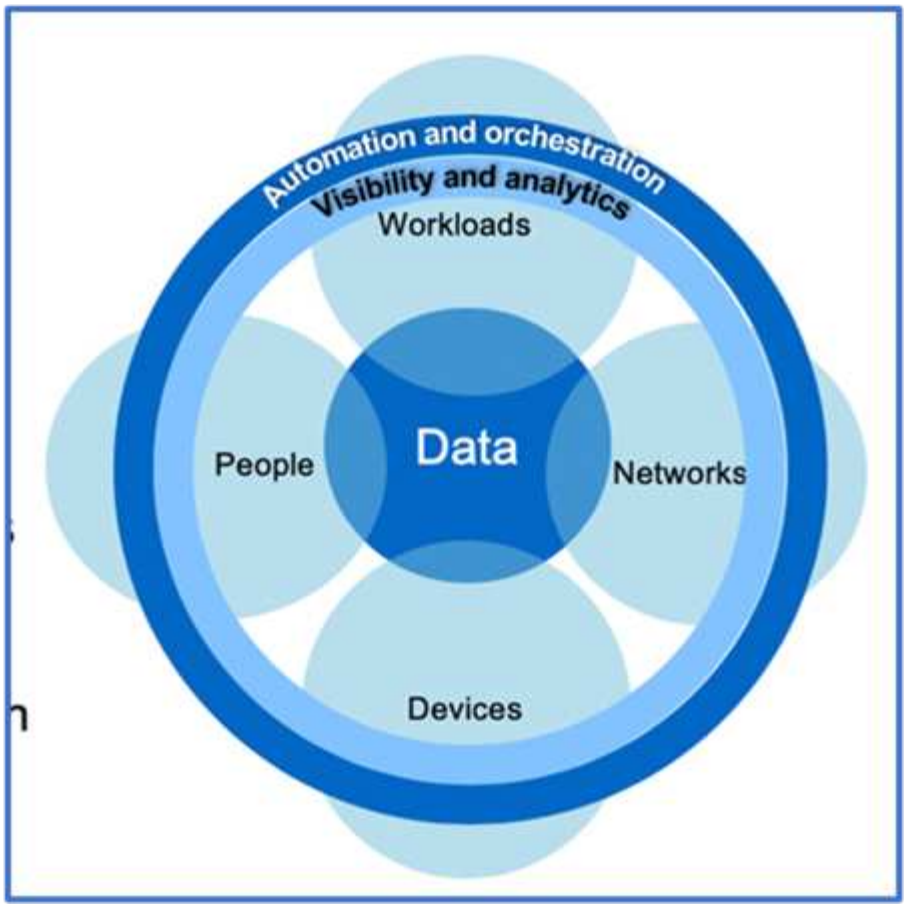
Ressources de sécurité

Pour plus d'informations sur le signalement de vulnérabilités et d'incidents, les réponses de sécurité NetApp et la confidentialité des clients, consultez le "Portail de sécurité NetApp".

Concevez une approche « zéro confiance » centrée sur les données avec ONTAP

Un réseau « zéro confiance » est défini par une approche centrée sur les données dans laquelle les contrôles de sécurité doivent être aussi proches que possible des données. Les fonctionnalités de ONTAP, associées à l'écosystème de partenaires NetApp FPolicy, peuvent fournir les contrôles nécessaires au modèle « zéro confiance » centré sur les données.

ONTAP est le logiciel de gestion des données riche en fonctions de sécurité de NetApp, et le moteur « zéro confiance » FPolicy est une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire et basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP.



Concevez un MCAP « zéro confiance » centré sur les données

Pour concevoir un MCAP Zero Trust axé sur les données, procédez comme suit :

1. Identifiez l'emplacement de toutes les données de l'entreprise.
2. Classez vos données.
3. Supprimez en toute sécurité les données dont vous n'avez plus besoin.
4. Comprendre quels rôles doivent avoir accès aux classifications de données.
5. Appliquez le principe du privilège minimum pour appliquer les contrôles d'accès.
6. Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données.
7. Utilisez le chiffrement pour les données au repos et en transit.
8. Contrôlez et consignez tous les accès.
9. Alertez les accès suspects ou les comportements à adopter.

Identifiez l'emplacement de toutes les données de l'entreprise

La fonctionnalité FPolicy de ONTAP associée à l'écosystème de partenaires Alliance NetApp de FPolicy vous permet d'identifier l'emplacement des données de votre entreprise et les personnes qui y ont accès. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. Pour plus d'informations sur l'analyse comportementale des utilisateurs, reportez-vous à la section contrôle et journalisation de tous les accès. Si vous ne comprenez pas où se trouvent vos données et qui y a accès, l'analyse comportementale des utilisateurs peut fournir une base pour établir une classification et une politique à partir d'observations empiriques.

Classez vos données

Dans la terminologie du modèle zéro confiance, la classification des données implique l'identification des données toxiques. Les données toxiques sont des données sensibles qui ne sont pas destinées à être exposées à l'extérieur d'une organisation. La divulgation de données toxiques peut contrevenir aux règlements et nuire à la réputation d'une entreprise. En termes de conformité réglementaire, les données toxiques incluent les données de titulaire de carte pour l' "Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS)", les données personnelles pour l' UE "Règlement général sur la protection des données (RGPD)"ou les données de santé pour l' "Loi américaine sur la transférabilité et la responsabilité en matière d'assurance maladie (HIPAA)". Utilisez NetApp "Classification BlueXP" (anciennement Cloud Data Sense), un kit d'outils piloté par l'IA, pour analyser, analyser et catégoriser automatiquement vos données.

Supprimez les données dont vous n'avez plus besoin en toute sécurité

Une fois les données de votre entreprise classifiées, vous pouvez découvrir que certaines de vos données ne sont plus nécessaires ou pertinentes pour le fonctionnement de votre entreprise. La conservation de données inutiles est une responsabilité et ces données doivent être supprimées. Pour obtenir un mécanisme avancé d'effacement cryptographique des données, consultez la description de la suppression sécurisée dans le chiffrement des données au repos.

Comprendre quels rôles doivent avoir accès aux classifications de données et appliquer le principe du privilège minimum pour appliquer les contrôles d'accès

Mapper l'accès aux données sensibles et appliquer le principe du privilège minimum implique de donner aux personnes de votre entreprise l'accès aux seules données requises pour accomplir leur travail. Ce processus implique le contrôle d'accès basé sur les rôles ("RBAC"), qui s'applique à l'accès aux données et à l'accès administratif.

Avec ONTAP, un SVM (Storage Virtual machine) peut être utilisé pour segmenter l'accès aux données de l'entreprise par les locataires au sein d'un cluster ONTAP. Le RBAC peut être appliqué à l'accès aux données ainsi qu'à l'accès administratif à la SVM. Le RBAC peut également être appliqué au niveau administratif du cluster.

En plus de RBAC, vous pouvez utiliser ONTAP "vérification multiadministrateur" (MAV) pour demander à un ou plusieurs administrateurs d'approuver des commandes telles que `volume delete` ou `volume snapshot delete`. Une fois MAV activé, la modification ou la désactivation de MAV nécessite l'approbation de l'administrateur MAV.

ONTAP est une autre façon de protéger les copies Snapshot "Verrouillage des copies Snapshot". Le verrouillage des copies Snapshot est une fonctionnalité SnapLock qui permet de rendre les copies Snapshot indélébiles, manuellement ou automatiquement, avec une période de conservation définie sur la règle de copie Snapshot du volume. Le verrouillage des copies Snapshot est également appelé verrouillage inviolable des copies Snapshot. L'objectif du verrouillage des copies Snapshot est d'empêcher les administrateurs peu scrupuleux ou non approuvés de supprimer les copies Snapshot sur les systèmes ONTAP primaires et secondaires. Il est possible d'effectuer une restauration rapide des copies Snapshot verrouillées sur des systèmes primaires afin de restaurer les volumes corrompus par des ransomwares.

Utilisez l'authentification multifacteur pour l'accès administratif et l'accès aux données

Outre le RBAC d'administration de cluster, "Authentification multifacteur (MFA)" peut être déployé pour l'accès administratif web ONTAP et l'accès à la ligne de commande SSH (Secure Shell). L'authentification multifacteur en matière d'accès administratif est obligatoire pour les organisations du secteur public américain ou celles qui doivent suivre la norme PCI-DSS. L'authentification multifacteur empêche un attaquant de compromettre un compte en utilisant uniquement un nom d'utilisateur et un mot de passe. L'authentification MFA nécessite au moins deux facteurs indépendants. Un exemple d'authentification à deux facteurs est quelque chose qu'un

utilisateur possède, comme une clé privée, et quelque chose qu'un utilisateur sait, comme un mot de passe. L'accès administratif Web à ONTAP System Manager ou à ActiveIQ Unified Manager est activé par le langage SAML (Security assertion Markup Language) 2.0. L'accès en ligne de commande SSH utilise une authentification à deux facteurs chaînée avec une clé publique et un mot de passe.

Vous pouvez contrôler l'accès des utilisateurs et des machines via des API dotées des fonctionnalités de gestion des identités et des accès de ONTAP :

- Utilisateur :
  - **Authentification et autorisation.** Grâce aux fonctionnalités de protocole NAS pour SMB et NFS.
  - **Vérification.** Syslog d'accès et d'événements. Une journalisation d'audit détaillée du protocole CIFS pour tester les règles d'authentification et d'autorisation. Audit précis et granulaire de l'accès NAS détaillé dans FPolicy au niveau des fichiers.
- Périphérique :
  - **Authentification.** Authentification basée sur certificat pour l'accès à l'API.
  - **Autorisation.** Contrôle d'accès basé sur des rôles (RBAC) par défaut ou personnalisé.
  - **Vérification.** Syslog de toutes les actions entreprises.

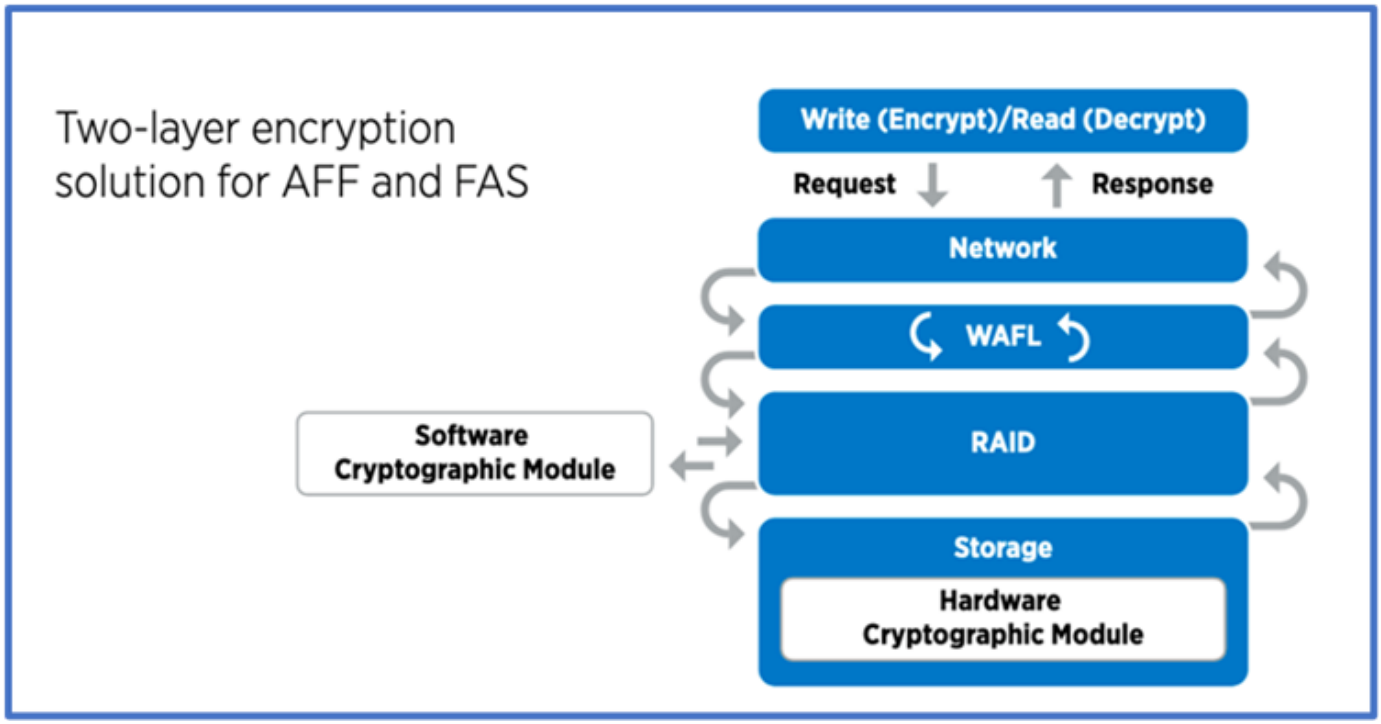
Utilisez le chiffrement pour les données au repos et en transit

Chiffrement des données au repos

Chaque jour, lorsqu'une entreprise réutilise des disques, renvoie des disques défectueux ou effectue des mises à niveau vers des disques de plus grande capacité, elle doit satisfaire de nouvelles exigences afin de réduire les risques liés aux systèmes de stockage et les écarts d'infrastructure. En tant qu'administrateurs et opérateurs de ressources de données, les ingénieurs du stockage doivent gérer et maintenir les données en toute sécurité tout au long de leur cycle de vie. "Chiffrement de stockage NetApp (NSE) ;#44 ; NetApp Volume Encryption (NVE) ;#44 ; et chiffrement d'agrégat NetApp" vous aider à chiffrer toutes vos données au repos en permanence, qu'elles soient toxiques ou non, et sans affecter les opérations quotidiennes. "NSE" Est une solution matérielle ONTAP de données au repos qui utilise des disques à autochiffrement validés conformes à la norme FIPS 140-2 de niveau 2. "NVE et NAE" Sont une solution logicielle de données au repos ONTAP qui utilise le "Module cryptographique NetApp conforme à la norme FIPS 140-2 de niveau 1". Avec NVE et NAE, vous pouvez utiliser des disques durs ou des disques SSD pour le chiffrement des données au repos. De plus, les disques NSE peuvent être utilisés pour fournir une solution de chiffrement à plusieurs couches native qui assure la redondance du chiffrement et une sécurité supplémentaire. Si l'une des couches est rompue, la seconde couche sécurise toujours les données. Ces fonctionnalités font de ONTAP une solution bien positionnée pour "chiffrement prêt pour le quantum".

NVE propose également une fonctionnalité appelée "suppression sécurisée" qui supprime de manière cryptographique les données toxiques des fuites de données lorsque les fichiers sensibles sont écrits sur un volume non classifié.

Soit le "Gestionnaire de clés intégré Onboard Key Manager (OKM)", qui est le gestionnaire de clés intégré à ONTAP, soit un "approuvée" tiers "gestionnaires de clés externes" peut être utilisé avec NSE et NVE pour stocker des clés en toute sécurité.



Comme le montre la figure ci-dessus, le chiffrement matériel et logiciel peut être combiné. Cette fonctionnalité a permis à l' "Validation de ONTAP dans les solutions commerciales de la NSA pour le programme classifié" de stocker des données les plus secrètes.

Chiffrement des données à la volée

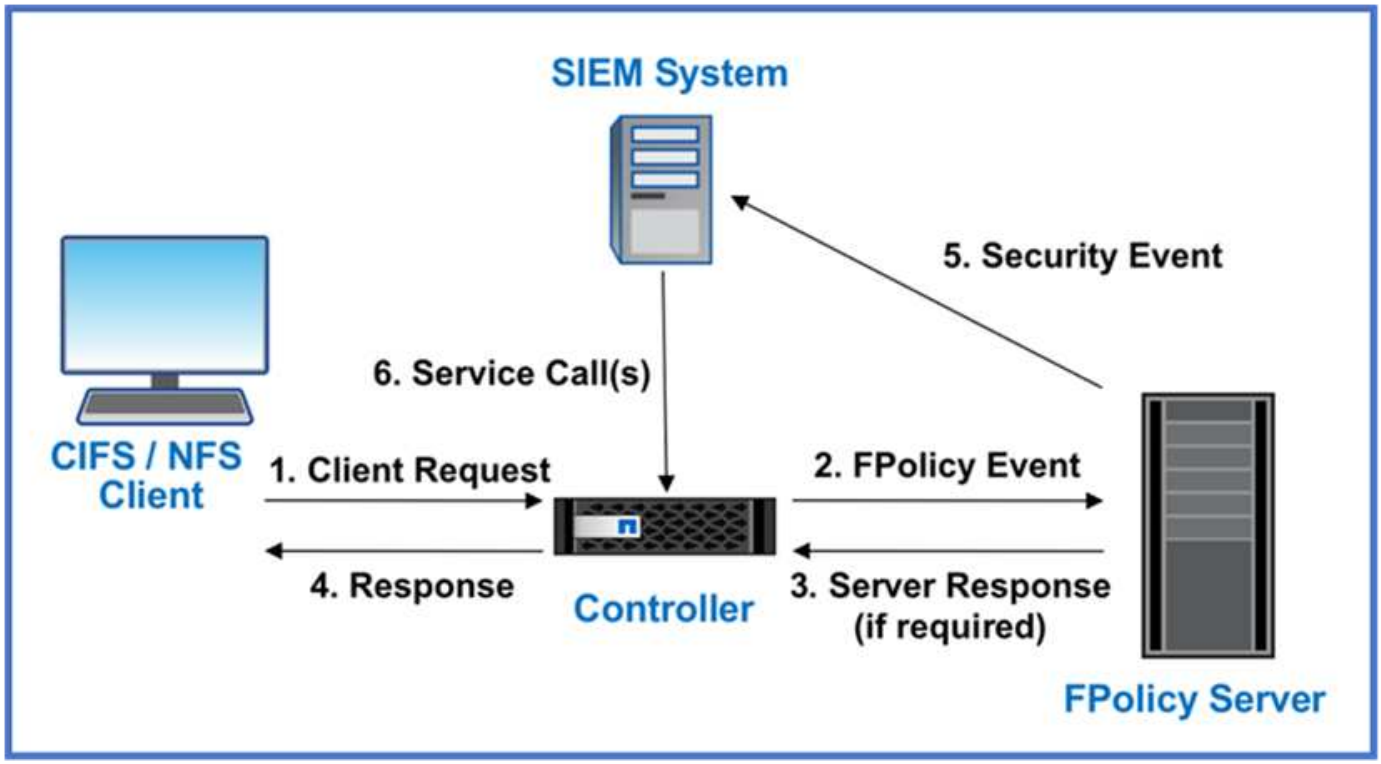
Le chiffrement des données à la volée ONTAP protège l'accès aux données utilisateur et l'accès au plan de contrôle. L'accès aux données utilisateur peut être chiffré par chiffrement SMB 3.0 pour l'accès aux partages Microsoft CIFS ou par krb5P pour NFS Kerberos 5. L'accès aux données utilisateur peut également être chiffré avec "IPSec" pour CIFS, NFS et iSCSI. L'accès au plan de contrôle est chiffré avec TLS (transport Layer Security). ONTAP fournit "FIPS" le mode de conformité pour l'accès au plan de contrôle, qui active les algorithmes approuvés FIPS et désactive les algorithmes non approuvés FIPS. La réplication des données est chiffrée avec "chiffrement des pairs de cluster". Cela assure le cryptage pour les technologies ONTAP SnapVault et SnapMirror.

Contrôlez et consignez tous les accès

Une fois les règles RBAC en place, vous devez déployer des fonctionnalités actives de surveillance, d'audit et d'alerte. Le moteur « zéro confiance » FPolicy de NetApp ONTAP, couplé au "Écosystème de partenaires NetApp FPolicy", fournit les contrôles nécessaires au modèle « zéro confiance » centré sur les données. NetApp ONTAP est un logiciel de gestion des données riche en fonctions de sécurité. Il "FPolicy" s'agit d'une fonctionnalité ONTAP de pointe qui offre une interface de notification d'événements granulaire basée sur des fichiers. Les partenaires NetApp FPolicy peuvent utiliser cette interface pour obtenir un niveau d'éclairage plus élevé de l'accès aux données dans ONTAP. La fonctionnalité FPolicy de ONTAP, associée à l'écosystème de partenaires Alliance NetApp de FPolicy, vous permet d'identifier l'emplacement et l'accès aux données de votre entreprise. Cette opération est effectuée à l'aide d'une analyse comportementale des utilisateurs qui identifie si les modèles d'accès aux données sont valides. L'analyse comportementale des utilisateurs peut être utilisée pour alerter l'utilisateur en cas d'accès aux données suspect ou aberrant qui ne correspond pas au modèle normal et, si nécessaire, prendre des mesures pour refuser l'accès.

Les partenaires FPolicy vont au-delà de l'analyse comportementale des utilisateurs et s'orientent vers le machine learning (ML) et l'intelligence artificielle (IA) pour assurer la fidélité des événements et réduire le nombre de faux positifs, voire de faux positifs. Tous les événements doivent être consignés sur un serveur

syslog ou sur un système de gestion des informations et des événements de sécurité (SIEM) pouvant également utiliser le ML et l'IA.



La solution Storage Workload Security de NetApp (anciennement appelée "Cloud Secure") utilise l'interface FPolicy et l'analytique comportementale des utilisateurs sur les systèmes de stockage ONTAP dans le cloud et sur site pour vous fournir des alertes en temps réel sur les comportements malveillants des utilisateurs. Storage Workload Security protège les données de l'entreprise contre les activités abusives ou les usurpations d'identité à l'aide de fonctionnalités avancées de machine learning et de détection des anomalies. Storage Workload Security : identifie les attaques par ransomware ou d'autres comportements malveillants, invoque les copies Snapshot et met en quarantaine les utilisateurs malveillants. Storage Workload Security dispose également d'une fonctionnalité d'analyse permettant de visualiser en détail les activités des utilisateurs et des entités. La sécurité des workloads de stockage fait partie de NetApp Cloud Insights.

Outre la sécurité des workloads de stockage, ONTAP dispose d'une fonctionnalité intégrée de détection des ransomwares appelée "Protection autonome contre les ransomwares" ARP. ARP utilise le machine learning pour déterminer si une activité anormale sur les fichiers indique qu'une attaque par ransomware est en cours, puis appelle une copie Snapshot et une alerte aux administrateurs. Storage Workload Security s'intègre à ONTAP pour recevoir des événements ARP et fournit une couche supplémentaire d'analytique et de réponses automatiques.

Contrôles d'orchestration et d'automatisation de la sécurité NetApp externes à ONTAP

L'automatisation vous permet d'effectuer un processus ou une procédure avec une assistance humaine minimale. L'automatisation permet aux entreprises d'étendre les déploiements « zéro confiance » bien au-delà des procédures manuelles pour se défendre contre les activités imcretes également automatisées.

Ansible est un outil open source de provisionnement logiciel, de gestion de la configuration et de déploiement des applications. Il fonctionne sur de nombreux systèmes Unix et peut configurer à la fois les systèmes Unix et

Microsoft Windows. Il comprend son propre langage déclaratif pour décrire la configuration du système. Ansible a été écrit par Michael DeHaan et acquis par Red Hat en 2015. Ansible se connecte temporairement à distance sans agent via SSH ou Windows Remote Management (permettant l'exécution à distance de PowerShell). NetApp a développé plus de "150 modules Ansible pour le logiciel ONTAP", permettant une intégration supplémentaire avec la structure d'automatisation Ansible. Les modules Ansible pour NetApp fournissent un ensemble d'instructions sur la manière de définir l'état souhaité et de le relayer vers l'environnement NetApp cible. Les modules sont conçus pour prendre en charge des tâches telles que la configuration de licences, la création d'agrégats et de machines virtuelles de stockage, la création de volumes et la restauration de snapshots, pour n'en nommer que quelques-uns. Un rôle Ansible a été "Publié sur GitHub" spécifique au guide de déploiement des fonctionnalités unifiées du Ministère de la Défense NetApp.

Avec la bibliothèque de modules disponibles, les utilisateurs peuvent facilement développer des playbooks Ansible et les personnaliser en fonction de leurs propres applications et des besoins de l'entreprise pour automatiser des tâches courantes. Une fois qu'un PlayBook est écrit, vous pouvez l'exécuter pour exécuter la tâche spécifiée, ce qui permet de gagner du temps et d'améliorer la productivité. NetApp a créé et partagé des exemples de playbooks pouvant être utilisés directement ou personnalisés en fonction de vos besoins.

Cloud Insights est un outil de surveillance de l'infrastructure qui permet de bénéficier d'une grande visibilité sur l'ensemble de l'infrastructure. Avec Cloud Insights, vous pouvez surveiller et optimiser toutes les ressources et résoudre les problèmes, y compris dans les instances de cloud public et dans vos data centers privés. Cloud Insights réduit le délai moyen de résolution de 90 % et empêche 80 % des problèmes cloud d'affecter les utilisateurs finaux. Il permet également de réduire de 33 % en moyenne les coûts de l'infrastructure cloud et de réduire l'exposition aux menaces internes en protégeant les données à l'aide d'informations exploitables. La fonctionnalité de sécurité des workloads de stockage d'Cloud Insights permet d'analyser le comportement des utilisateurs avec l'IA et LE ML afin d'alerter les utilisateurs en cas de comportements anormaux liés à une menace interne. Pour ONTAP, Storage Workload Security utilise le moteur FPolicy « zéro confiance ».

Zero Trust et déploiements de cloud hybride

NetApp est la référence en matière de gestion des données dans le cloud hybride

NetApp propose diverses options d'extension des systèmes de gestion des données sur site au cloud hybride avec Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) et les principaux fournisseurs. Les solutions de cloud hybride NetApp prennent en charge les mêmes contrôles de sécurité « zéro confiance » que ceux disponibles avec les systèmes ONTAP sur site et le stockage Software-defined ONTAP Select.

Vous pouvez facilement étendre la capacité des clouds publics sans contraintes classiques de dépenses d'investissement en utilisant NetApp Cloud Volumes Service, le premier service de fichiers cloud haute performance pour AWS et GCP, et Azure NetApp Files pour Microsoft Azure. Idéales pour les charges de travail qui exploitent les données de manière intensive, telles que l'analytique et le DevOps, ces services cloud associent un stockage à la demande flexible de NetApp à la gestion des données ONTAP dans une offre entièrement gérée.

Pour ceux qui recherchent des services de données avancés pour les services de stockage bloc dans le cloud ou objet, tels que AWS EBS et S3 ou le stockage Azure, Cloud Volumes ONTAP assure la gestion des données entre votre environnement sur site et le cloud public avec une seule vue commune. Exécuté dans AWS ou Azure en tant qu'instance à la demande, Cloud Volumes ONTAP fournit l'efficacité du stockage, la disponibilité et l'évolutivité du logiciel ONTAP. ONTAP permet de déplacer les données entre vos systèmes ONTAP sur site et votre environnement de stockage AWS ou Azure grâce au logiciel de réplication des données NetApp SnapMirror.

En savoir plus sur le contenu ONTAP « zéro confiance »

Pour en savoir plus sur les informations fournies dans le contenu ONTAP « zéro confiance », consultez ces documents et/ou sites web :

- "Rapport d'enquête sur les violations de données Verizon"
- "Stratégie de modernisation numérique du Ministère de la défense"
- "Architecture « zéro confiance » NIST SP 800-207"
- "Répertoire de partenaires NetApp : partenaires alliance de sécurité"
- "Utilisation de FPolicy pour le contrôle et la gestion des fichiers sur les SVM"
- "PCI-DSS 3.2 ONTAP 9"
- "Règlement général sur la protection des données (RGPD)"
- "Résumé de la règle de confidentialité HIPPA"
- "Classification de NetApp BlueXP"
- "Vérification multi-administrateurs"
- "Verrouillage inviolable des copies Snapshot"
- "Authentification multifacteur dans ONTAP 9"
- "NetApp Storage Encryption, disques avec autocryptage NVMe, NetApp Volume Encryption et NetApp Aggregate Encryption"
- "NetApp Storage Encryption"
- "NetApp Volume Encryption et chiffrement d'agrégat NetApp"
- "Certificat de module cryptographique NetApp FIPS-140-2"
- "Chiffrement des données au repos Quantum Ready par NetApp"
- "La sécurité au service de l'innovation : NetApp et Ontrack remportent le prix Flash Memory Summit"
- "Activation de la gestion intégrée des clés"
- "Matrice d'interopérabilité NetApp"
- "Configuration de la gestion externe des clés"
- "Solutions commerciales pour les applications classées"
- "IPSec ONTAP"
- "La configuration de sécurité est modifiée pour activer le mode FIPS"
- "Activation du chiffrement de peering de cluster sur une relation entre pairs existante"
- "Sécurité des workloads de stockage (Cloud Secure)"
- "Commencez à automatiser vos workflows de développement avec NetApp et Ansible"
- "Module Ansible spécifique au guide de déploiement des fonctionnalités unifiées du Ministère de la Défense NetApp"
- "Authentification administrateur et RBAC"
- "Chiffrement des données au repos ONTAP"
- "Tr-4569 Guide de renforcement de la sécurité pour NetApp ONTAP 9"

Informations sur le copyright

Informations sur les marques commerciales