Zero-Trust-Modell aktivieren

ONTAP 9

NetApp
July 12, 2024

Inhalt

Zero-Trust-Modell aktivieren

NetApp und Zero Trust

Zero Trust war bisher ein netzwerkorientierter Ansatz der Architektur von Microcore and Perimeter (MCAP) zum Schutz von Daten, Services, Applikationen oder Assets mit Kontrolloptionen, die als Segmentierungsgateway bekannt sind. NetApp ONTAP verfolgt bei der Zero-Trust-Strategie einen Daten-orientierten Ansatz, bei dem das Storage-Managementsystem zum Segmentierungs-Gateway wird, um die Daten unserer Kunden zu schützen und den Zugriff darauf zu überwachen. Insbesondere die FPolicy Zero Trust Engine und das FPolicy Partner-Ecosystem werden zum Kontrollzentrum, um normale und fehlende Datenzugriffsmuster detailliert zu verstehen und Bedrohungen von innen zu erkennen.

Ab Juli 2024 wurde der Inhalt des technischen Berichts *TR-4015: NetApp and Zero Trust: Enabling a Data-Centric Zero Trust model*, das zuvor als PDF veröffentlicht wurde, in die restliche ONTAP Produktdokumentation integriert.

Ihre Daten sind die wichtigsten Ressourcen in Ihrem Unternehmen. Insider-Bedrohungen sind laut 2022 die Ursache von 18 % der Datenschutzverletzungen. "Verizon Data Breach Investigations Report" Die branchenführende Zero-Trust-Kontrolle rund um Ihre Daten mit der Datenmanagement-Software von NetApp ONTAP sorgt für eine erhöhte Wachsamkeit.

Was Ist Zero Trust?

Das Zero-Trust-Modell wurde zuerst von Forrester Research entwickelt "John Kindervag" . Sie sieht Netzwerksicherheit von innen nach außen statt von außen vor. Der Inside-Out Zero Trust-Ansatz identifiziert einen Microcore und Perimeter (MCAP). Bei MCAP handelt es sich um eine interne Definition von Daten, Services, Applikationen und Assets, die durch umfassende Kontrollen geschützt werden. Das Konzept eines sicheren äußeren Perimeters ist veraltet. Entitäten, denen eine vertrauenswürdige und erfolgreiche Authentifizierung über den Perimeter gestattet ist, können das Unternehmen dann anfällig für Angriffe machen. Insider befinden sich per Definition bereits innerhalb des sicheren Perimeters. Mitarbeiter, Auftragnehmer und Partner sind Insider und müssen für den Betrieb mit entsprechenden Kontrollmechanismen sorgen, um ihre Rollen innerhalb der Infrastruktur Ihres Unternehmens zu erfüllen.

Zero Trust wurde im September 2019 als eine Technologie genannt, die dem DoD Versprechen gibt "GJ19-23 DoD Strategie zur digitalen Modernisierung". Zero Trust ist Eine Cybersicherheitsstrategie, die in der gesamten Architektur Sicherheit einbettet, um Datenschutzverletzungen zu stoppen. Dieses datenorientierte Sicherheitsmodell beseitigt die Idee vertrauenswürdiger oder nicht vertrauenswürdiger Netzwerke, Geräte, Personas oder Prozesse und wechselt zu auf Multi-Attribut-basierten Vertrauensstufen, die Authentifizierungs- und Autorisierungsrichtlinien unter dem Begriff „Least Privileged Access“ ermöglichen. Um Zero Trust zu implementieren, müssen wir überdenken, wie wir die vorhandene Infrastruktur nutzen, um Sicherheit einfacher und effizienter zu implementieren und gleichzeitig einen ungehinderten Betrieb zu ermöglichen.“

Im August 2020 veröffentlichte der NIST "Spezielle Pub 800-207 Zero Trust-Architektur" (ZTA). ZTA konzentriert sich auf den Schutz von Ressourcen und nicht auf Netzwerksegmente, da der Standort des Netzwerks nicht mehr als Hauptkomponente der Sicherheitslage der Ressource angesehen wird. Ressourcen sind Daten und Computing. ZTA-Strategien sind für Enterprise Network Architects. ZTA führt einige neue Terminologie aus den ursprünglichen Forrester-Konzepten ein. Sicherungsmechanismen, die als Policy Decision Point (PDP) und Policy Enforcement Point (PEP) bezeichnet werden, sind analog zu einem Forrester

Segmentierungs-Gateway. ZTA stellt vier Implementierungsmodelle vor:

- Geräte-Agent- oder Gateway-basierte Bereitstellung
- Enclave-basierte Implementierung (entspricht in etwa dem Forrester MCAP)
- Portalbasierte Implementierung von Ressourcen
- Geräteanwendung Sandbox

Für die Zwecke dieser Dokumentation verwenden wir Konzepte und Terminologie von Forrester Research und nicht die NIST ZTA.

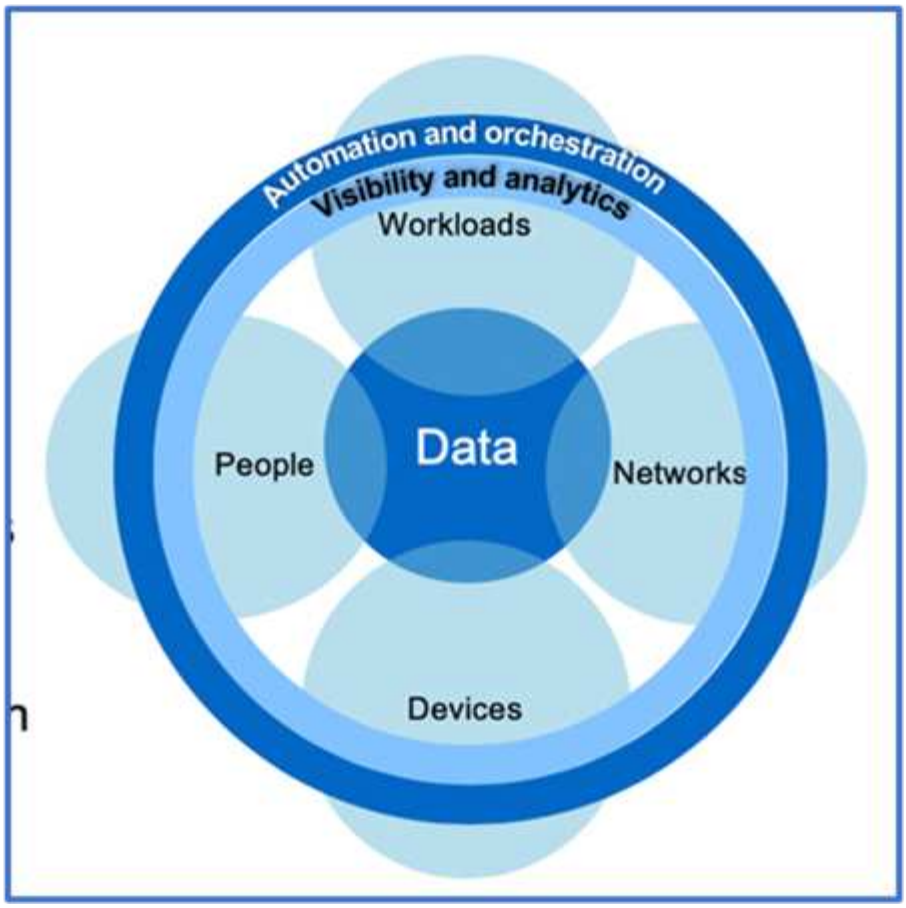
Sicherheitsressourcen

Informationen zur Meldung von Schwachstellen und Vorfällen, NetApp Sicherheitsreaktionen und Vertraulichkeit der Kundenvertraulichkeit finden Sie im "Sicherheitsportal von NetApp".

Entwerfen eines datenorientierten Ansatzes für Zero Trust mit ONTAP

Ein Zero-Trust-Netzwerk wird durch einen datenorientierten Ansatz definiert, bei dem die Sicherheitskontrollen so nah wie möglich an den Daten sein sollten. Die Funktionen von ONTAP in Kombination mit dem NetApp FPolicy Partner-Ecosystem bieten die erforderlichen Kontrollen für das datenorientierte Zero-Trust-Modell.

ONTAP ist eine sicherheitsreiche Datenmanagement-Software von NetApp und die FPolicy Zero Trust Engine ist eine branchenführende ONTAP-Funktion, die eine granulare, dateibasierte Ereignisbenachrichtigung bietet. NetApp FPolicy Partner können diese Schnittstelle nutzen, um den Datenzugriff innerhalb von ONTAP besser zu nutzen.



Entwerfen Sie eine datenorientierte MCAP mit Zero Trust

Gehen Sie wie folgt vor, um einen datenorientierten Zero Trust MCAP zu entwickeln:

1. Ermitteln Sie den Standort aller Unternehmensdaten.
2. Daten klassifizieren:
3. Entsorgen Sie Daten, die Sie nicht mehr benötigen.
4. Welche Rollen sollten auf die Datenklassifizierungen zugreifen können?
5. Wenden Sie das Prinzip „Least Privilege“ an, um Zugriffskontrollen durchzusetzen.
6. Multi-Faktor-Authentifizierung für administrativen Zugriff und Datenzugriff
7. Verschlüsselung von Daten im Ruhezustand und aktiven Daten
8. Überwachen und protokollieren Sie den gesamten Zugriff.
9. Alarmieren Sie verdächtige Zugriffe oder Verhaltensweisen.

Ermitteln Sie den Standort aller Unternehmensdaten

Mit der FPolicy Funktion von ONTAP und dem NetApp Alliance Partner Ecosystem von FPolicy Partnern können Sie herausfinden, wo sich die Daten Ihres Unternehmens befinden und wer Zugriff auf sie hat. Dies erfolgt mithilfe von Benutzerverhaltensanalysen, die feststellen, ob Datenzugriffsmuster gültig sind. Weitere Details zu User Behavioral Analytics werden unter Überwachen und Protokollieren aller Zugriffe erläutert. Wenn Sie nicht verstehen, wo sich Ihre Daten befinden und wer Zugriff darauf hat, kann die Verhaltensanalyse von Benutzern als Grundlage für die Erstellung von Klassifizierungen und Richtlinien anhand empirischer Beobachtungen dienen.

Daten klassifizieren

In der Terminologie des Zero-Trust-Modells beinhaltet die Klassifizierung von Daten die Identifizierung toxischer Daten. Giftige Daten sind sensible Daten, die nicht außerhalb eines Unternehmens offengelegt werden sollen. Die Offenlegung giftiger Daten könnte die Einhaltung gesetzlicher Vorschriften verletzen und den Ruf eines Unternehmens schädigen. Im Hinblick auf die Einhaltung gesetzlicher Vorschriften umfassen toxische Daten Karteninhaberdaten für die , personenbezogene Daten für die "Payment Card Industry Data Security Standard (PCI-DSS)"EU "DSGVO (Datenschutz-Grundverordnung)"oder Gesundheitsdaten für die "Health Insurance Portability and Accountability Act (HIPAA)". Mit NetApp (ehemals Cloud Data Sense), einem KI-gestützten Toolkit, können "BlueXP Klassifizierung" Sie Ihre Daten automatisch scannen, analysieren und kategorisieren.

Entsorgen Sie Daten, die Sie nicht mehr benötigen

Nach der Klassifizierung Ihrer Unternehmensdaten stellen Sie möglicherweise fest, dass einige Ihrer Daten für die Funktion Ihres Unternehmens nicht mehr erforderlich oder relevant sind. Die Aufbewahrung unnötiger Daten ist eine Haftung, und diese Daten sollten gelöscht werden. Einen erweiterten Mechanismus zum kryptografischen Löschen von Daten finden Sie in der Beschreibung zum sicheren Löschen von Daten im Ruhezustand.

Verstehen Sie, welche Rollen auf die Datenklassifizierungen zugreifen sollten, und wenden Sie das Prinzip der geringsten Berechtigungen an, um Zugriffskontrollen durchzusetzen

Das Zuordnen von Zugriff auf sensible Daten und die Anwendung des Prinzips der geringsten Rechte bedeutet, dass Mitarbeiter in Ihrem Unternehmen nur auf die Daten zugreifen können, die für die Ausführung ihrer Aufgaben erforderlich sind. Dieser Prozess beinhaltet eine rollenbasierte Zugriffssteuerung ("RBAC", die für den Datenzugriff und administrativen Zugriff gilt.

Mit ONTAP kann eine Storage Virtual Machine (SVM) verwendet werden, um den Zugriff auf Unternehmensdaten durch Mandanten innerhalb eines ONTAP Clusters zu segmentieren. RBAC kann sowohl auf den Datenzugriff als auch auf den administrativen Zugriff auf die SVM angewendet werden. RBAC kann auch auf der Cluster-Administrationsebene angewendet werden.

Zusätzlich zu RBAC können Sie ONTAP (MAV) verwenden "Verifizierung durch mehrere Administratoren" , damit ein oder mehrere Administratoren Befehle wie oder genehmigen müssen `volume delete` `volume snapshot delete`. Wenn MAV aktiviert ist, muss MAV durch Ändern oder Deaktivieren der MAV-Administratorfreigabe genehmigt werden.

Eine weitere Möglichkeit zum Schutz von Snapshot Kopien ist ONTAP "Sperren von Snapshot-Kopien". Sperrung von Snapshot Kopien ist eine SnapLock Funktion. Hier sind Snapshots nicht mehr manuell oder automatisch löschbar dank einer Aufbewahrungsfrist für Snapshot Kopien des Volumes. Snapshot Kopien werden auch als manipulationssichere Sperrung von Snapshot Kopien bezeichnet. Durch das Sperren von Snapshot Kopien sollen schädliche oder nicht vertrauenswürdige Administratoren daran gehindert werden, Snapshot Kopien auf primären und sekundären ONTAP Systemen zu löschen. Eine schnelle Recovery von gesperrten Snapshot Kopien auf Primärsystemen kann zur Wiederherstellung von Volumes durchgeführt werden, die durch Ransomware beschädigt sind.

Multi-Faktor-Authentifizierung für administrativen Zugriff und Datenzugriff

Zusätzlich zur Cluster-administrativen RBAC "Multi-Faktor-Authentifizierung (MFA)" kann für den ONTAP Web-administrativen Zugriff und den SSH-Zugriff (Secure Shell) über die Befehlszeile implementiert werden. MFA für administrativen Zugriff ist eine Voraussetzung für US-öffentliche Einrichtungen oder solche, die dem PCI-DSS folgen müssen. MFA macht es einem Angreifer unmöglich, ein Konto mit nur einem Benutzernamen und Passwort zu kompromittieren. MFA erfordert zwei oder mehr unabhängige Faktoren für die Authentifizierung. Ein Beispiel für eine zwei-Faktor-Authentifizierung ist etwas, das ein Benutzer besitzt, wie z. B. einen privaten

Schlüssel, und etwas, das ein Benutzer kennt, z. B. ein Kennwort. Administrativer Webzugriff auf ONTAP System Manager oder ActiveIQ Unified Manager wird über die SAML (Security Assertion Markup Language) 2.0 aktiviert. Bei SSH-Befehlszeilenzugriff wird eine verkettete zwei-Faktor-Authentifizierung mit einem öffentlichen Schlüssel und einem Kennwort verwendet.

Mit den Identitäts- und Zugriffsverwaltungsfunktionen von ONTAP können Sie den Benutzer- und Maschinenzugriff über APIs steuern:

- Benutzer:
  - **Authentifizierung und Autorisierung.** Über NAS-Protokollfunktionen für SMB und NFS.
  - **Audit.** Syslog für Zugriff und Ereignisse Detaillierte Audit-Protokollierung des CIFS-Protokolls zum Testen von Authentifizierungs- und Autorisierungsrichtlinien Fein abgestimmte FPolicy-Prüfung von detailliertem NAS-Zugriff auf Dateiebene
- Gerät:
  - **Authentifizierung.** Zertifikatbasierte Authentifizierung für API-Zugriff.
  - **Genehmigung.** Standardmäßige oder benutzerdefinierte rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)
  - **Audit.** Syslog aller durchgeführten Aktionen.

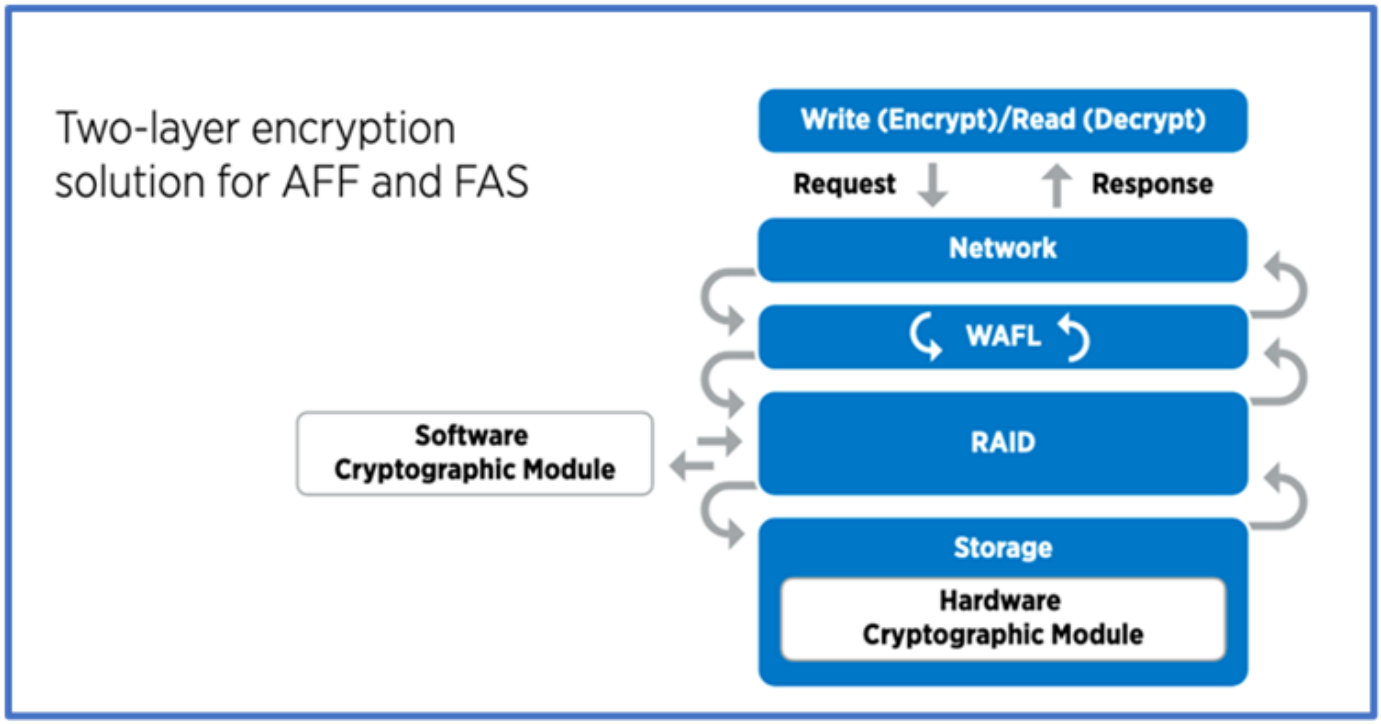
Verschlüsselung von Daten im Ruhezustand und aktiven Daten

Verschlüsselung von Daten im Ruhezustand

Jeden Tag gelten neue Anforderungen zur Minderung von Risiken für Storage-Systeme und Infrastrukturlücken, wenn ein Unternehmen Laufwerke wiederverwendet, defekte Laufwerke zurückgibt oder Upgrades auf größere Laufwerke durchführt, indem sie diese verkauft oder eintauschen. Von Storage Engineers wird in ihrer Rolle als Administratoren und Betreiber der Datenbestände erwartet, dass sie die Daten während ihres gesamten Lebenszyklus sicher managen und aufbewahren. "NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), NetApp Aggregate Encryption" Damit können Sie alle Ihre Daten im Ruhezustand jederzeit verschlüsseln – unabhängig davon, ob sie toxisch sind oder nicht, und ohne den täglichen Betrieb zu beeinträchtigen. "NSE" Es handelt sich um eine ONTAP Lösung für Hardware-Daten im Ruhezustand, die mit FIPS 140-2 Level 2 validierte Self-Encrypting Drives nutzt. "NVE und NAE" Sind eine ONTAP Software Data-at-Rest-Lösung, die auf die nutzt "Validiertes NetApp Cryptographic Module nach FIPS 140-2 Level 1". Mit NVE und NAE können entweder Festplatten oder Solid State Drives für die Verschlüsselung von Daten im Ruhezustand genutzt werden. Außerdem können NSE-Laufwerke verwendet werden, um eine native, mehrstufige Verschlüsselungslösung für Verschlüsselungsredundanz und zusätzliche Sicherheit bereitzustellen. Ist eine Schicht verletzt, sichert die zweite Schicht weiterhin die Daten. Dank dieser Funktionen ist ONTAP für "Quantum-fähige Verschlüsselung".

NVE bietet zudem eine Funktion namens „ "Sicheres Löschen" kryptografisch“ zur Beseitigung toxischer Daten bei Verschütten von Daten, wenn sensible Dateien auf ein nicht klassifiziertes Volume geschrieben werden.

Entweder der "Onboard Key Manager (OKM)"-Schlüsselmanager, der in ONTAP integriert ist, oder "Genehmigt" ein Drittanbieter "Externe Schlüsselmanager" kann mit NSE und NVE zum sicheren Speichern von Schlüsseln verwendet werden.



Wie in der Abbildung oben zu sehen ist, kann die Hardware- und softwarebasierte Verschlüsselung kombiniert werden. Diese Fähigkeit führte zu der, die die "Validierung von ONTAP in die kommerziellen Lösungen der NSA für das klassifizierte Programm" Speicherung von streng geheimen Daten ermöglicht.

Verschlüsselung von aktiven Daten

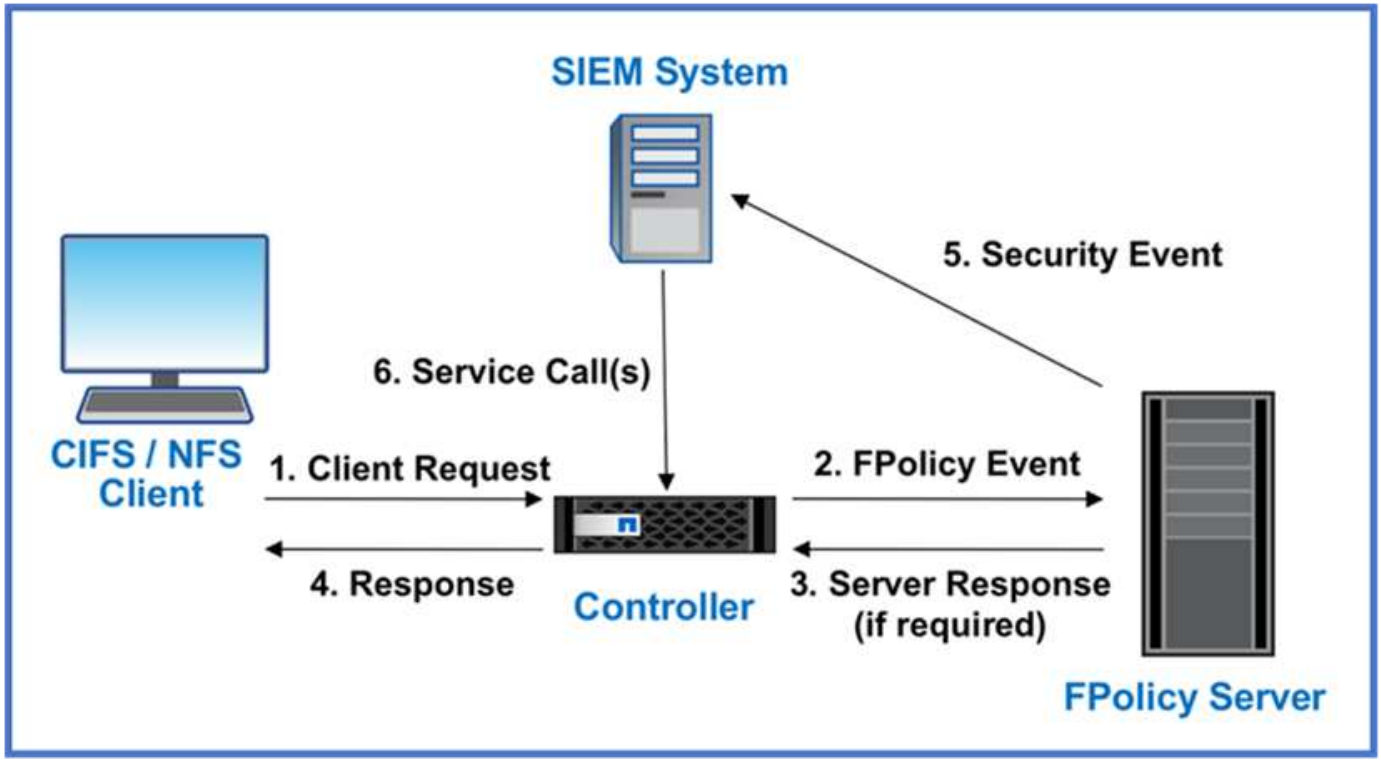
Die ONTAP Verschlüsselung von aktiven Daten sichert den Zugriff auf Benutzerdaten und Zugriff auf Kontrollebene. Der Benutzerdatenzugriff kann durch SMB 3.0-Verschlüsselung für den Zugriff auf Microsoft CIFS-Freigaben oder durch krb5P für NFS Kerberos 5 verschlüsselt werden. Der Zugriff auf Benutzerdaten kann auch mit für CIFS, NFS und iSCSI verschlüsselt werden "IPsec" . Der Zugriff auf die Kontrollebene wird mit Transport Layer Security (TLS) verschlüsselt. ONTAP bietet "FIPS" einen Compliance-Modus für den Zugriff auf die Kontrollebene, mit dem FIPS-genehmigte Algorithmen aktiviert und nicht FIPS-zertifizierte Algorithmen deaktiviert werden. Die Datenreplikation wird mit verschlüsselt "Cluster-Peer-Verschlüsselung". Dadurch wird Verschlüsselung für die ONTAP SnapVault und SnapMirror Technologien bereitgestellt.

Überwachen und protokollieren Sie den gesamten Zugriff

Nachdem die RBAC-Richtlinien festgelegt sind, müssen Sie aktive Monitoring-, Audit- und Warnfunktionen implementieren. Die FPolicy Zero-Trust-Engine von NetApp ONTAP bietet in Kombination mit dem die "Partner-Ecosystem von NetApp FPolicy"erforderlichen Kontrollen für das datenorientierte Zero-Trust-Modell. NetApp ONTAP ist eine sicherheitsrelevante Datenmanagement-Software und "FPolicy" eine branchenführende ONTAP-Funktion, die eine granulare, dateibasierte Ereignisbenachrichtigung bietet. NetApp FPolicy Partner können diese Schnittstelle nutzen, um den Datenzugriff innerhalb von ONTAP besser zu nutzen. Mit der FPolicy Funktion von ONTAP und dem NetApp Alliance Partner Ecosystem von FPolicy Partnern können Sie feststellen, wo sich die Daten Ihres Unternehmens befinden und wer Zugriff auf sie hat. Dies erfolgt mithilfe von Benutzerverhaltensanalysen, die feststellen, ob Datenzugriffsmuster gültig sind. Mithilfe von Analysen des Benutzerverhaltens lässt sich ein Alarm bei verdächtigem oder irridenem Datenzugriff erstellen, der nicht dem normalen Muster entspricht, und gegebenenfalls Maßnahmen ergreifen, um den Zugriff zu verweigern.

FPolicy-Partner gehen über die Verhaltensanalyse von Benutzern hinaus auf maschinelles Lernen (ML) und künstliche Intelligenz (KI) um, was zu mehr Ereignistreue und weniger, wenn überhaupt, falsche Positives führt. Alle Ereignisse sollten bei einem Syslog-Server oder bei einem SIEM-System (Security Information and

Event Management) protokolliert werden, das auch ML und KI einsetzen kann.



NetApp Storage Workload Security (ehemals bekannt als "Cloud Secure") nutzt die FPolicy Schnittstelle und Verhaltensanalysen für Benutzer sowohl in Cloud- als auch in lokalen ONTAP Storage-Systemen, um Ihnen Echtzeitwarnungen über bösartiges Benutzerverhalten zu geben. Dank erweitertem Machine Learning und Anomalieerkennung werden Unternehmensdaten vor Missbrauch durch böswillige oder kompromittierte Benutzer geschützt. Storage Workload Security kann Ransomware-Angriffe oder andere fehleranhaftende Verhaltensweisen identifizieren, Snapshot-Kopien aufrufen und böswillige Benutzer unter Quarantäne stellen. Storage Workload Security verfügt außerdem über eine forensische Funktion zur detaillierten Anzeige von Benutzer- und Entitäten. Storage-Workload-Sicherheit ist Teil von NetApp Cloud Insights.

Zusätzlich zur Sicherheit von Storage-Workloads verfügt ONTAP über eine integrierte Funktion zur Erkennung von Ransomware, die als (ARP) bekannt "Autonomer Schutz Durch Ransomware" ist. ARP ermittelt mithilfe von Machine Learning, ob anormale Dateiaktivitäten auf einen Ransomware-Angriff hindeuten. Außerdem ruft ARP eine Snapshot Kopie auf und warnt Administratoren. Storage Workload Security ist in ONTAP integrierbar, um ARP-Ereignisse zu empfangen und eine zusätzliche Analysemebene und automatische Reaktionen zu ermöglichen.

Kontrollmechanismen für die Sicherheitsautomatisierung und Orchestrierung von NetApp außerhalb von ONTAP

Durch Automatisierung können Sie Prozesse oder Verfahren mit minimaler menschlicher Unterstützung durchführen. Durch Automatisierung sind Unternehmen in der Lage, Zero-Trust-Implementierungen weit über manuelle Verfahren hinaus zu skalieren und sich so gegen ebenfalls automatisierte Aktivitäten zu wehren, bei denen Fehlkreationen entstehen.

Ansible ist ein Open-Source-Tool zur Softwarebereitstellung, zum Konfigurationsmanagement und zur Applikationsbereitstellung. Es läuft auf vielen Unix-ähnlichen Systemen und kann sowohl Unix-ähnliche Systeme als auch Microsoft Windows konfigurieren. Es enthält seine eigene deklarative Sprache, um die

Systemkonfiguration zu beschreiben. Ansible wurde von Michael DeHaan geschrieben und 2015 von Red hat übernommen. Ansible funktioniert ohne Agenten und stellt zur Durchführung von Aufgaben vorübergehend eine Remote-Verbindung über SSH oder Windows Remote Management her (sodass PowerShell Remote ausgeführt werden kann). NetApp hat mehr als entwickelt "150 Ansible-Module für ONTAP-Software"und ermöglicht eine weitere Integration in das Automatisierungs-Framework Ansible. Ansible-Module für NetApp bieten eine Anleitung, wie der gewünschte Zustand definiert wird, und übertragen dies auf die NetApp Zielumgebung. Die Module werden zur Unterstützung von Aufgaben wie beispielsweise das Einrichten von Lizenzierung, Erstellen von Aggregaten und Storage Virtual Machines, Erstellen von Volumes und Wiederherstellen von Snapshots erstellt. Eine Ansible-Rolle war "Veröffentlicht auf GitHub" speziell auf den Implementierungsleitfaden für NetApp Unified Capabilities (UC) zugeschnitten.

Mit der Bibliothek verfügbarer Module können Benutzer auf einfache Weise Ansible-Playbooks entwickeln und für die eigenen Applikationen und geschäftlichen Anforderungen anpassen, um Routineaufgaben zu automatisieren. Nachdem ein Playbook verfasst ist, können Sie es ausführen, um die angegebene Aufgabe auszuführen. Dies spart Zeit und erhöht die Produktivität. NetApp hat Beispiel-Playbooks erstellt und geteilt, die direkt verwendet oder an die eigenen Anforderungen angepasst werden können.

Cloud Insights ist ein Infrastruktur-Monitoring-Tool, mit dem Sie Ihre gesamte Infrastruktur im Blick haben. Cloud Insights überwacht nicht nur alle Ressourcen, die sowohl Public Cloud-Instanzen als auch private Datacenter umfassen, sondern hilft auch dabei, Fehler aufzuspüren und den Ressourceneinsatz zu optimieren. Cloud Insights kann die durchschnittliche Zeit bis zur Problemlösung um 90 % verkürzen und 80 % der Cloud-Probleme für Endbenutzer verhindern. Außerdem lassen sich die Kosten für die Cloud-Infrastruktur um durchschnittlich 33 % senken. Durch den Schutz Ihrer Daten mithilfe verwertbarer Informationen verringern sie das Risiko von Bedrohungen von innen. Die Funktion für Storage-Workload-Sicherheit von Cloud Insights ermöglicht benutzerverhaltensanalysen mit KI und ML, Warnmeldungen zu erstellen, wenn aufgrund von Bedrohungen von innen ein fehlendes Benutzerverhalten auftritt. Bei ONTAP nutzt Storage Workload Security die Zero-Trust-FPolicy-Engine.

Zero-Trust- und Hybrid-Cloud-Implementierungen

NetApp ist die Instanz für Daten in der Hybrid Cloud. NetApp bietet eine Vielzahl von Optionen zur Erweiterung von On-Premises-Datenmanagementsystemen zu einer Hybrid Cloud mit Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) und anderen führenden Cloud-Providern. Hybrid-Cloud-Lösungen von NetApp unterstützen dieselben Zero-Trust-Sicherheitskontrollen, die in On-Premises-ONTAP-Systemen und softwaredefiniertem ONTAP Select Storage verfügbar sind.

Mit dem NetApp Cloud Volumes Service, dem ersten Cloud-nativen Fileservice der Enterprise-Klasse für AWS und GCP sowie Azure NetApp Files für Microsoft Azure, lässt sich die Kapazität in Public Clouds ohne typische Investitionsbeschränkungen einfach erweitern. Diese Cloud-Datenservices sind ideal für datenintensive Workloads, wie z. B. Analysen und DevOps. Sie kombinieren flexiblen On-Demand-Storage als Service von NetApp mit ONTAP Datenmanagement in einem vollständig gemanagten Angebot.

Für Kunden, die erweiterte Datenservices für Cloud-Block- oder Objekt-Storage-Services wie AWS EBS und S3 oder Azure Storage benötigen, bietet Cloud Volumes ONTAP Datenmanagement zwischen ihrer On-Premises-Umgebung und der Public Cloud mit einer einzigen Ansicht. Cloud Volumes ONTAP wird in AWS oder Azure als On-Demand-Instanz ausgeführt und bietet die Storage-Effizienz, Verfügbarkeit und Skalierbarkeit der ONTAP Software. Mit der Datenreplizierungssoftware NetApp SnapMirror können Daten zwischen lokalen ONTAP Systemen und AWS oder Azure Storage-Umgebungen verschoben werden ONTAP.

Erfahren Sie mehr über ONTAP Zero Trust Inhalte

Weitere Informationen zu den im ONTAP Zero-Trust-Inhalt beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- "Verizon Data Breach Investigations Report"
- "DoD Strategie zur digitalen Modernisierung"
- "NIST SP 800-207 Zero-Trust-Architektur"
- "NetApp Partner Connect: Security Alliance-Partner"
- "Verwenden von FPolicy für Datei-Monitoring und -Management bei SVMs"
- "PCI-DSS 3.2 ONTAP 9"
- "DSGVO (Datenschutz-Grundverordnung)"
- "Zusammenfassung der HIPPA-Datenschutzregel"
- "NetApp BlueXP Klassifizierung"
- "Überprüfung durch mehrere Administratoren"
- "Manipulationssichere Snapshot Kopie Sperrung"
- "Multi-Faktor-Authentifizierung in ONTAP 9"
- "NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption und NetApp Aggregate Encryption"
- "NetApp Storage Encryption"
- "NetApp Volume Encryption und NetApp Aggregate Encryption"
- "NetApp Cryptographic Module FIPS-140-2-Zertifikat"
- "Quantum-fähige Data-at-Rest-Verschlüsselung von NetApp"
- "Innovationen mit Sicherheit: NetApp und Ontrack gewinnen den Flash Memory Summit Award"
- "Integriertes Verschlüsselungsmanagement"
- "NetApp Interoperabilitäts-Matrix-Tool"
- "Konfiguration des externen Schlüsselmanagements"
- "Kommerzielle Lösungen für klassifizierte"
- "ONTAP IPsec"
- "Sicherheitskonfiguration ändern, um den FIPS-Modus zu aktivieren"
- "Aktivieren der Verschlüsselung von Cluster-Peering für eine vorhandene Peer-Beziehung"
- "Workload-Sicherheit für Storage (Cloud Secure)"
- "Einstieg in die Automatisierung von Entwicklungs-Workflows – mit NetApp und Ansible"
- "Ansible-Modul speziell für den Bereitstellungsleitfaden (Unified Capabilities, UC) des NetApp DoD"
- "Administratorauthentifizierung und RBAC"
- "Verschlüsselung ruhender Daten mit ONTAP"
- "TR-4569 Sicherheits- Hardening Guide for NetApp ONTAP 9"