Sicherheit

ONTAP Technical Reports

NetApp
January 23, 2026

Inhalt

Sicherheit

Technische Berichte zur Sicherheit von ONTAP

ONTAP entwickelt sich weiter und Sicherheit ist dabei ein integraler Bestandteil der Lösung. Die neueste Version von ONTAP enthält viele neue Sicherheitsfunktionen, die für Ihr Unternehmen von unschätzbarem Wert sind, um die Daten in der gesamten Hybrid Cloud zu schützen, Ransomware-Angriffen vorzubeugen und die von der Branche empfohlenen Vorgehensweisen einzuhalten. Diese neuen Funktionen unterstützen Ihr Unternehmen außerdem dabei, sich weiter in Richtung eines Zero-Trust-Modells zu bewegen.

Diese technischen Berichte erweitern die "ONTAP Sicherheit und Datenverschlüsselung"Produktdokumentation.

Cyber-Vault: ONTAP

"Cyber-Vault: ONTAP" Die auf ONTAP basierende Cyber-Vault von NetApp bietet Unternehmen eine umfassende und flexible Lösung für den Schutz ihrer wichtigsten Datenbestände. Dank der Nutzung logischer Air-Gapping-Verfahren zur robusten Härtung können Sie mit ONTAP sichere, isolierte Storage-Umgebungen erstellen, die gegen neue Cyberbedrohungen gewappnet sind. Mit ONTAP gewährleisten Sie die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Daten und profitieren gleichzeitig von der Agilität und Effizienz Ihrer Storage-Infrastruktur.

Ransomware

"TR-4572: Die NetApp Lösung für Ransomware" Erfahren Sie, wie sich Ransomware weiterentwickelt hat, und wie Sie Angriffe identifizieren, die Ausbreitung verhindern und mit der NetApp Lösung für Ransomware so schnell wie möglich wiederherstellen können. Die in diesem Dokument enthaltenen Anleitungen und Lösungen sollen Unternehmen dabei helfen, über Cyber-resiliente Lösungen zu verfügen und gleichzeitig ihre vorgegebenen Sicherheitsziele für Vertraulichkeit, Integrität und Verfügbarkeit von Informationssystemen zu erfüllen.

"TR-4526: Konformer WORM Storage mit NetApp SnapLock"
Viele Unternehmen setzen auf WORM-Storage (Write Once, Read Many), um gesetzliche Vorgaben einzuhalten oder einfach nur um eine weitere Schicht zu ihrer Datensicherungsstrategie hinzuzufügen. Erfahren Sie, wie Sie SnapLock, die WORM-Lösung in ONTAP, in Umgebungen integrieren, die WORM-Datenspeicher erfordern.

Zero Trust

"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. ONTAP verfolgt für Zero Trust 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.

Multi-Faktor-Authentifizierung

"TR-4647: Multi-Faktor-Authentifizierung in ONTAP Best Practices and Implementation Guide"
Informieren Sie sich über die Multi-Faktor-Authentifizierung von ONTAP für administrativen Zugriff über System Manager, Active IQ Unified Manager und ONTAP Secure Shell (SSH)-CLI-Authentifizierung.

"TR-4717: ONTAP-SSH-Authentifizierung mit einer gemeinsamen Zugriffskarte"
Erfahren Sie, wie Sie SSH-Clients von Drittanbietern in Verbindung mit der ActivClient-Software konfigurieren und testen, um einen ONTAP-Storage-Administrator über den öffentlichen Schlüssel zu authentifizieren, der auf einer Common Access Card (CAC) gespeichert ist, wenn er in ONTAP konfiguriert ist.

Mandantenfähigkeit

"TR-4160: Sichere Mandantenfähigkeit in ONTAP"
Erfahren Sie, wie Sie mithilfe von Storage-VMs in ONTAP sichere Mandantenfähigkeit implementieren. Hierzu gehören auch Entwurfsüberlegungen und empfohlene Vorgehensweisen.

Standards

"TR-4401: PCI-DSS 4.0 und ONTAP"
Erfahren Sie, wie Sie ein System anhand des PCI DSS 4.0-Standards validieren und die Anforderungen der für ein NetApp ONTAP-System geltenden Kontrollen erfüllen.

Attributbasierte Zugriffssteuerung

"Attributbasierte Zugriffssteuerung mit ONTAP" Erfahren Sie, wie Sie die NFSv4.2-Sicherheitsetiketten und erweiterten Attribute (xattrs) konfigurieren, um die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) und die attributbasierte Zugriffskontrolle (ABAC) zu unterstützen. Dabei handelt es sich um eine Autorisierungsstrategie, die Berechtigungen auf Basis von Benutzer-, Ressourcen- und Umgebungsattributen definiert.

NetApp Lösung für Ransomware

Ransomware und das Datensicherungsportfolio von NetApp

Ransomware ist nach wie vor eine der größten Bedrohungen, die 2024 für Geschäftsunterbrechungen verantwortlich sind. Laut den "Sophos State of Ransomware 2024", Ransomware-Angriffe betroffen 72 % der befragten Publikum . Ransomware-Angriffe sind heute raffinierter und gezielter ausgeführt. Bedrohungsakteure setzen fortschrittliche Techniken wie künstliche Intelligenz ein, um ihre Wirkung und ihren Gewinn zu maximieren.

Unternehmen müssen die gesamte Sicherheitslage in ihren Bereichen wie Umgebung, Netzwerk, Identität, Applikation und Speicherort der Daten auf Storage-Ebene prüfen und diese Ebenen sichern. In der heutigen Bedrohungslandschaft wird ein datenorientierter Ansatz für Cyberschutz auf Storage-Ebene eingeführt. Obwohl keine einzige Lösung alle Angriffe vereiteln kann, bietet die Verwendung eines Portfolios von Lösungen, einschließlich Partnerschaften und Dritter, eine mehrstufige Verteidigung.

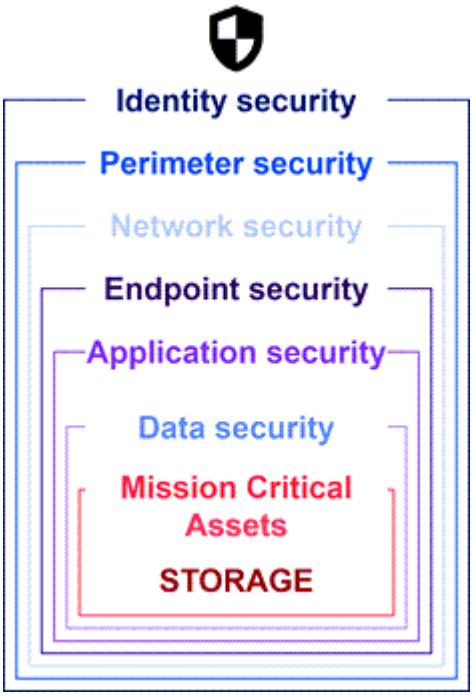
Das NetApp Produktportfolio bietet verschiedene effektive Tools für Transparenz, Erkennung und Problembehebung, damit Sie Ransomware frühzeitig erkennen, eine Ausbreitung vermeiden und bei Bedarf schnell eine Wiederherstellung durchführen können, um kostspielige Ausfallzeiten zu vermeiden. Traditionelle

mehrschichtige Verteidigungslösungen sind nach wie vor weit verbreitet, ebenso wie Lösungen von Drittanbietern und Partnern für Transparenz und Erkennung. Eine effektive Gegenmaßnahmen sind nach wie vor ein wichtiger Teil der Reaktion auf Bedrohungen. Der einzigartige Branchenansatz, der die unveränderliche NetApp Snapshot Technologie und die logische Air Gap-Lösung von SnapLock nutzt, ist ein Alleinstellungsmerkmal in der Branche und die Best Practice zur Behebung von Ransomware-Angriffen.

Ab Juli 2024 ist der Inhalt des zuvor als PDF veröffentlichten technischen Berichts *TR-4572: NetApp Ransomware Protection* auf docs.netapp.com verfügbar.

Daten sind das primäre Ziel

Cyberkriminelle setzen Daten zunehmend direkt ins Visier und erkennen ihren Wert. Die Sicherheit von Umgebung, Netzwerk und Anwendung ist zwar wichtig, kann aber umgangen werden. Die Storage-Ebene konzentriert sich auf den Schutz der Daten an der Quelle und stellt eine entscheidende letzte Verteidigungslinie dar. Ziel von Ransomware-Angriffen ist es, Zugang zu Produktionsdaten zu erhalten und sie zu verschlüsseln oder unzugänglich zu machen. Um dorthin zu gelangen, müssen Angreifer bereits vorhandene Verteidigungsmechanismen durchbohrt haben, die von Unternehmen heute eingesetzt werden, von Perimeter bis Anwendungssicherheit.



Leider nutzen viele Unternehmen die Sicherheitsfunktionen auf Datenebene nicht. An dieser Stelle kommt das NetApp Portfolio für Ransomware-Schutz ins Spiel, das Sie in der letzten Verteidigungslinie schützt.

Die realen Kosten von Ransomware

Die Lösegeldzahlung selbst ist nicht der größte monetäre Effekt auf ein Unternehmen. Obwohl die Zahlung nicht unbedeutend ist, verblasst sie im Vergleich zu den Downtime-Kosten, die durch einen Ransomware-Vorfall verursacht werden.

Lösegeldzahlungen sind nur ein Element der Recovery-Kosten im Zusammenhang mit Ransomware-Ereignissen. Ohne gezahlte Lösegeld gaben 2024 Unternehmen nach einem Ransomware-Angriff durchschnittliche Kosten für "2024 Sophos State of Ransomware" die Wiederherstellung von 2,73 Millionen US-Dollar an. Dies entspricht einem Anstieg von fast 1 Millionen US-Dollar gegenüber den 1,82 Millionen US-Dollar, die 2023 laut Bericht gemeldet wurden. Für Unternehmen, die stark von der IT-Verfügbarkeit abhängig

sind, wie E-Commerce, Aktienhandel und Gesundheitswesen, können die Kosten 10-mal höher oder höher sein.

Auch die Kosten für Cyberversicherungen steigen weiter, da die Wahrscheinlichkeit eines Ransomware-Angriffs auf Versicherte sehr hoch ist.

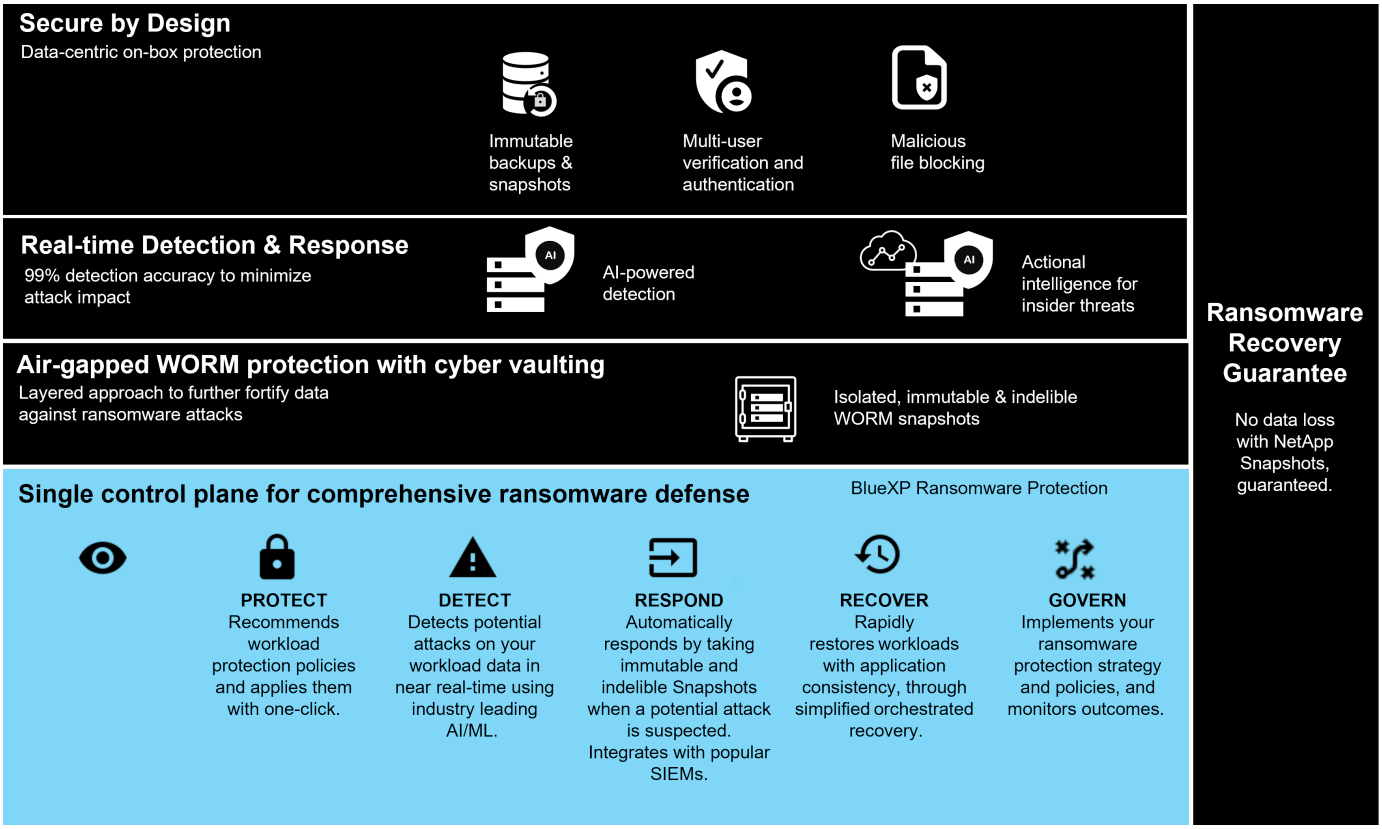
Schutz vor Ransomware auf Datenebene

NetApp versteht die umfassende Sicherheit Ihres Unternehmens, von der Umgebung bis zum Speicherort Ihrer Daten auf der Storage-Ebene. Ihr Sicherheits-Stack ist komplex und sollte Sicherheit auf jeder Ebene Ihres Technologie-Stacks bieten.

Der Echtzeitschutz auf Datenebene ist noch wichtiger und hat spezielle Anforderungen. Um effektiv zu sein, müssen Lösungen auf dieser Ebene folgende wichtige Attribute aufweisen:

- **Sicherheit durch Design**, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren
- * Echtzeit-Erkennung und Reaktion*, um die Auswirkungen eines erfolgreichen Angriffs zu minimieren
- **Air-Gap WORM-Schutz** zur Isolierung kritischer Daten-Backups
- **Eine einzelne Kontrollebene** für umfassende Ransomware-Verteidigung

NetApp kann all dies und noch mehr bieten.



Das NetApp Portfolio für Ransomware-Schutz

NetApp "Integrierter Ransomware-Schutz"bietet robusten und vielseitigen Schutz Ihrer kritischen Daten in Echtzeit. Im Kern überwachen fortschrittliche KI-gestützte Erkennungsalgorithmen kontinuierlich die Datenmuster und identifizieren potenzielle Ransomware-Bedrohungen schnell mit einer Genauigkeit von 99 %. Durch schnelle Reaktion auf Angriffe kann unser Storage schnell Snapshot von Daten erstellen und die Kopien

sichern, was zu einer schnellen Wiederherstellung führt.

Zur weiteren Stärkung der Daten "Cyber-Vaulting"isoliert die Funktion von NetApp Daten über einen logischen Air Gap. Durch den Schutz wichtiger Daten gewährleisten wir eine schnelle Business Continuity.

NetApp"NetApp Ransomware-Schutz" reduziert den Betriebsaufwand mit einer einzigen Steuerungsebene zur intelligenten Koordination und Ausführung einer durchgängigen, Workload-zentrierten Ransomware-Abwehr. So können Sie gefährdete kritische Workload-Daten mit einem einzigen Klick identifizieren und schützen, die Auswirkungen eines potenziellen Angriffs präzise und automatisch erkennen und darauf reagieren, um diese zu begrenzen, und Workloads innerhalb von Minuten (nicht Tagen) wiederherstellen. So bleiben Ihre wertvollen Workload-Daten geschützt und kostspielige Unterbrechungen werden minimiert.

Als native, integrierte ONTAP-Lösung zum Schutz von unberechtigtem Zugriff auf Daten "Verifizierung durch mehrere Administratoren (Multi-Admin Verification, MAV)"verfügt über eine robuste Reihe von Funktionen, die dafür sorgen, dass Vorgänge wie Löschen von Volumes, Erstellen zusätzlicher administrativer Benutzer oder Löschen von Snapshots nur nach Genehmigung durch mindestens einen zweiten designierten Administrator ausgeführt werden können. So werden gefährdete, böswillige oder unerfahrene Administratoren daran gehindert, unerwünschte Änderungen vorzunehmen oder Daten zu löschen. Sie können so viele festgelegte Administratorgenehmiger konfigurieren, wie Sie möchten, bevor ein Snapshot gelöscht werden kann.

NetApp ONTAP erfüllt die Anforderungen für eine webbasierte "Multi-Faktor-Authentifizierung (MFA)" in System Manager und für die SSH-CLI-Authentifizierung.

Der NetApp Schutz vor Ransomware sorgt in einer sich ständig weiterentwickelnden Bedrohungslandschaft für ein gutes Gefühl. Ihr umfassender Ansatz schützt nicht nur vor aktuellen Ransomware-Varianten, sondern passt sich auch neuen Bedrohungen an. So bietet er langfristige Sicherheit für Ihre Dateninfrastruktur.

Weitere Schutzoptionen

- "Digital Advisor Ransomware-Schutz"
- "Data Infrastructure Insights Speicher-Workload-Sicherheit"
- "FPolicy"
- "SnapLock und manipulationssichere Snapshots"

Recovery-Garantie bei Ransomware

NetApp bietet die Garantie, Snapshot-Daten bei einem Ransomware-Angriff wiederherzustellen. Unser Versprechen: Wenn wir Ihnen bei der Wiederherstellung Ihrer Snapshot-Daten nicht helfen können, machen wir es richtig. Die Garantie gilt für Neukäufe von AFF Systemen der A-Serie, AFF C-Serie, ASA und FAS.

Weitere Informationen .

- "Recovery Garantie Servicebeschreibung"
- "Blog zur Recovery-Garantie von Ransomware".

Verwandte Informationen

- "Ressourcen-Seite auf der NetApp Support Site"
- "NetApp Produktsicherheit"

SnapLock und manipulationssichere Snapshots für den Schutz vor Ransomware

Eine entscheidende Waffe im Snap-Arsenal von NetApp ist SnapLock, das sich beim Schutz vor Ransomware-Bedrohungen als äußerst effektiv erwiesen hat. Indem

SnapLock das Löschen von Daten durch Unbefugte verhindert, bietet es eine zusätzliche Sicherheitsschicht, die auch bei Angriffen die Unversehrtheit und den Zugriff auf kritische Daten sicherstellt.

SnapLock-Compliance

SnapLock Compliance (SLC) bietet unlöschbaren Schutz Ihrer Daten. SLC verhindert das Löschen von Daten, selbst wenn ein Administrator versucht, das Array neu zu initialisieren. Im Gegensatz zu anderen Konkurrenzprodukten ist SnapLock Compliance nicht anfällig für Social Engineering-Hacks durch die Support-Teams dieser Produkte. Daten, die durch SnapLock Compliance Volumes geschützt sind, können wiederhergestellt werden, bis sie ihr Ablaufdatum erreicht haben.

Zur Aktivierung von SnapLock "ONTAP One"ist eine Lizenz erforderlich.

Weitere Informationen .

- "SnapLock Dokumentation"

Manipulationssichere Snapshots

Manipulationssichere Snapshot Kopien (TPS) bieten eine praktische und schnelle Möglichkeit, Daten vor böswilligen Handlungen zu schützen. Im Gegensatz zu SnapLock Compliance wird TPS in der Regel auf Primärsystemen verwendet, auf denen der Benutzer die Daten für einen bestimmten Zeitraum schützen und lokal für schnelle Wiederherstellungen belassen kann oder wenn Daten nicht vom Primärsystem repliziert werden müssen. TPS verwendet SnapLock-Technologien, um zu verhindern, dass der primäre Snapshot auch von einem ONTAP-Administrator gelöscht wird, der dieselbe SnapLock-Aufbewahrungsfrist verwendet. Das Löschen von Snapshots wird auch dann verhindert, wenn das Volume nicht SnapLock aktiviert ist, obwohl Snapshots nicht dieselbe unlöschbare Eigenschaft von SnapLock Compliance Volumes aufweisen.

Um Snapshots manipulationssicher zu machen, ist eine "ONTAP One" Lizenz erforderlich.

Weitere Informationen .

- "Sperren Sie einen Snapshot, um sich vor Ransomware-Angriffen zu schützen".

FPolicy Dateisperrung

FPolicy verhindert das Speichern unerwünschter Dateien auf einer Storage Appliance der Enterprise-Klasse. FPolicy bietet Ihnen auch eine Möglichkeit, bekannte Ransomware-Dateierweiterungen zu blockieren. Ein Benutzer hat weiterhin volle Zugriffsrechte auf den Home-Ordner, aber FPolicy lässt es einem Benutzer nicht zu, Dateien zu speichern, die von seinem Administrator als blockiert markiert wurden. Es spielt keine Rolle, ob diese Dateien MP3-Dateien oder bekannte Ransomware-Dateierweiterungen sind.

Blockieren Sie bösartige Dateien mit dem nativen FPolicy-Modus

Der native Modus von NetApp FPolicy (eine Weiterentwicklung des Namens, Dateirichtlinie) ist ein blockierendes Framework mit Dateierweiterungen, mit dem Sie unerwünschte Dateierweiterungen je nach Eingang in Ihre Umgebung blockieren können. Seit über einem Jahrzehnt ist ONTAP Cloud Teil von ONTAP. Es ist unglaublich hilfreich, wenn es darum geht, Sie beim Schutz vor Ransomware zu unterstützen. Diese Zero Trust Engine ist wertvoll, weil Sie zusätzliche Sicherheitsmaßnahmen erhalten, die über die Zugriffssteuerungslisten (ACL)-Berechtigungen hinausgehen.

Im ONTAP System Manager und der NetApp Console steht eine Liste mit über 3000 Dateierweiterungen als

Referenz zur Verfügung.

> Einige Erweiterungen können in Ihrer Umgebung legitim sein, und das Blockieren kann zu unerwarteten Problemen führen. Erstellen Sie zunächst Ihre eigene Liste, die für die jeweilige Umgebung geeignet ist, bevor Sie native FPolicy konfigurieren.

Der native FPolicy-Modus ist in allen ONTAP Lizenzen enthalten.

Weitere Informationen .

- "Blog: Kampf gegen Ransomware: Teil drei – ONTAP FPolicy, ein weiteres leistungsstarkes natives Tool (aka kostenlos)"

Aktivieren Sie UEBA (User and Entity Behavior Analytics) mit dem externen FPolicy-Modus

Der externe FPolicy-Modus ist ein Benachrichtigungs- und Kontrollframework für die Dateiaktivität, das eine Übersicht über die Datei- und Benutzeraktivität bietet. Diese Benachrichtigungen können von einer externen Lösung verwendet werden, um KI-basierte Analysen durchzuführen, um schädliches Verhalten zu erkennen.

Der externe FPolicy-Modus kann auch so konfiguriert werden, dass er auf die Genehmigung des FPolicy-Servers wartet, bevor bestimmte Aktivitäten durchlaufen werden. Mehrere Richtlinien wie diese können auf einem Cluster konfiguriert werden, was für ein hohes Maß an Flexibilität sorgt.

> FPolicy-Server müssen auf FPolicy-Anfragen reagieren, wenn sie für eine Genehmigung konfiguriert sind. Andernfalls kann die Storage-System-Performance beeinträchtigt werden.

Der externe FPolicy-Modus ist in enthalten"Alle ONTAP Lizenzen".

Weitere Informationen .

- "Blog: Kampf gegen Ransomware: Teil vier – UBA und ONTAP mit FPolicy externen Modus."

Data Infrastructure Insights Speicher-Workload-Sicherheit

Storage Workload Security (SWS) ist eine Funktion von NetApp Data Infrastructure Insights, die die Sicherheitslage, Wiederherstellbarkeit und Verantwortlichkeit einer ONTAP Umgebung erheblich verbessert. SWS verfolgt einen benutzerzentrierten Ansatz und verfolgt alle Dateiaktivitäten jedes authentifizierten Benutzers in der Umgebung. Es verwendet erweiterte Analysen, um normale und saisonale Zugriffsmuster für jeden Benutzer zu ermitteln. Diese Muster werden verwendet, um verdächtiges Verhalten schnell zu erkennen, ohne dass Ransomware-Signaturen erforderlich sind.

Wenn SWS eine potenzielle Ransomware oder Datenlöschung erkennt, kann es beispielsweise folgende automatische Maßnahmen ergreifen:

- Erstellen Sie einen Snapshot des betroffenen Volumes.
- Blockieren Sie das Benutzerkonto und die IP-Adresse, die möglicherweise von schädlicher Aktivität vermutet werden.
- Senden Sie eine Benachrichtigung an Administratoren.

Da SWS automatisierte Maßnahmen ergreifen kann, um Bedrohungen von innen schnell zu stoppen und alle Dateiaktivitäten zu verfolgen, macht die Recovery nach einem Ransomware-Ereignis erheblich einfacher und schneller. Mit den integrierten erweiterten Tools für die Prüfung und Forensik können Benutzer sofort sehen,

welche Volumes und Dateien von einem Angriff betroffen waren, von welchem Benutzerkonto der Angriff stammte und welche böswilligen Aktionen ausgeführt wurden. Automatische Snapshots verringern den Schaden und beschleunigen die Dateiwiederherstellung.

Warnmeldungen aus dem Autonomen Ransomware-Schutz (ARP) von ONTAP sind auch in SWS sichtbar und bieten Kunden, die sowohl ARP als auch SWS zum Schutz vor Ransomware-Angriffen verwenden, eine einzige Schnittstelle.

Weitere Informationen .

- "Einblicke in die NetApp Data Infrastructure Insights"

In NetApp ONTAP integrierte, KI-basierte Erkennung und Reaktion

Ransomware-Bedrohungen werden immer raffinierter – auch Ihre Abwehrmechanismen sollten sich auswachsen. Der autonome Ransomware-Schutz (ARP) von NetApp wird über KI mit intelligenter Anomalieerkennung bereitgestellt, die in ONTAP integriert ist. Aktivieren Sie diese Möglichkeit, um Ihre Cyber-Resilienz um eine weitere Verteidigungsebene zu erweitern.

ARP und ARP/AI können über die integrierte Management-Schnittstelle von ONTAP, System Manager, konfiguriert und für einzelne Volumes aktiviert werden.

Autonomer Schutz durch Ransomware (ARP)

Autonomous Ransomware Protection (ARP), eine weitere seit 9.10.1 integrierte native ONTAP-Lösung, untersucht die Dateiaktivität und Datenentropie des NAS-Storage-Volumes, um potenzielle Ransomware-Angriffe automatisch zu erkennen. ARP bietet Administratoren Erkennung in Echtzeit, Einblicke und einen Punkt für die Daten-Recovery für eine nie dagewesene Erkennung potenzieller Ransomware.

Bei ONTAP 9.15.1 und älteren Versionen, die ARP unterstützen, startet ARP im Lernmodus, um die typische Workload-Datenaktivität zu erlernen. Dies kann in den meisten Umgebungen sieben Tage dauern. Nach Abschluss des Lernmodus wechselt ARP automatisch in den aktiven Modus und sucht nach abnormalen Workload-Aktivitäten, die möglicherweise eine Ransomware sein könnten.

Wenn eine anormale Aktivität erkannt wird, wird sofort ein automatischer Snapshot erstellt. Dieser bietet einen Wiederherstellungspunkt, der dem Zeitpunkt des Angriffs mit minimalen infizierten Daten so nahe wie möglich liegt. Gleichzeitig wird eine automatische Warnung (konfigurierbar) generiert, mit der Administratoren die anormalen Dateiaktivitäten sehen können, damit sie feststellen können, ob die Aktivität tatsächlich schädlich ist, und entsprechende Maßnahmen ergreifen können.

Wenn es sich bei der Aktivität um eine zu erwartende Arbeitslast handelt, können Administratoren sie leicht als

falsch positiv markieren. ARP lernt diese Änderung als normale Workload-Aktivität und markiert sie nicht mehr als einen potenziellen Angriff in der Zukunft.

Um ARP zu aktivieren, "ONTAP One"ist eine Lizenz erforderlich.

Weitere Informationen .

- "Autonomer Schutz Durch Ransomware"

Autonomer Ransomware-Schutz/KI (ARP/AI)

ARP/AI wurde als Tech Preview in ONTAP 9.15.1 eingeführt und ermöglicht eine neue Stufe der Echtzeiterkennung von NAS-Storage-Systemen. Die neue KI-gestützte Erkennungstechnologie ist mit über einer Million Dateien und verschiedenen bekannten Ransomware-Angriffen trainiert. Neben den in ARP verwendeten Signalen erkennt ARP/AI auch die Header-Verschlüsselung. Dank der AI-Leistung und der zusätzlichen Signale kann ARP/AI eine Erkennungsgenauigkeit von über 99 % erzielen. Dies wurde von SE Labs validiert, einem unabhängigen Testlabor, das ARP/AI die höchste AAA-Bewertung verlieh.

Da das Training der Modelle kontinuierlich in der Cloud stattfindet, ist für ARP/AI kein Lernmodus erforderlich. Er ist aktiv, sobald er eingeschaltet wird. Ein kontinuierliches Training bedeutet auch, dass ARP/AI immer gegen neue Arten von Ransomware-Angriffen validiert wird, sobald sie auftreten. ARP/AI verfügt außerdem über Funktionen für automatische Updates, die für alle Kunden neue Parameter bereitstellen, um die Ransomware-Erkennung auf dem neuesten Stand zu halten. Alle anderen Erkennungs-, Erkennungs- und Wiederherstellungspunkt-Funktionen von ARP werden für ARP/AI gepflegt.

Um ARP/AI "ONTAP One"zu aktivieren, ist eine Lizenz erforderlich.

Weitere Informationen .

- "Blog: Die KI-basierte Echtzeit-Ransomware-Erkennungslösung von NetApp erreicht AAA-Bewertung"

Luftgewindelter WORM-Schutz mit Cyber-Vaulting in ONTAP

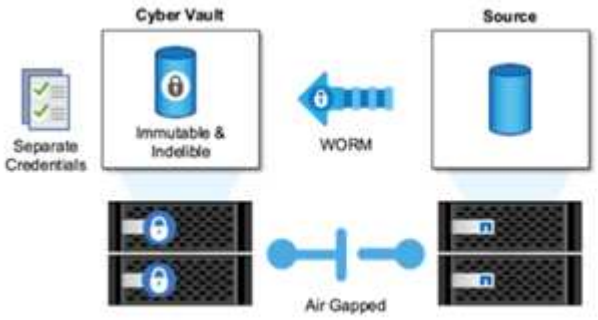
Der Ansatz von NetApp bei einer Cyber-Vault ist eine speziell entwickelte Referenzarchitektur für eine logisch luftgefragte Cyber-Vault. Dieser Ansatz nutzt Technologien zur Erhöhung der Sicherheit und Compliance wie SnapLock, um unveränderliche und nicht löschbare Snapshots zu ermöglichen.

Cyber-Vaulting mit SnapLock Compliance und eine logische Luftspalt

Ein wachsender Trend ist für Angreifer, die Sicherungskopien zu zerstören und in einigen Fällen sogar zu verschlüsseln. Aus diesem Grund empfehlen viele in der Cybersecurity-Branche, Air Gap-Backups als Teil einer umfassenden Cyber-Resilienz-Strategie zu verwenden.

Das Problem besteht darin, dass herkömmliche Luftspalten (Band- und Offline-Medien) die Wiederherstellungszeit erheblich erhöhen können und somit die Ausfallzeiten und die damit verbundenen Gesamtkosten erhöhen. Auch ein moderner Ansatz für eine Luftspaltlösung kann sich als problematisch erweisen. Wenn beispielsweise der Backup-Vault vorübergehend geöffnet wird, um neue Sicherungskopien zu erhalten, und dann die Verbindung zu den primären Daten getrennt und die Netzwerkverbindung geschlossen wird, um wieder „Air Gap“ zu erhalten, kann ein Angreifer die temporäre Öffnung nutzen. Während der Online-Verbindung kann ein Angreifer die Daten kompromittieren oder zerstören. Durch diese Art von Konfiguration wird auch in der Regel unerwünschte Komplexität erhöht. Eine logische Luftspalte ist ein ausgezeichneter Ersatz für eine traditionelle oder moderne Luftspalte, weil sie die gleichen Sicherheitsschutzprinzipien hat und gleichzeitig das Backup online hält. Mit NetApp lösen Sie die Komplexität von Tape- oder Festplattenluftapping mit logischem Air Gating, das sich mit unveränderlichen Snapshots und NetApp SnapLock Compliance

erreichen lässt.



NetApp hat die Funktion SnapLock vor mehr als 10 Jahren veröffentlicht, um den Anforderungen an die Daten-Compliance gerecht zu werden, beispielsweise den Health Insurance Portability and Accountability Act (HIPAA), den Sarbanes-Oxley Act (Sarbanes-Oxley) und weitere gesetzliche Datenvorschriften. Sie können außerdem primäre Snapshots in SnapLock Volumes speichern, um den WORM-Vorgang durchzuführen und so das Löschen zu verhindern. Es gibt zwei SnapLock-Lizenzversionen: SnapLock Compliance und SnapLock Enterprise. Als Schutz vor Ransomware empfiehlt NetApp SnapLock Compliance, da Sie einen bestimmten Aufbewahrungszeitraum festlegen können, in dem Snapshots gesperrt sind. Snapshots können selbst von ONTAP Administratoren oder der Unterstützung von NetApp nicht gelöscht werden.

Weitere Informationen .

- "Blog: Übersicht über die ONTAP Cyber-Vault"

Manipulationssichere Snapshots

SnapLock Compliance als logische Air Gap bietet Ihnen den ultimativen Schutz, um zu verhindern, dass Angreifer Ihre Backup-Kopien löschen. Allerdings müssen Sie die Snapshots mit SnapVault auf ein sekundäres Volume mit SnapLock-Aktivierung verschieben. Daher implementieren viele Kunden diese Konfiguration auf einem Sekundärspeicher im gesamten Netzwerk. Dies kann zu längeren Wiederherstellungszeiten führen, im Gegensatz zur Wiederherstellung eines Snapshots eines primären Volumes auf dem Primärspeicher.

Ab ONTAP 9.12.1 bieten manipulationssichere Snapshots Schutz auf SnapLock Compliance-Ebene für Ihre Snapshots auf dem primären Storage und in primären Volumes nahe an. Es ist nicht erforderlich, den Snapshot mit SnapVault auf ein sekundäres SnapLocked-Volume zu speichern. Manipulationssichere Snapshots setzen die SnapLock Technologie ein, um zu verhindern, dass der primäre Snapshot gelöscht wird, selbst wenn ein vollständiger ONTAP Administrator dieselbe Aufbewahrungsfrist für SnapLock verwendet. Dies sorgt für schnellere Wiederherstellungszeiten und die Möglichkeit, dass ein FlexClone-Volume durch einen manipulationssicheren, geschützten Snapshot gesichert wird. Dies ist mit einem herkömmlichen, archivierten SnapLock Compliance Snapshot nicht möglich.

Der Hauptunterschied zwischen SnapLock Compliance und manipulationssicheren Snapshots besteht darin, dass SnapLock Compliance das ONTAP-Array nicht initialisiert und gelöscht werden kann, wenn SnapLock Compliance-Volumes mit archivierten Snapshots existieren, die ihr Ablaufdatum noch nicht erreicht haben. Um Snapshots manipulationssicher zu machen, ist eine SnapLock Compliance Lizenz erforderlich.

Weitere Informationen .

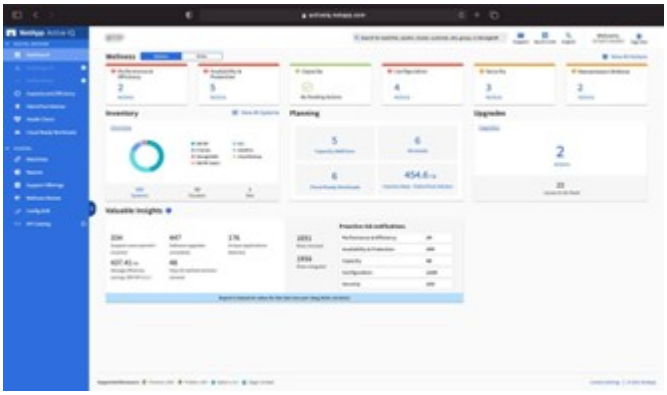
- "Sperren Sie einen Snapshot, um sich vor Ransomware-Angriffen zu schützen"

Digital Advisor Ransomware-Schutz

Digital Advisor powered by Active IQ vereinfacht die proaktive Pflege und Optimierung

von NetApp Storage mit umsetzbarer Intelligenz für optimales Datenmanagement. Gestützt auf Telemetriedaten aus unserer hochdiversen Installationsbasis nutzt es fortschrittliche KI- und ML-Techniken, um Möglichkeiten zur Risikominderung sowie zur Verbesserung der Leistung und Effizienz Ihrer Speicherumgebung aufzudecken.

Das kann nicht nur "Digitaler Berater von NetApp" helfen "Beseitigung von Sicherheitslücken", sondern bietet auch Einblicke und Anleitungen für den Schutz vor Ransomware. Eine dedizierte „Wellness“-Karte zeigt die erforderlichen Maßnahmen und die damit verbundenen Risiken an. So können Sie sicher sein, dass Ihre Systeme diese Best Practices-Empfehlungen erfüllen.



Zu den Risiken und Maßnahmen, die auf der Seite „Ransomware Defense Wellness“ nachverfolgt werden, gehören Folgendes (und vieles mehr):

- Die Anzahl der Volume-Snapshots ist niedrig. Dies verringert den potenziellen Schutz vor Ransomware.
- FPolicy ist nicht für alle Storage Virtual Machines (SVMs) aktiviert, die für NAS-Protokolle konfiguriert sind.

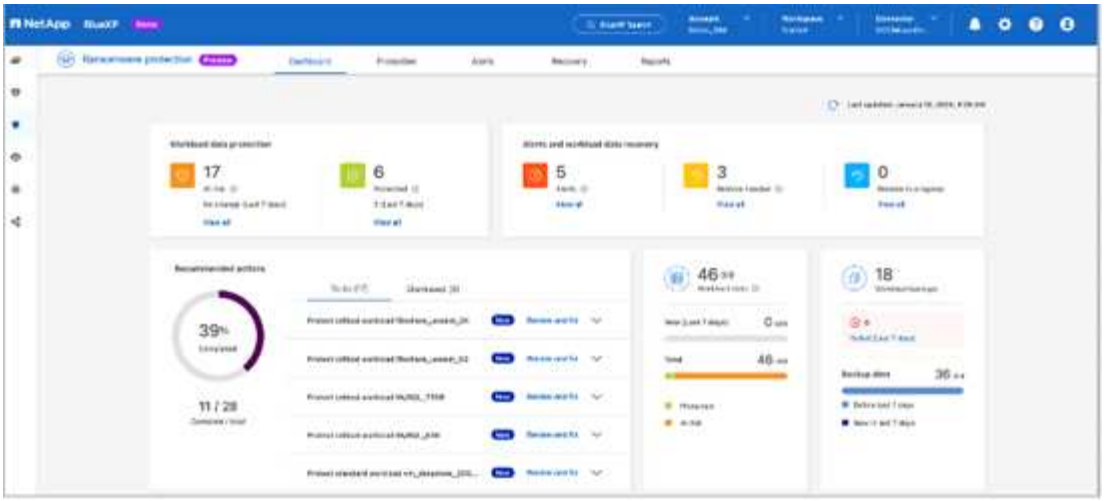
Ransomware-Schutz in Aktion sehen:"Digital Advisor"

Umfassende Ausfallsicherheit mit NetApp Ransomware-Schutz

Es ist wichtig, dass Ransomware so früh wie möglich erkannt wird, damit Sie die Verbreitung verhindern und kostspielige Ausfallzeiten vermeiden können. Eine wirksame Strategie zur Erkennung von Ransomware sollte jedoch mehr als nur eine Schutzebene umfassen. Der Ransomware-Schutz von NetApp verfolgt einen umfassenden Ansatz, der Echtzeit-On-Box-Funktionen umfasst, die sich über die NetApp Console auf Datendienste erstrecken, sowie eine isolierte, mehrschichtige Lösung für Cyber-Vaulting.

NetApp Ransomware-Schutz

Die NetApp Console ist eine einzelne Steuerebene zur intelligenten Orchestrierung einer umfassenden, Workload-zentrierten Ransomware-Abwehr. Der NetApp Ransomware-Schutz vereint die leistungsstarken Cyber-Resilience-Funktionen von ONTAP, wie ARP, FPolicy und manipulationssichere Snapshots, und NetApp -Datendienste, wie NetApp Backup and Recovery. Darüber hinaus werden Empfehlungen und Anleitungen mit automatisierten Workflows hinzugefügt, um eine End-to-End-Verteidigung über eine einzige Benutzeroberfläche bereitzustellen. Es arbeitet auf Workload-Ebene, um sicherzustellen, dass die Anwendungen, die Ihr Unternehmen betreiben, geschützt sind und im Falle eines Angriffs so schnell wie möglich wiederhergestellt werden können.



Kundenvorteile:

- Durch unterstützte Ransomware-Vorbereitung wird der betriebliche Overhead verringert und die Effizienz verbessert
- Die KI/ML-gestützte Anomalieerkennung bietet eine höhere Genauigkeit und schnellere Reaktionen zur Eindämmung von Risiken
- Mithilfe der applikationskonsistenten Wiederherstellung lassen sich Workloads einfacher und in wenigen Minuten wiederherstellen

"NetApp Ransomware-Schutz"erleichtert das Erreichen dieser NIST-Funktionen:

- Automatische Erkennung* und Priorisierung von Daten im NetApp-Speicher * mit Fokus auf die wichtigsten anwendungsbasierten Workloads *.
- **One-Click-Schutz** für Datensicherung mit Top-Workload, unveränderliche, sichere Konfiguration, bösartige Dateiblockierung und verschiedene Sicherheitsdomänen.
- * Mit * KI-basierter Anomalieerkennung der nächsten Generation * Ransomware so schnell wie möglich genau erkennen*
- Automatisierte Reaktion und Workflows sowie Integration mit Top * SIEM und XDR Lösungen.*
- Schnelle Datenwiederherstellung mit einer vereinfachten **orchestrierten Recovery** zur Beschleunigung der Applikations-Uptime.
- Implementieren Sie Ihren Ransomware-Schutz **Strategie** und **Richtlinien** und **Ergebnisse überwachen**.

NetApp und Zero Trust

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 ist der Inhalt des technischen Berichts *TR-4829: NetApp and Zero Trust: Enabling a Data-Centric Zero Trust model*, der zuvor als PDF veröffentlicht wurde, auf docs.netapp.com verfügbar.

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 John Kindervag bei Forrester Research entwickelt. 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 in der Infrastruktur Ihres Unternehmens sorgen.

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.

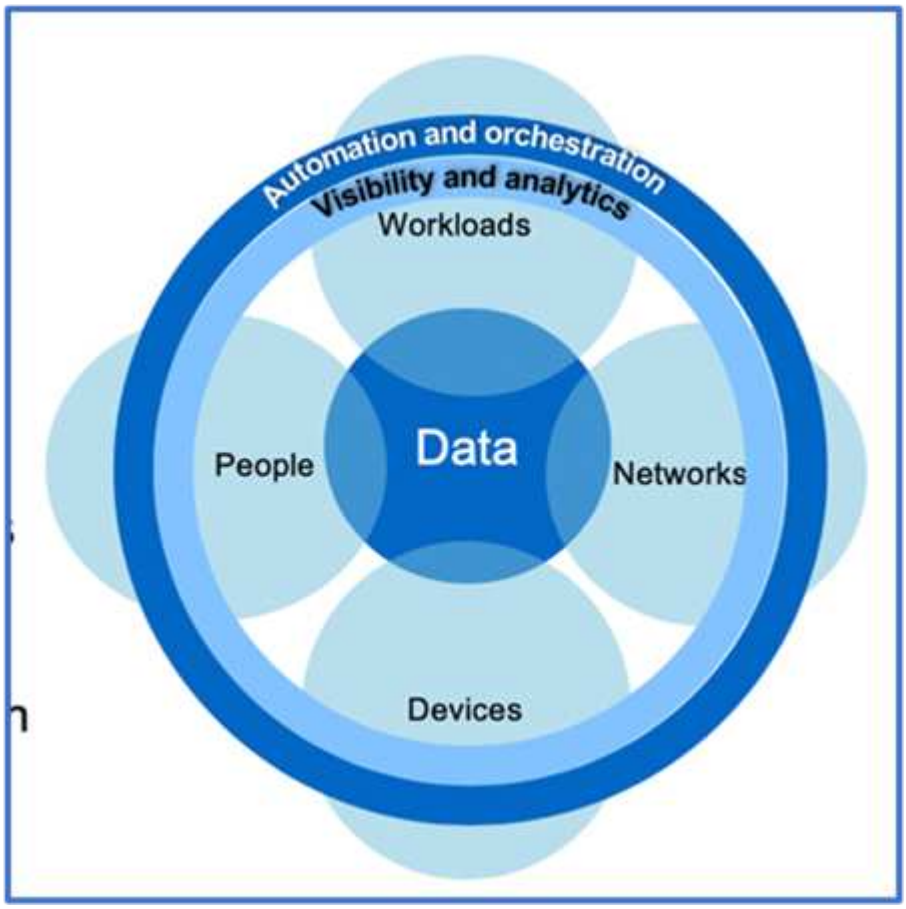
Sicherheitsressourcen

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. Bei toxischen Daten handelt es sich um sensible Daten, die nicht dazu bestimmt sind, außerhalb einer Organisation preisgegeben zu werden. Die Offenlegung toxischer Daten könnte gegen gesetzliche Vorschriften verstoßen und den Ruf eines Unternehmens schädigen. Im Hinblick auf die Einhaltung gesetzlicher Vorschriften umfassen toxische Daten Karteninhaberdaten für die "Payment Card Industry Data Security Standard (PCI-DSS)" , personenbezogene Daten für die EU "DSGVO (Datenschutz-Grundverordnung)" oder Gesundheitsdaten für die "Health Insurance Portability and Accountability Act (HIPAA)" . Sie können NetApp verwenden "NetApp Data Classification" (früher bekannt als Cloud Data Sense), ein KI-gesteuertes Toolkit zum automatischen Scannen, Analysieren und Kategorisieren Ihrer Daten.

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 andere Möglichkeit, Snapshots zu schützen, ist mit ONTAP "Snapshot wird gesperrt". Beim Snapshot-Sperren handelt es sich um eine SnapLock-Funktion, bei der Snapshots manuell oder automatisch mit einer Aufbewahrungsfrist auf der Snapshot-Richtlinie des Volumes unlöschbar gemacht werden. Snapshot-Sperrung wird auch als manipulationssichere Snapshot Sperrung bezeichnet. Mit dem Zweck der Snapshot-Sperrung

können Sie verhindern, dass abnormale oder nicht vertrauenswürdige Administratoren Snapshots auf primären und sekundären ONTAP Systemen löschen. Eine schnelle Recovery von gesperrten Snapshots auf Primärsystemen kann zur Wiederherstellung von durch Ransomware beschädigten Volumes erreicht werden.

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

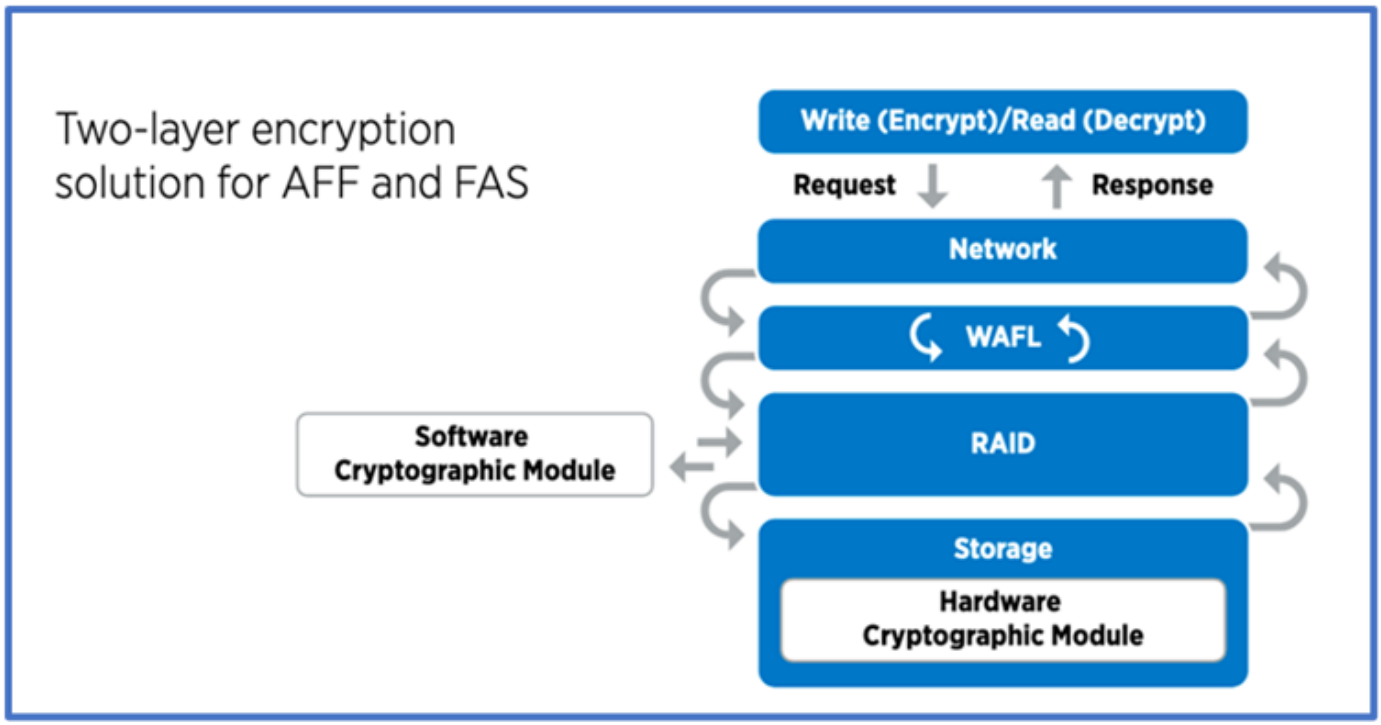
Verschlüsselung von Daten im Ruhezustand

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" Die ONTAP Hardwarelösung "Daten im Ruhezustand" verwendet validierte Self-Encrypting Drives nach FIPS 140-2 Level 2. "NVE und NAE" Sind eine ONTAP-Softwarelösung "Daten im Ruhezustand" , die den 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)"in ONTAP integrierte Schlüsselmanager 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

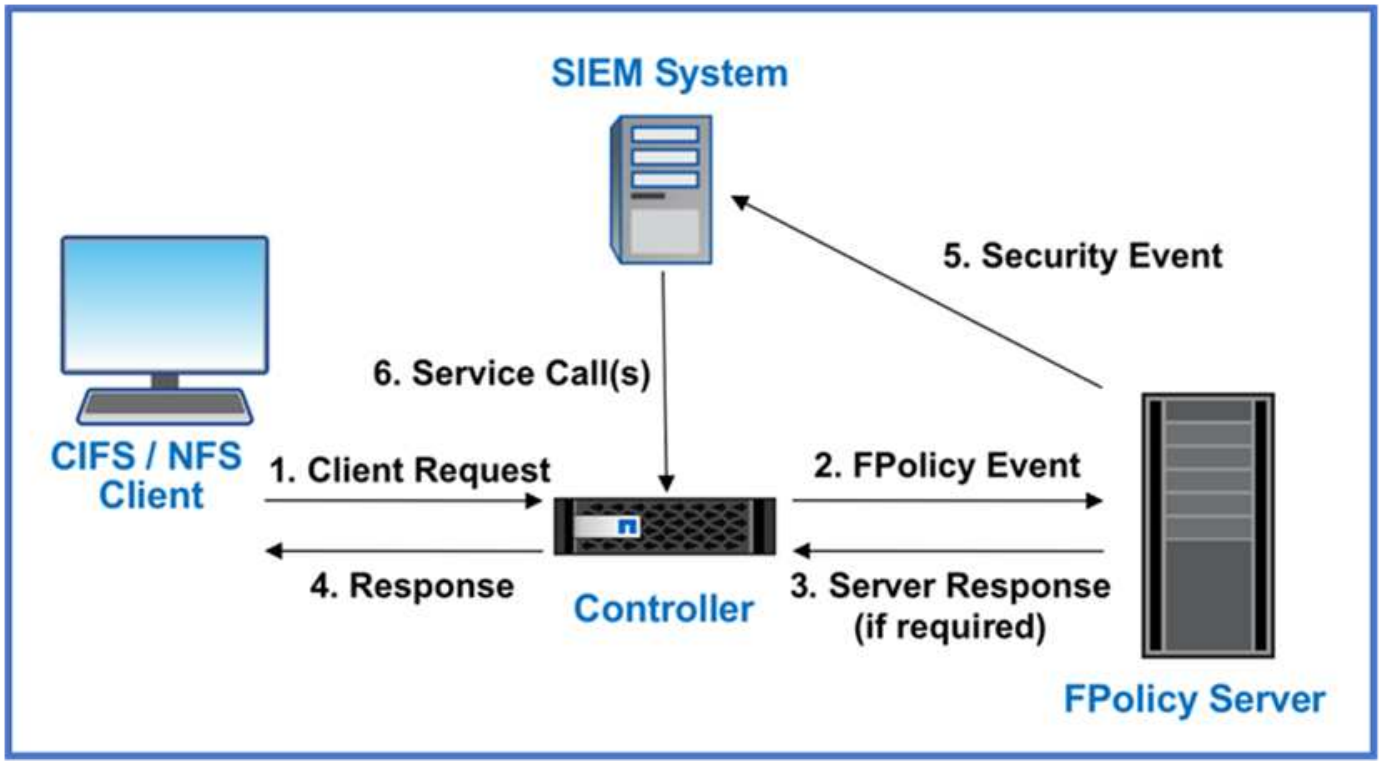
Die ONTAP Verschlüsselung von aktiven Daten sichert den Zugriff auf Benutzerdaten und Zugriff auf Kontrollebene. Der Benutzerdatenzugriff kann durch SMB 3.0-Verschlüsselung für den Zugriff auf Microsoft CIFS-Freigaben oder durch krb5P für NFS Kerberos 5 verschlüsselt werden. Der Zugriff auf Benutzerdaten 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.



NetApps "DII-Speicher-Workload-Sicherheit" nutzt die FPolicy-Schnittstelle und die Benutzerverhaltensanalyse sowohl auf Cloud- als auch auf lokalen ONTAP Speichersystemen, um Sie in Echtzeit vor böswilligem Benutzerverhalten zu warnen. Storage Workload Security schützt Unternehmensdaten durch fortschrittliches maschinelles Lernen und Anomalieerkennung vor Missbrauch durch böswillige oder kompromittierte Benutzer. Storage Workload Security kann Ransomware-Angriffe oder andere schädliche Verhaltensweisen erkennen, Snapshots aufrufen und böswillige Benutzer unter Quarantäne stellen. Storage Workload Security verfügt außerdem über eine forensische Funktion, um Benutzer- und Entitätsaktivitäten detailliert anzuzeigen. Storage Workload Security ist Teil von NetApp Data Infrastructure 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, und ruft einen Snapshot 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.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

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.

Data Infrastructure Insights ist ein Tool zur Infrastrukturüberwachung, das Ihnen Einblick in Ihre gesamte Infrastruktur gibt. Mit Data Infrastructure Insights können Sie alle Ihre Ressourcen überwachen, Fehler beheben und optimieren, einschließlich Ihrer öffentlichen Cloud-Instanzen und Ihrer privaten Rechenzentren. Data Infrastructure Insights kann die durchschnittliche Zeit bis zur Lösung um 90 % verkürzen und verhindern, dass 80 % der Cloud-Probleme Endbenutzer betreffen. Darüber hinaus können Sie die Kosten für die Cloud-Infrastruktur um durchschnittlich 33 % senken und Ihre Anfälligkeit gegenüber Insider-Bedrohungen verringern, indem Sie Ihre Daten mit verwertbaren Informationen schützen. Die Storage Workload Security-Funktion von Data Infrastructure Insights ermöglicht die Analyse des Benutzerverhaltens mit KI und ML, um zu warnen, wenn aufgrund einer Insider-Bedrohung abweichendes Benutzerverhalten auftritt. Für ONTAP nutzt Storage Workload Security die Zero Trust FPolicy-Engine.

Zero-Trust- und Hybrid-Cloud-Implementierungen

NetApp ist die Datenautorität für die Hybrid Cloud. NetApp bietet eine Vielzahl von Optionen zur Erweiterung lokaler Datenmanagementsysteme auf die Hybrid Cloud mit Amazon Web Services (AWS), Microsoft Azure, Google Cloud und anderen führenden Cloud-Anbietern. NetApp Hybrid-Cloud-Lösungen unterstützen dieselben Zero Trust-Sicherheitskontrollen, die auch für lokale ONTAP -Systeme und softwaredefinierten ONTAP Select Speicher verfügbar sind.

Sie können die Kapazität in öffentlichen Clouds ohne die typischen CAPEX-Einschränkungen problemlos erweitern, indem Sie Cloud-native Dateidienste der Enterprise-Klasse für AWS (FSxN), Google Cloud (GCNV) und Azure NetApp Files für Microsoft Azure verwenden. Diese Cloud-Datendienste eignen sich ideal für datenintensive Workloads wie Analysen und DevOps und kombinieren elastischen On-Demand-Speicher als Service von NetApp mit ONTAP Datenmanagement in einem vollständig verwalteten Angebot.

ONTAP ermöglicht die Datenübertragung zwischen Ihren lokalen ONTAP -Systemen und der AWS-, Google Cloud- oder Azure-Speicherumgebung mit der Datenreplikationssoftware NetApp SnapMirror .

Attributbasierte Zugriffssteuerung

Attributbasierte Zugriffssteuerung mit ONTAP

Ab Version 9.12.1 können Sie ONTAP mit NFSv4.2-Sicherheitsetiketten und erweiterten Attributen (xattrs) konfigurieren, um rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) mit Attributen und attributbasierter Zugriffssteuerung (Attribute Based Access Control, ABAC) zu unterstützen.

ABAC ist eine Autorisierungsstrategie, die Berechtigungen basierend auf Benutzerattributen, Ressourcenattributen und Umgebungsbedingungen definiert. Die Integration von ONTAP mit NFS v4.2 Security Labels und xattrs entspricht den NIST Standards für ABAC Lösungen, wie in NIST Special Publication 800-162.

Sie können NFS v4.2-Sicherheitsetiketten und xattrs verwenden, um Dateien benutzerdefinierte Attribute und Labels zuzuweisen. ONTAP kann in die ABAC-orientierte Identitäts- und Zugriffsmanagement-Software integriert werden, um auf der Grundlage dieser Attribute und Labels granulare Richtlinien zur Zugriffskontrolle von Dateien und Ordnern durchzusetzen.

Verwandte Informationen

- "Ansätze für ABAC mit ONTAP"
- "NFS in NetApp ONTAP: Best Practice und Implementierungsleitfaden"

Ansätze zur attributbasierten Zugriffssteuerung (ABAC) in ONTAP

ONTAP bietet verschiedene Ansätze zur Erzielung einer attributbasierten Zugriffssteuerung (File-Level-Based Access Control, ABAC), einschließlich NFS v4.2 Security Labels und Extended Attributes (xattrs) mithilfe von NFS.

NFS v4.2-Sicherheitslabels

Ab ONTAP 9.9 wird die NFS v4.2-Funktion mit der Bezeichnung NFS unterstützt.

NFS v4.2-Sicherheitsetiketten sind eine Möglichkeit, den granularen Datei- und Ordnerzugriff mithilfe von SELinux-Labels und Mandatory Access Control (MAC) zu verwalten. Diese MAC-Labels werden mit Dateien und Ordnern gespeichert und funktionieren in Verbindung mit UNIX-Berechtigungen und NFS v4.x ACLs.

Durch die Unterstützung von NFS v4.2-Sicherheitsetiketten erkennt ONTAP jetzt die SELinux-Label-Einstellungen des NFS-Clients und versteht sie. Die Sicherheitslabels für NFS v4.2 sind in RFC-7204 abgedeckt.

Zu den Anwendungsfällen für die NFS v4.2-Sicherheitslabels gehören:

- MAC-Beschriftung von Virtual Machine (VM) Images
- Datensicherheitsklassifizierung für den öffentlichen Sektor (geheime, streng geheime und andere Klassifizierungen)
- Sicherheits-Compliance
- Diskless Linux

Aktivieren Sie die NFS v4.2-Sicherheitsetiketten

Sie können die NFS v4.2-Sicherheitsetiketten mit dem folgenden Befehl aktivieren oder deaktivieren (erweiterte Berechtigung erforderlich):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Erfahren Sie mehr über `vserver nfs modify` in der "ONTAP-Befehlsreferenz".

Durchsetzungsmodi für NFS v4.2-Sicherheitslabels

Ab ONTAP 9.9 unterstützt ONTAP die folgenden Erzwingungsmodi:

- **Eingeschränkter Servermodus**: ONTAP kann die Labels nicht erzwingen, sondern speichern und übertragen.

  Die Möglichkeit, MAC-Labels zu ändern, liegt bei der Durchsetzung durch den Client.

- **Gastmodus**: Wenn der Client nicht NFS-aware (v4.1 oder niedriger) ist, werden MAC-Labels nicht übertragen.

  ONTAP unterstützt derzeit nicht den Vollmodus (Speichern und Erzwingen von MAC-Etiketten).

Beispiele für Sicherheitsetiketten in NFS v4.2

Die folgende Beispielkonfiguration zeigt Konzepte mit Red hat Enterprise Linux Version 9.3 (Plough).

Der Benutzer `jrsmith`, der basierend auf den Anmeldeinformationen von John R. Smith erstellt wurde, hat das folgende Konto Privileges:

- Benutzername = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Es gibt zwei Rollen: Das Administratorkonto, das ein privilegierter Benutzer und ein Benutzer ist `jrsmith`, wie in der folgenden MLS-Privileges-Tabelle beschrieben:

Benutzer	Rolle	Typ	Stufen
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

In dieser Beispielumgebung hat der Benutzer `jrsmith` Zugriff auf Dateien auf den Ebenen `s0` bis `s3`. Wir können die bestehenden Sicherheitsklassifizierungen wie unten beschrieben verbessern, um sicherzustellen, dass Administratoren keinen Zugriff auf benutzerspezifische Daten haben.

- s0 = Berechtigungsverwaltung Benutzerdaten

- s0 = nicht klassifizierte Daten
- s1 = vertraulich
- s2 = geheime Daten
- s3 = Top-Geheimdaten

Beispiel für NFS v4.2-Sicherheitsetiketten mit MCS

Zusätzlich zu Multi-Level Security (MLS) können Sie mit einer weiteren Funktion namens Multi-Category Security (MCS) Kategorien wie Projekte definieren.

NFS-Sicherheitsetikett	Wert
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Erweiterte Attribute (xattrs)

Ab ONTAP 9.12.1 unterstützt ONTAP xattrs. Xattrs ermöglicht die Zuordnung von Metadaten zu Dateien und Verzeichnissen über das hinaus, was vom System bereitgestellt wird, wie z. B. Zugriffskontrolllisten (ACLs) oder benutzerdefinierte Attribute.

Um xattrs zu implementieren, können Sie und `getfattr` Kommandozeilen-Dienstprogramme in Linux verwenden `setfattr`. Diese Tools bieten eine leistungsstarke Möglichkeit, zusätzliche Metadaten für Dateien und Verzeichnisse zu managen. Sie sollten mit Vorsicht eingesetzt werden, da eine unsachgemäße Verwendung zu unerwartetem Verhalten oder Sicherheitsproblemen führen kann. Detaillierte Anweisungen zur Verwendung finden Sie stets auf den `setfattr` Manpages und `getfattr` in anderen zuverlässigen Dokumentationen.

Wenn xattrs auf einem ONTAP-Dateisystem aktiviert ist, können Benutzer beliebige Attribute auf Dateien festlegen, ändern und abrufen. Diese Attribute können verwendet werden, um zusätzliche Informationen über die Datei zu speichern, die nicht von den standardmäßigen Dateiattributen erfasst werden, z. B. Informationen zur Zugriffssteuerung.

Für die Verwendung von xattrs in ONTAP gibt es mehrere Anforderungen und Grenzen:

- Red hat Enterprise Linux 8.4 oder höher
- Ubuntu 22.04 oder höher
- Jede Datei kann bis zu 128 xattrs haben
- Xattr-Schlüssel sind auf 255 Byte begrenzt
- Die kombinierte Schlüssel- oder Wertgröße beträgt 1,729 Byte pro xattr
- Verzeichnisse und Dateien können xattrs haben
- Zum Festlegen und Abrufen von xattrs `w` oder Schreibmodus müssen Bits für den Benutzer und die Gruppe aktiviert sein

Xattrs werden innerhalb des Benutzer-Namespace verwendet und haben keine intrinsische Bedeutung für ONTAP selbst. Stattdessen werden ihre praktischen Anwendungen ausschließlich von der Client-seitigen Anwendung bestimmt und verwaltet, die mit dem Dateisystem interagiert.

Anwendungsbeispiele für xattr:

- Aufzeichnen des Namens der Anwendung, die für die Erstellung einer Datei verantwortlich ist
- Beibehalten eines Verweises auf die E-Mail-Nachricht, aus der eine Datei abgerufen wurde
- Einrichten eines Kategorisierungsrahmens für die Organisation von Dateiobjekten
- Beschriften von Dateien mit der URL ihrer ursprünglichen Download-Quelle

Befehle zum Verwalten von xattrs

- `setfattr` Legt ein erweitertes Attribut einer Datei oder eines Verzeichnisses fest:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Beispielbefehl:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` Ruft den Wert eines bestimmten erweiterten Attributs ab oder listet alle erweiterten Attribute einer Datei oder eines Verzeichnisses auf:

  Spezifisches Attribut:
  `getfattr -n <attribute_name> <file or directory name>`

  Alle Attribute:
  `getfattr <file or directory name>`

  Beispielbefehl:

  ```
  getfattr -n user.comment example.txt
  ```

Beispiele für das Schlüsselwertpaar xattr

In der folgenden Tabelle sind zwei Beispiele für das Schlüsselwertpaar xattr aufgeführt:

Xattr	Wert
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Benutzerberechtigungen mit ACE für xattrs

Ein Access Control Entry (ACE) ist eine Komponente innerhalb einer ACL, die die Zugriffsrechte oder Berechtigungen definiert, die einem einzelnen Benutzer oder einer Benutzergruppe für eine bestimmte Ressource, z. B. eine Datei oder ein Verzeichnis, gewährt werden. Jeder ACE gibt die Art des erlaubten oder abgelehnten Zugriffs an und ist mit einem bestimmten Sicherheitsprinzipal (Benutzer- oder Gruppenidentität) verknüpft.

Access Control Entry (ACE) für xattrs erforderlich

- Abrufen von xattr: Die Berechtigungen, die ein Benutzer benötigt, um die erweiterten Attribute einer Datei oder eines Verzeichnisses zu lesen. Das „R“ bedeutet, dass Leseberechtigung erforderlich ist.
- Xattrs festlegen: Die Berechtigungen, die zum Ändern oder Festlegen der erweiterten Attribute benötigt werden. „A“, „w“ und „T“ stellen verschiedene Beispiele für Berechtigungen wie Append, Write und eine bestimmte Berechtigung in Bezug auf xattrs dar.
- Dateien: Benutzer benötigen Append, Write und möglicherweise eine spezielle Berechtigung im Zusammenhang mit xattrs, um erweiterte Attribute zu setzen.
- Verzeichnisse: Eine bestimmte Berechtigung "T" ist erforderlich, um erweiterte Attribute zu setzen.

Dateityp	Xattr. Abrufen	Xattrs einstellen
Datei	R	A,w,T
Verzeichnis	R	T

Integration mit ABAC Identitäts- und Zugriffskontrollsoftware

Um die Funktionen von ABAC voll auszuschöpfen, kann ONTAP in eine ABAC-orientierte Identitäts- und Zugriffsverwaltungssoftware integriert werden.

In einem ABAC-System spielen der Policy Enforcement Point (PEP) und der Policy Decision Point (PDP) eine entscheidende Rolle. Der PEP ist für die Durchsetzung von Zugriffssteuerungsrichtlinien verantwortlich, während der PDP die Entscheidung darüber trifft, ob der Zugriff auf der Grundlage der Richtlinien gewährt oder verweigert werden soll.

In einer praktischen Umgebung würde ein Unternehmen eine Mischung aus NFS-Sicherheitsetiketten und xattrs einsetzen. Diese werden verwendet, um eine Vielzahl von Metadaten darzustellen, einschließlich Klassifizierung, Sicherheit, Anwendung und Inhalt, die alle entscheidend für ABAC Entscheidungen sind. Xattrs, zum Beispiel, kann verwendet werden, um die Ressourcenattribute zu speichern, die die PDP für seinen Entscheidungsprozess verwendet. Ein Attribut kann definiert werden, um die Klassifizierungsstufe einer Datei darzustellen (z. B. „nicht klassifiziert“, „vertraulich“, „geheim“ oder „streng geheim“). Die PDP könnte dann dieses Attribut nutzen, um eine Richtlinie durchzusetzen, die Benutzern den Zugriff auf Dateien einschränkt, die eine Klassifizierungsstufe haben, die ihrem Sicherheitsniveau entspricht oder kleiner ist.

Dieser Inhalt setzt voraus, dass die Identitäts-, Authentifizierungs- und Zugriffsdienste des Kunden mindestens einen PEP und ein PDP umfassen, die als Vermittler für den Zugriff auf das Dateisystem fungieren.

Beispiel für einen Prozessablauf für ABAC

1. Benutzer stellt Anmeldeinformationen (z. B. PKI, OAuth, SAML) für den Systemzugriff auf PEP bereit und ruft Ergebnisse von PDP ab.

   Die Rolle des PEP besteht darin, die Zugriffsanforderung des Benutzers abzufangen und an das PDP weiterzuleiten.

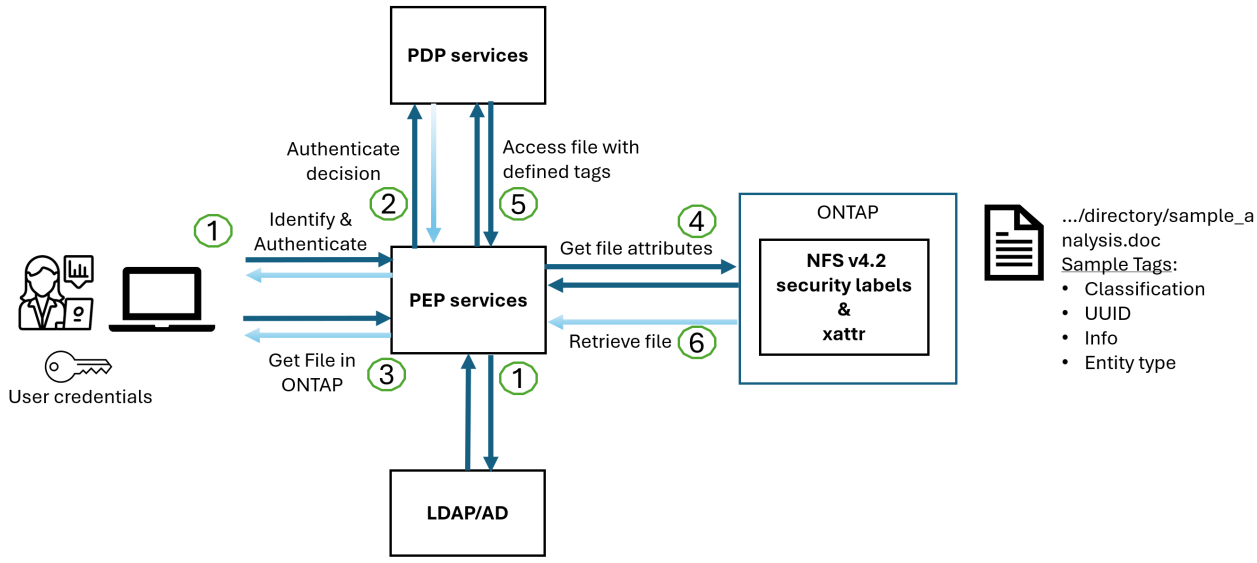
2. Die PDP wertet diese Anforderung dann anhand der festgelegten ABAC-Richtlinien aus.

   In diesen Richtlinien werden verschiedene Attribute berücksichtigt, die sich auf den Benutzer, die betreffende Ressource und die Umgebung beziehen. Auf der Grundlage dieser Richtlinien trifft die PDP eine Zugriffsentscheidung, entweder zuzulassen oder abzulehnen, und teilt diese Entscheidung dann dem PEP zurück.

PDP stellt PEP Richtlinien zur Durchsetzung bereit. Der PEP erzwingt dann diese Entscheidung, indem er die Zugriffsanfrage des Benutzers gemäß der Entscheidung des PDP entweder gewährt oder ablehnt.

3. Nach einer erfolgreichen Anfrage fordert der Benutzer eine in ONTAP gespeicherte Datei an (z. B. AFF, AFF-C).
4. Wenn die Anforderung erfolgreich war, erhält PEP fein abgestufte Zugangskontroll-Tags aus dem Dokument.
5. PEP fordert die Richtlinie für den Benutzer auf Grundlage der Zertifikate dieses Benutzers an.
6. PEP trifft eine Entscheidung auf der Grundlage von Richtlinien und Tags, wenn der Benutzer Zugriff auf die Datei hat, und lässt den Benutzer die Datei abrufen.

Der eigentliche Zugriff kann mit Token erfolgen.



ONTAP Cloning und SnapMirror

Die Klon- und SnapMirror-Technologien von ONTAP bieten effiziente und zuverlässige Datenreplizierungs- und Klonfunktionen und stellen sicher, dass alle Aspekte von Dateidaten, einschließlich xattrs, zusammen mit der Datei erhalten und übertragen werden. Xattrs sind wichtig, da sie zusätzliche Metadaten, die einer Datei zugeordnet sind, wie z. B. Sicherheitslabels, Zugriffskontrollinformationen und benutzerdefinierte Daten, speichern. Diese sind für die Aufrechterhaltung des Kontexts und der Integrität dieser Datei von wesentlicher Bedeutung.

Wenn ein Volume mit der FlexClone-Technologie von ONTAP geklont wird, wird ein exaktes, beschreibbares Replikat des Volumes erstellt. Dieser Klonprozess ist sofort und platzsparend und umfasst alle Dateidaten und Metadaten, um sicherzustellen, dass xattrs vollständig repliziert werden. SnapMirror sorgt auf ähnliche Weise dafür, dass Daten originalgetreu auf ein sekundäres System gespiegelt werden. Dazu gehört xattrs, die entscheidend sind für Anwendungen, die auf diese Metadaten angewiesen sind, um korrekt zu funktionieren.

Durch die Einbeziehung von xattrs sowohl beim Klonen als auch bei der Replizierung stellt NetApp ONTAP sicher, dass der vollständige Datensatz mit allen seinen Merkmalen verfügbar und konsistent über primäre und sekundäre Storage-Systeme hinweg ist. Dieser umfassende Datenmanagementansatz ist für Unternehmen unerlässlich, die eine konsistente Datensicherung, schnelle Wiederherstellung und die Einhaltung von Compliance- und gesetzlichen Standards benötigen. Zudem vereinfacht sie das Management von Daten in verschiedenen Umgebungen, sowohl vor Ort als auch in der Cloud. Benutzer können sich darauf verlassen,

dass ihre Daten während dieser Prozesse vollständig und unverändert sind.

> Für NFS v4.2-Sicherheits-Labels sind die Einschränkungen definiert inNFS v4.2-Sicherheitslabels.

Prüfen von Änderungen an Beschriftungen

Das Auditing von Änderungen an xattrs oder NFS-Sicherheitsetiketten ist ein wichtiger Aspekt der Verwaltung und Sicherheit von Dateisystemen. Standard-Dateisystemauditing-Tools ermöglichen die Überwachung und Protokollierung aller Änderungen an einem Dateisystem, einschließlich Änderungen an xattrs und Sicherheitsetiketten.

In Linux-Umgebungen wird der `auditd` Daemon häufig verwendet, um Auditing für Dateisystemereignisse einzurichten. Es ermöglicht Administratoren, Regeln zu konfigurieren, um auf bestimmte Systemaufrufe im Zusammenhang mit xattr-Änderungen zu achten, wie `setxattr`,, `lsetxattr` und `fsetxattr` um Attribute und, `lremovexattr` zu setzen `removexattr` und `fremovexattr` Attribute zu entfernen.

ONTAP FPolicy erweitert diese Funktionen durch ein robustes Framework für das Monitoring und die Kontrolle von Dateivorgängen in Echtzeit. FPolicy kann zur Unterstützung verschiedener xattr-Ereignisse konfiguriert werden. Dies ermöglicht eine granulare Kontrolle über Dateivorgänge und die Durchsetzung umfassender Datenmanagement-Richtlinien.

Für Benutzer, die xattrs verwenden, insbesondere in NFS v3- und NFS v4-Umgebungen, werden nur bestimmte Kombinationen von Dateioperationen und -Filtern für die Überwachung unterstützt. Die Liste der unterstützten Dateioperationen und Filterkombinationen für das FPolicy Monitoring von NFS v3- und NFS v4-Dateizugriffsereignissen ist unten detailliert:

Unterstützte Dateivorgänge	Unterstützte Filter
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

Beispiel eines auditd-Protokollausschlags für eine setattr-Operation:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Die Aktivierung "ONTAP FPolicy" für Benutzer, die mit xattrs arbeiten, bietet eine Ebene der Sichtbarkeit und Kontrolle, die für die Aufrechterhaltung der Integrität und Sicherheit des Dateisystems unerlässlich ist. Mithilfe

der erweiterten Monitoring-Funktionen von FPolicy können Unternehmen sicherstellen, dass alle Änderungen an xattrs nachverfolgt, geprüft und an ihren Sicherheits- und Compliance-Standards ausgerichtet werden. Dieser proaktive Ansatz beim Filesystem-Management ist daher die Aktivierung von ONTAP FPolicy nur für Unternehmen empfehlenswert, die ihre Daten-Governance- und Sicherungsstrategien verbessern möchten.

Beispiele für die Kontrolle des Zugriffs auf Daten

Der folgende Beispieleintrag für Daten, die in John R. Smiths PKI-Zertifikat gespeichert sind, zeigt, wie der Ansatz von NetApp auf eine Datei angewendet werden kann und eine feingranulare Zugriffskontrolle bietet.

> Diese Beispiele dienen zur Veranschaulichung, und es liegt in der Verantwortung des Kunden, die mit den NFS v4.2-Sicherheitslabels und xattrs verbundenen Metadaten zu ermitteln. Details zur Aktualisierung und Aufbewahrung von Etiketten werden aus einfachen Grund weggelassen.

Beispiel PKI-Zertifikatwerte

Taste	Wert
EntitySecurityMark	t:s01 = NICHT KLASSIFIZIERT

Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

Taste	Wert
Spezifikation	„DoD“
uuid	B4111349-7875-4115-ad30-0928565f2e15

AdminOrganisation	{
	"value": "DoD"
	}

Briefings	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

Bürgerstatus	{
	"value": "US"
	}

Taste	Wert
Abstände	`[ { "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" } ]`
LänderOfMitgliedschaften	`[ { "value": "USA" } ]`
DigitalIdentifier	`{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }`
DissTos	`{ "value": "DoD" }`
DytOrganisation	`{ "value": "DoD" }`

Taste	Wert

EntityType	<pre>{
	"value": "GOV"
	}</pre>

FineAccessControls	<pre>[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]</pre>

Diese PKI-Berechtigungen zeigen die Zugangsdaten von John R. Smith, einschließlich des Zugriffs nach Datentyp und Zuordnung.

In Szenarien, in denen IC-TDF-Metadaten getrennt von der Datei gespeichert werden, empfiehlt NetApp eine zusätzliche Ebene feingranularer Zugriffskontrolle. Dabei werden Informationen zur Zugriffssteuerung sowohl auf Verzeichnisebene als auch in Verbindung mit jeder Datei gespeichert. Betrachten Sie als Beispiel die folgenden Tags, die mit einer Datei verknüpft sind:

- Sicherheitslabels für NFS v4.2: Werden für Sicherheitsentscheidungen verwendet
- Xattrs: Geben Sie ergänzende Informationen, die für die Datei und die Anforderungen an das organisatorische Programm relevant sind

Die folgenden Schlüssel-Wert-Paare sind Beispiele für Metadaten, die als xattrs gespeichert werden können und detaillierte Informationen über den Ersteller der Datei und die zugehörigen Sicherheitsklassifizierungen bieten. Diese Metadaten können von den Client-Applikationen genutzt werden, um fundierte Zugriffsentscheidungen zu treffen und Dateien gemäß den Standards und Anforderungen des Unternehmens zu organisieren.

Beispiel für xattr Schlüssel-Wert-Paare

Taste	Wert
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`

Taste	Wert
`user.specification`	`"INFO"`

Taste	Wert

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Taste	Wert
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
}
```

Verwandte Informationen

- "NFS in NetApp ONTAP: Best Practice und Implementierungsleitfaden"
- "ONTAP-Befehlsreferenz"
- Anforderung von Kommentaren (RFC)
  - "RFC 7204: Anforderungen für gekennzeichnetes NFS"
  - "RFC 2203: RPCSEC_GSS-Protokollspezifikation"
  - "RFC 3530: Network File System (NFS) Version 4 Protocol"