NetApp Lösung für Ransomware

ONTAP Technical Reports

NetApp
January 23, 2026

Inhalt

NetApp Lösung für Ransomware . . . 1
- Ransomware und das Datensicherungsportfolio von NetApp . . . 1
  - Daten sind das primäre Ziel . . . 1
  - Die realen Kosten von Ransomware . . . 1
  - Schutz vor Ransomware auf Datenebene . . . 2
  - Das NetApp Portfolio für Ransomware-Schutz . . . 2
  - Recovery-Garantie bei Ransomware . . . 3
- SnapLock und manipulationssichere Snapshots für den Schutz vor Ransomware . . . 3
  - SnapLock-Compliance . . . 3
  - Manipulationssichere Snapshots . . . 4
- FPolicy Dateisperrung . . . 4
  - Blockieren Sie bösartige Dateien mit dem nativen FPolicy-Modus . . . 4
  - Aktivieren Sie UEBA (User and Entity Behavior Analytics) mit dem externen FPolicy-Modus . . . 5
- Data Infrastructure Insights Speicher-Workload-Sicherheit . . . 5
- In NetApp ONTAP integrierte, KI-basierte Erkennung und Reaktion . . . 6
  - Autonomer Schutz durch Ransomware (ARP) . . . 6
  - Autonomer Ransomware-Schutz/KI (ARP/AI) . . . 6
- Luftgewindelter WORM-Schutz mit Cyber-Vaulting in ONTAP . . . 7
  - Cyber-Vaulting mit SnapLock Compliance und eine logische Luftspalt . . . 7
  - Manipulationssichere Snapshots . . . 8
- Digital Advisor Ransomware-Schutz . . . 8
- Umfassende Ausfallsicherheit mit NetApp Ransomware-Schutz . . . 9
  - NetApp Ransomware-Schutz . . . 9

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.

[Sicherheitsschichten von der Umgebung bis zur Datensicherheit]

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 den Schutz vor Ransomware umfasst die beschriebenen kritischen Attribute]

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.

[Ergebnisse von Angriffen auf die Data Infrastructure Insights und die Speicher-Workload-Sicherheit]

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.

[Logischer Air Gap mit NetApp Cyber Vault]

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.

[Die NetApp überwacht den Systemzustand im Digital Advisor Dashboard]

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.

[NetApp Ransomware Protection bietet KI-basierte Informationen und Unterstützung, die erforderlich sind, um den Verlust von Workload-Daten zu minimieren und eine schnelle Wiederherstellung zu ermöglichen. Dieses Bild zeigt die Benutzeroberfläche der NetApp Console .]

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**.