Über den Ransomware-Schutz von NetApp

ONTAP 9

NetApp
August 31, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/ransomware-solutions/ransomware-overview.html on August 31, 2024. Always check docs.netapp.com for the latest.

Inhalt

Über den Ransomware-Schutz von NetApp . . . 1
Ransomware und das Datensicherungsportfolio von NetApp . . . 1
SnapLock und manipulationssichere Snapshot Kopien für den Schutz vor Ransomware . . . 3
FPolicy Dateisperrung . . . 4
Cloud Insights Storage-Workload-Sicherheit (CISWS) . . . 5
In NetApp ONTAP integrierte, KI-basierte Erkennung und Reaktion . . . 6
LUFTGEZAPFTEM WORM-Schutz mit Cyber-Vaulting . . . 7
Active IQ Ransomware-Schutz . . . 8
Umfassende Ausfallsicherheit mit BlueXP Ransomware-Schutz . . . 9

Über den Ransomware-Schutz von NetApp

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 wurde der Inhalt des technischen Berichts *TR-4572: NetApp Ransomware Protection*, der zuvor als PDF veröffentlicht wurde, in die restliche ONTAP Produktdokumentation integriert.

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 "BlueXP vor Ransomware-Schutz"verringert die Betriebslast mithilfe einer zentralen Kontrollebene, mit der sich eine vollständige, Workload-zentrierte Ransomware-Verteidigung auf intelligente Weise koordinieren und ausführen lässt. So können Sie mit einem einzigen Klick kritische Workload-Daten identifizieren und schützen. Sie können dann den Einfluss eines potenziellen Angriffs exakt und automatisch erkennen und darauf reagieren, damit er die Auswirkungen eines Angriffs begrenzen kann. Zudem lassen sich Workloads innerhalb von Minuten statt Tagen wiederherstellen. So werden Ihre wertvollen Workload-Daten geschützt und kostspielige Unterbrechungen 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 Snapshot Kopien 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 designierte Administratorgenehmiger konfigurieren, wie Sie möchten, bevor eine Snapshot-Kopie 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

- "Active IQ Ransomware-Schutz"
- "Cloud Insights Storage-Workload-Sicherheit (CISWS)"
- "FPolicy"
- "SnapLock und manipulationssichere Snapshot Kopien"

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 http://mysupport.netapp.com/ontap/resources
- NetApp Produktsicherheit https://security.netapp.com/resources/

SnapLock und manipulationssichere Snapshot Kopien 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 Snapshot Kopien

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 die primäre Snapshot-Kopie von einem ONTAP-Administrator gelöscht wird, der dieselbe SnapLock-Aufbewahrungsfrist verwendet. Das Löschen von Snapshot Kopien wird auch dann verhindert, wenn das Volume nicht SnapLock aktiviert ist, obwohl Snapshots nicht dieselbe unlöschbare Eigenschaft von SnapLock Compliance Volumes aufweisen.

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

Weitere Informationen .

- "Sperren Sie eine Snapshot Kopie, 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 BlueXP 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."

Cloud Insights Storage-Workload-Sicherheit (CISWS)

Storage Workload Security (SWS) ist eine Funktion von NetApp Cloud Insights, die die Sicherheit, Wiederherstellbarkeit und Verantwortlichkeit einer ONTAP-Umgebung erheblich verbessert. SWS verfolgt einen benutzerzentrierten Ansatz, der alle Dateiaktivitäten von jedem authentifizierten Benutzer in der Umgebung verfolgt. Es verwendet erweiterte Analysen, um normale und saisonale Zugriffsmuster für jeden Benutzer zu erstellen. Diese Muster erkennen verdächtige Verhaltensmuster schnell, ohne dass Ransomware-Signaturen erforderlich sind.

Wenn SWS einen potenziellen Ransomware-, Datenlösch- oder Exfiltrationsangriff erkennt, kann es folgende automatische Aktionen ausführen:

- 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 Cloud Insights-Angriffen zur Storage-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 .

- "NetApp Cloud 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 anormale Aktivitäten erkannt werden, wird sofort eine automatische Snapshot-Kopie erstellt. Dadurch wird ein Wiederherstellungspunkt nahe des Angriffs mit minimalen infizierten Daten erstellt. 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"

LUFTGEZAPFTEM WORM-Schutz mit Cyber-Vaulting

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 beseitigen Sie die Komplexität von Tape- oder Festplattenablösungen mit logischem Air Gating, das mit unveränderlichen Snapshot Kopien und NetApp SnapLock Compliance erreicht werden kann.

[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 Snapshot-Kopien in SnapLock Volumes speichern, damit die Kopien auf WORM gespeichert werden können, um das Löschen zu verhindern. Es gibt zwei SnapLock-Lizenzversionen: SnapLock Compliance und SnapLock Enterprise. Für den Schutz vor Ransomware empfiehlt NetApp SnapLock Compliance, da Sie einen bestimmten Aufbewahrungszeitraum festlegen können, in dem Snapshot Kopien gesperrt sind und nicht gelöscht werden können – selbst von ONTAP Administratoren oder der Unterstützung von NetApp.

Weitere Informationen .

- "Blog: Mehrschichtiger Schutz vor Ransomware mit der Cyber Vault-Lösung von NetApp"

Manipulationssichere Snapshot Kopien

SnapLock Compliance als logische Air Gap bietet Ihnen den ultimativen Schutz, um zu verhindern, dass Angreifer Ihre Backup-Kopien löschen. Allerdings müssen Sie die Snapshot-Kopien 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 der Snapshot Kopie eines primären Volumes auf dem Primärspeicher.

Ab ONTAP 9.12.1 bieten manipulationssichere Snapshot Kopien Schutz auf SnapLock Compliance-Ebene für Ihre Snapshot-Kopien auf primärem Storage und primären Volumes. Es besteht keine Notwendigkeit, die Snapshot-Kopie mit SnapVault auf ein sekundäres SnapLocked-Volume zu speichern. Manipulationssichere Snapshot Kopien setzen die SnapLock Technologie ein, um zu verhindern, dass die primäre Snapshot Kopie 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 eine manipulationssichere, geschützte Snapshot Kopie gesichert wird. Dies ist mit einer herkömmlichen SnapLock Compliance vaulted Snapshot Kopie nicht möglich.

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

Weitere Informationen .

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

Active IQ Ransomware-Schutz

NetApp Active IQ ist ein digitaler Berater, der die proaktive Betreuung und Optimierung von NetApp Storage mithilfe nützlicher Informationen für optimales Datenmanagement vereinfacht. Dank der Telemetriedaten unserer sehr unterschiedlichen installierten Basis nutzt das System fortschrittliche KI- und ML-Techniken, um Chancen zur Risikominimierung und zur Verbesserung der Performance und Effizienz Ihrer Storage-Umgebung zu erkennen.

Das kann nicht nur "NetApp Active IQ" 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 Active IQ Konsole überwacht den Systemzustand]

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

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

Active IQ Ransomware-Schutz in Aktion sehen:"NetApp Active IQ"

Umfassende Ausfallsicherheit mit BlueXP Ransomware-Schutz

Es ist wichtig, dass Ransomware-Erkennung so früh wie möglich erfolgt, damit Sie die Ausbreitung verhindern und kostspielige Ausfallzeiten vermeiden können. Eine effektive Strategie zur Erkennung von Ransomware sollte jedoch mehr als eine einzige Schutzschicht umfassen. Zum Schutz vor Ransomware bei NetApp gehört ein umfassender Ansatz. Dazu gehören integrierte Echtzeit-Funktionen, die sich auf Datenservices mithilfe von BlueXP erweitern, sowie eine isolierte und mehrstufige Lösung für CyberArchivierung.

BlueXP vor Ransomware-Schutz

BlueXP ist eine zentrale Managementoberfläche für die intelligente Orchestrierung eines umfassenden, Workload-zentrierten Ransomware-Schutzes. BlueXP zum Schutz vor Ransomware führt die leistungsstarken Funktionen von ONTAP zur Cyberresilienz zusammen: ARP, FPolicy und manipulationssichere Snapshots sowie BlueXP Datenservices wie BlueXP Backup und Recovery. Außerdem geben Sie dort Empfehlungen und Anleitungen in automatisierten Workflows ein, um über eine zentrale Benutzeroberfläche eine lückenlose Verteidigung zu ermöglichen. Er wird auf Workload-Ebene ausgeführt, um zu gewährleisten, dass die Applikationen, die Ihr Unternehmen führen, geschützt sind und im Falle eines Angriffs so schnell wie möglich wiederhergestellt werden können.

[BlueXP Ransomware Protection ist KI-basiertes Wissen und Unterstützung, die erforderlich sind, um Workload-Datenverluste zu minimieren und schnell wieder ins Normalität zurückzukehren. Dieses Bild zeigt die BlueXP -Benutzeroberfläche.]

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

"BlueXP vor Ransomware-Schutz" Macht diese NIST-Funktionen einfacher zu erreichen:

- 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**.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.