



Dokumentation zum Schutz durch Ransomware

Ransomware Protection

NetApp
January 09, 2023

This PDF was generated from <https://docs.netapp.com/de-de/cloud-manager-ransomware/index.html> on January 09, 2023. Always check docs.netapp.com for the latest.

Inhaltsverzeichnis

- Dokumentation zum Schutz durch Ransomware 1
- Was ist neu mit Ransomware Schutz 2
 - 9 Januar 2023 2
 - Bis 11. Dezember 2022 2
 - 13. November 2022 2
 - 6. September 2022. 2
 - 7. August 2022 3
 - 12. Juni 2022 3
 - 11 Mai 2022 4
 - 15 März 2022 4
 - 9 Februar 2022. 4
- Los geht's 5
 - Erfahren Sie mehr über Ransomware-Schutz 5
 - Monitoring des Status von Ransomware-Warnmeldungen 7
- Verwenden Sie Ransomware-Schutz 8
 - Verwalten von Cyber-Sicherheitsempfehlungen für Ihre Datenquellen 8
- Wissen und Support 26
 - Für den Support anmelden 26
 - Holen Sie sich Hilfe 30
- Rechtliche Hinweise 34
 - Urheberrecht 34
 - Marken 34
 - Patente 34
 - Datenschutzrichtlinie 34
 - Open Source 34

Dokumentation zum Schutz durch Ransomware

Was ist neu mit Ransomware Schutz

Alles zum Schutz vor Ransomware.

9 Januar 2023

Unterstützung wurde hinzugefügt, um Ransomware-Schutz-Benachrichtigungen per E-Mail und im Notification Center zu erhalten

Ransomware Protection ist in den BlueXP Notification Service integriert. Sie können Ransomware-Schutzbenachrichtigungen anzeigen, indem Sie in der BlueXP-Menüleiste auf die Benachrichtigungsglocke klicken. Sie können BlueXP auch so konfigurieren, dass Benachrichtigungen per E-Mail als Benachrichtigungen gesendet werden, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht im System angemeldet sind. Die E-Mail kann an alle Empfänger gesendet werden, die auf Ransomware-Warnungen achten müssen. ["Erfahren Sie, wie"](#).

Bis 11. Dezember 2022

Neue Empfohlene Maßnahmen wurden zur Ransomware Protection Score Panel hinzugefügt

Für die folgenden Ransomware-Sicherungsprobleme in Ihren Storage-Systemen werden nun zwei neue Empfehlungen angezeigt:

- *Berechtigungen für X-sensible Objekte mit breiten Berechtigungen verkleinern* - in Ihren Datenquellen wurden sensible Dateien mit offenen Berechtigungen gefunden
- *Patch X Open CVEs Across Y-Datenquellen* - Unpatched CVEs wurden auf Ihren ONTAP-Systemen gefunden

Sie können diese Aktionen in der UI auswählen und dann den Workflow befolgen, um die zugrunde liegenden Probleme zu lösen. ["Siehe die Liste aller empfohlenen Maßnahmen"](#).

13. November 2022

Neue Panels zur Anzeige Ihrer gesamten Ransomware-Schutzpunktzahl und empfohlenen Maßnahmen

Das *Ransomware Protection Score* Panel zeigt die Gesamtpunktzahl und die Bereiche der Cybersicherheit, in denen potenzielle Probleme bestehen. Im Panel *Recommended Actions* werden die möglichen Maßnahmen aufgeführt, die Sie ergreifen können, um Ihre Widerstandsfähigkeit gegen einen Ransomware-Angriff zu verbessern, und es wird ein Link zur Untersuchung der Probleme angezeigt, damit Sie die Maßnahmen gegebenenfalls anwenden können. Diese beiden neuen Felder arbeiten zusammen, um zu ermitteln, wie stabil Ihre Daten bei einem Ransomware-Angriff ist und was Sie tun können, um Ihren Wert zu verbessern. ["Hier erfahren Sie mehr"](#).

6. September 2022

Neues Panel zur Anzeige von Ransomware-Vorfällen auf Ihren Clustern erkannt

Der Bereich *Ransomware Incidents* zeigt Ransomware-Angriffe auf Ihren Systemen. Aktuell werden ONTAP Cluster vor Ort unterstützt, auf denen Autonomous Ransomware Protection (ARP) ausgeführt wird. ARP nutzt Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Aktivitäten, die auf einen Ransomware-Angriff hinweisen könnten, proaktiv zu erkennen und zu warnen. ["Hier erfahren Sie mehr"](#).

7. August 2022

Neues Panel zur Anzeige von Sicherheitsschwachstellen auf Ihren Clustern

Das Fenster *Speichersystemsicherheitsschwachstellen* zeigt die Gesamtzahl der hohen, mittleren und niedrigen Sicherheitslücken, die das Active IQ Digital Advisor Tool auf jedem Ihrer ONTAP Cluster gefunden hat. Hohe Schwachstellen sollten sofort untersucht werden, um sicherzustellen, dass Ihre Systeme nicht für Angriffe geöffnet sind. ["Weitere Informationen finden Sie hier"](#).

Neues Fenster zum Anzeigen unveränderlicher gescannter Dateien

Die *kritische Unveränderlichkeit* zeigt die Anzahl der Elemente in Ihrer Arbeitsumgebung, die dank der ONTAP SnapLock Technologie vor Modifizierung und Löschung in WORM-Storage geschützt sind. So sehen Sie, wie viele Ihrer Daten eine unveränderliche Kopie haben, damit Sie ein besseres Verständnis Ihrer Backup- und Recovery-Pläne gegen Ransomware erhalten. ["Weitere Informationen finden Sie hier"](#).

12. Juni 2022

Der NAS-Filesystem-Audit-Status wird jetzt für Ihre ONTAP Storage VMs nachverfolgt

Der *Cyber Resilience Map* wird eine Warnmeldung hinzugefügt, wenn in weniger als 40 % der Storage VMs in der Arbeitsumgebung die Dateisystemprüfung aktiviert ist. Sie können die genaue Anzahl der SVMs anzeigen, die SMB- und NFS-Ereignisse nicht in einem Audit-Protokoll im Fenster „*Harden Your ONTAP Environment*“ nachverfolgen und protokollieren. Anschließend können Sie entscheiden, ob das Auditing über diese SVMs aktiviert werden soll.

Warnmeldungen werden jetzt angezeigt, wenn On-Box-Anti-Ransomware nicht für Ihre Volumes aktiv ist

Diese Informationen wurden zuvor im Panel *Harden Your ONTAP Environments* für On-Prem-ONTAP-Systeme gemeldet. Aber jetzt wird in der *Cyber Resilience Map* ein Alarm gemeldet, wenn die integrierte Anti-Ransomware-Funktion in weniger als 40 % der Volumes aktiviert ist, damit Sie diese Informationen im Dashboard anzeigen können.

FSX für ONTAP Systeme werden nun für die Aktivierung von Volume Snapshots nachverfolgt

Das Fenster „*Harden Your ONTAP Environments*“ stellt jetzt den Status von Snapshot Kopien für Volumes auf Ihren FSX für ONTAP Systeme bereit. Wenn weniger als 40 % der Volumes durch Snapshots geschützt werden, erhalten Sie auch eine Warnung in der *Cyber Resilience Map*.

11 Mai 2022

Neues Panel zur Überwachung der Sicherheit in Ihren ONTAP-Umgebungen

Ein neues Panel *Harden Your ONTAP Environments* gibt den Status bestimmter Einstellungen in Ihren ONTAP-Systemen an, die verfolgen, wie sicher Ihre Bereitstellung gemäß dem ist ["NetApp Leitfaden zur verstärkte Sicherheit von ONTAP-Systemen"](#) Und zum ["ONTAP Anti-Ransomware-Funktion"](#) Die ungewöhnliche Aktivitäten proaktiv erkennen und warnen.

Sie können die Empfehlungen prüfen und anschließend entscheiden, wie Sie potenzielle Probleme beheben möchten. Sie können die Schritte befolgen, um die Einstellungen auf Ihren Clustern zu ändern, die Änderungen auf ein anderes Mal zu verschieben oder den Vorschlag zu ignorieren. ["Weitere Informationen finden Sie hier"](#).

Neues Fenster zum Schutz verschiedener Datenkategorien mit Cloud Backup

In diesem neuen *Backup Status* Panel wird aufgezeigt, wie umfassend Ihre wichtigsten Datenkategorien gesichert werden, falls Sie eine Wiederherstellung aufgrund eines Ransomware-Angriffs benötigen. Diese Daten sind in einer visuellen Darstellung der Anzahl der durch Cloud Backup gesicherten Elemente einer bestimmten Kategorie in einer Umgebung dargestellt. ["Weitere Informationen finden Sie hier"](#).

15 März 2022

Neues Feld, um den Berechtigungsstatus Ihrer geschäftskritischen Daten zu verfolgen

Ein neues Panel *Analyse von geschäftskritischen Datenberechtigungen* zeigt den Berechtigungsstatus von Daten an, die für Ihr Unternehmen von entscheidender Bedeutung sind. So können Sie schnell einschätzen, wie gut Sie Ihre geschäftskritischen Daten schützen. ["Weitere Informationen finden Sie hier"](#).

Öffnen Sie Permissions Area umfasst nun OneDrive- und SharePoint-Konten

Der Bereich „Offene Berechtigungen“ im Ransomware Protection Dashboard umfasst nun die Berechtigungen für Dateien, die in OneDrive-Konten und SharePoint-Konten gescannt werden.

9 Februar 2022

Neuer Ransomware-Schutz Service

Mit dem neuen Ransomware-Schutz-Service können Sie relevante Informationen über Cybersicherheit anzeigen und beurteilen, wie belastbar Ihre Daten für einen Cyber-Angriff sind. Außerdem erhalten Sie eine Liste mit Alarmen und Lösungen, um Ihre Daten sicherer zu machen.

["Erfahren Sie mehr über diesen neuen Service"](#).

Los geht's

Erfahren Sie mehr über Ransomware-Schutz

Ransomware-Angriffe können das Unternehmen Zeit, Ressourcen und Image-Schäden kosten. Mit dem BlueXP (früher Cloud Manager) Ransomware Protection Service können Sie relevante Informationen zur Cybersicherheit anzeigen und beurteilen, wie widerstandsfähig Ihr Unternehmen ist für einen Cyber-Angriff. Außerdem erhalten Sie eine Liste mit Alarmen und Lösungen, um Ihre Daten sicherer zu machen.

["Erfahren Sie mehr über Anwendungsfälle zum Schutz vor Ransomware"](#).



Der Ransomware-Schutz-Service ist derzeit ein Beta-Angebot.

Funktionen

Ransomware Protection bietet einen zentralen Kontrollpunkt für das Management und die Optimierung der Datensicherheit in verschiedenen Arbeitsumgebungen und Infrastrukturebenen, um besser auf Bedrohungen reagieren zu können, wenn sie auftreten. Es bietet derzeit mehrere Funktionen, die Ihnen bei der Sicherung von Cyberspeichern helfen können. Aktuelle Funktionen bestimmen, wann:

- Durch regelmäßige Snapshot-Kopien werden Volumes in Ihren Arbeitsumgebungen nicht geschützt.
- Volumes in Ihren Arbeitsumgebungen sind durch das Erstellen von Backups in der Cloud mit nicht geschützt ["Cloud-Backup"](#).
- Volumes in Ihren Arbeitsumgebungen sind mittels ONTAP SnapLock Technologie vor Modifizierung und Löschung auf DEM WORM Storage geschützt. ["Weitere Informationen zu SnapLock"](#).
- Daten in den Arbeitsumgebungen und Datenquellen werden nicht mit gescannt ["Cloud-Daten Sinnvoll"](#) Erkennen von Compliance- und Datenschutzbedenken und ermitteln von Optimierungschancen.

Diese Funktion ist auch im Hinblick auf die Sicherung mit Ransomware wichtig, da sie Ihnen ein besseres Verständnis darüber ermöglicht, wo sich Ihre wichtigen (sensiblen, geschäftskritischen) Daten befinden, damit Sie sich ganz auf den Schutz konzentrieren können.

- Falls eine Wiederherstellung aufgrund eines Ransomware-Angriffs erforderlich ist, werden die wichtigsten Datenkategorien nicht gesichert.
- Eine anormale Zunahme des Prozentsatzes der verschlüsselten Dateien in einer Arbeitsumgebung oder Datenquelle ist aufgetreten.

Dies kann ein Indikator dafür sein, dass ein Ransomware-Angriff in Ihrem Netzwerk begonnen hat.

- Sensible Daten befinden sich in Dateien in einer Arbeitsumgebung oder in einer Datenquelle, und die Zugriffsberechtigungen sind zu hoch.
- Benutzer wurden zu den Active Directory-Domänenadministratorgruppen hinzugefügt.
- Die ONTAP Softwareversion auf Ihren Clustern ist veraltet und sollte aktualisiert werden, um die besten Schutz- und Sicherheitsfunktionen sowie die neuesten Funktionen bereitzustellen.
- Das Auditing von NAS-Dateisystemen ist auf ONTAP-Systemen nicht aktiviert.

Durch das Aktivieren der CIFS-Prüfung werden Überwachungsereignisse für Ihre Systemadministratoren

generiert, die Informationen wie Änderungen der Ordnerrechte, fehlgeschlagene Lese- oder Schreibversuche sowie das Erstellen, Ändern oder Löschen von Dateien nachverfolgen.

- Integrierte Anti-Ransomware-Funktionen sind auf Ihren ONTAP-Systemen nicht aktiviert.

Die Anti-Ransomware-Funktionen von ONTAP erkennen proaktiv anormale Aktivitäten, die auf einen Ransomware-Angriff hindeuten könnten, und warnen vor diesen.

- Wenn ONTAP Anti-Ransomware auf Ihren Systemen aktiviert ist, werden die verschiedenen Ransomware-Vorfälle als Warnmeldungen angezeigt.
- Die Anzahl der hohen, mittleren und niedrigen Sicherheitslücken, die das Active IQ Digital Advisor-Tool auf Ihren ONTAP-Clustern gefunden hat.

Sie können die Sicherheitsanfälligkeit anzeigen und anschließend die empfohlene Aktion befolgen, um das Problem zu beheben.

["Sehen Sie sich an, wie Sie diese potenziellen Probleme im Dashboard zum Schutz vor Ransomware sehen können."](#)

Beim Einsatz von Cloud Volumes ONTAP Systemen gibt es zusätzliche Ransomware-Schutzmaßnahmen, die sich direkt in der Arbeitsumgebung implementieren lassen. ["Zusätzlicher Schutz vor Ransomware – so geht's"](#).

Unterstützte Arbeitsumgebungen und Datenquellen

["Cloud-Daten Sinnvoll"](#) Ist eine Voraussetzung für die Nutzung des Ransomware Protection Service. Nachdem Data Sense installiert und aktiviert ist, können Sie Ransomware Protection verwenden, um zu sehen, wie belastbar Ihre Daten ist, um Cyber-Angriff auf die folgenden Arten von Arbeitsumgebungen und Datenquellen:

- Arbeitsumgebungen:*
- Cloud Volumes ONTAP (implementiert in AWS, Azure oder GCP)
- On-Premises ONTAP Cluster
- Azure NetApp Dateien
- Amazon FSX für ONTAP
- Amazon S3

Datenquellen:

- File Shares von anderen Anbietern
- Objekt-Storage (nutzt S3-Protokoll)
- Datenbanken (Amazon RDS, MongoDB, MySQL, Oracle, PostgreSQL, SAP HANA, SQL SERVER)
- OneDrive Accounts
- SharePoint Online- und On-Premises-Accounts
- Google Drive-Konten

Ransomware Protection überwacht auch Ihre globale Active Directory-Konfiguration, wenn Sie haben ["Konfiguriert in Cloud Data Sense"](#).

Funktionsweise von Ransomware-Schutz

Auf hoher Ebene funktioniert Ransomware Protection wie folgt:


1. Ransomware Protection sammelt Informationen von Ihren Storage-Systemen, Cloud Data Sense, Cloud Backup und von anderen BlueXP und NetApp Ressourcen, um das Ransomware Protection Dashboard auszufüllen.
2. Sie verwenden das Ransomware-Schutz-Dashboard, um einen Überblick zu bekommen, wie gut Ihre Systeme geschützt sind.
3. Mithilfe der bereitgestellten Berichterstellungs-Tools können Sie den Schutz von Cyberspeichern unterstützen.

Kosten

Es gibt keine separaten Kosten für den Ransomware-Schutz-Service während der Beta.

Monitoring des Status von Ransomware-Warnmeldungen

Sie können den Status von Ransomware-Warnungen im BlueXP Notification Center anzeigen. Sie können außerdem Benachrichtigungen per E-Mail konfigurieren, damit Sie auch dann über wichtige Systemaktivitäten informiert werden können, wenn Sie nicht beim System angemeldet sind.

Das Notification Center verfolgt den Fortschritt von Ransomware-Zwischenfällen und kann so überprüfen, ob sie gelöst wurden oder nicht. Sie können die Benachrichtigungen anzeigen, indem Sie auf die Schaltfläche () klicken. In der BlueXP-Menüleiste. Sie können BlueXP auch so konfigurieren, dass Benachrichtigungen per E-Mail als Warnmeldungen gesendet werden.

Derzeit gibt es ein Ereignis, das E-Mail-Benachrichtigungen auslöst:

- Potenzielle Ransomware-Angriffe auf Ihrem System erkannt

Standardmäßig erhalten BlueXP-Kontoadministratoren E-Mails für alle „kritischen“ und „Empfehlungsmeldungen“. Alle anderen Benutzer und Empfänger sind standardmäßig so konfiguriert, dass sie keine Benachrichtigungs-E-Mails erhalten. E-Mails können an alle BlueXP Benutzer, die Teil Ihres NetApp Cloud-Kontos sind, oder an alle anderen Empfänger gesendet werden, die auf Sicherheitsvorfälle bei Ransomware achten müssen.

Sie müssen die Benachrichtigungstyp "kritisch" auswählen, um die Ransomware Protection E-Mail-Benachrichtigungen zu erhalten.

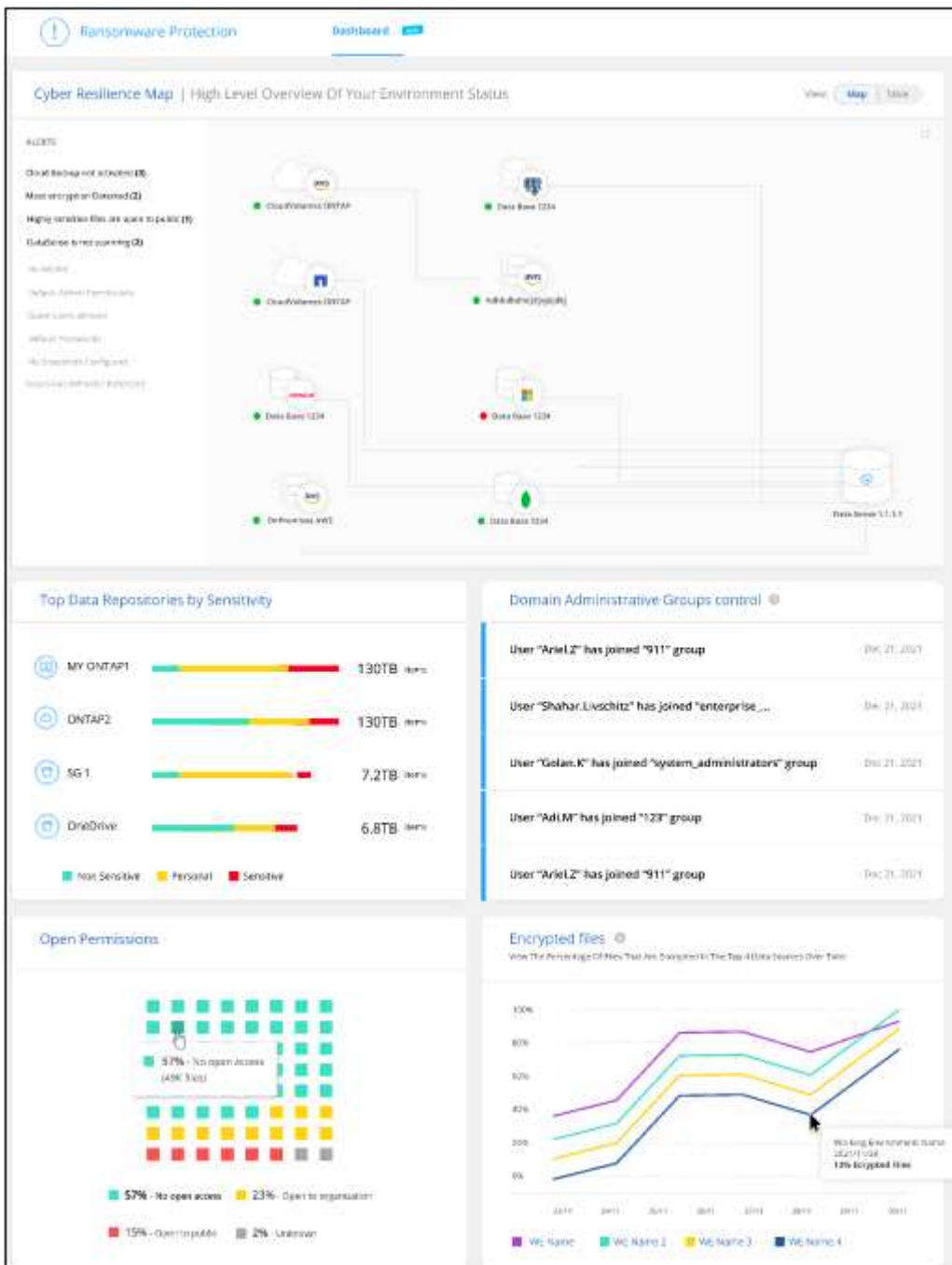
["Erfahren Sie mehr über das Benachrichtigungscenter"](#) Und wie Sie Alarmierung bei Ransomware-Sicherungsvorfällen per E-Mail versenden.

Verwenden Sie Ransomware-Schutz

Verwalten von Cyber-Sicherheitsempfehlungen für Ihre Datenquellen

Nutzen Sie das Ransomware Protection Dashboard, um einen Überblick über die Cyber-Ausfallsicherheit aller Ihrer BlueXP (früher Cloud Manager) Arbeitsumgebungen und zusätzlichen Datenquellen zu erhalten. Sie können in jedem Bereich nach unten gehen, um weitere Details und mögliche Korrekturmaßnahmen zu finden.

Wählen Sie im Menü BlueXP links die Option **Schutz > Ransomware-Schutz**.



Ransomware-Schutzpunktzahl und empfohlene Maßnahmen

Das Bedienfeld „Ransomware Protection Score“ bietet eine einfache Möglichkeit, zu erkennen, wie stabil Ihre Daten bei einem Ransomware-Angriff ist. Es ist eine Zusammenfassung aller Maßnahmen, die empfohlen werden, um Ihre Datensicherheit und Cyber-Ausfallsicherheit zu verbessern. Dieses Panel funktioniert in Verbindung mit dem Fenster Empfohlene Maßnahmen. Es gibt zwei Teile der Ransomware Protection Score Panel:

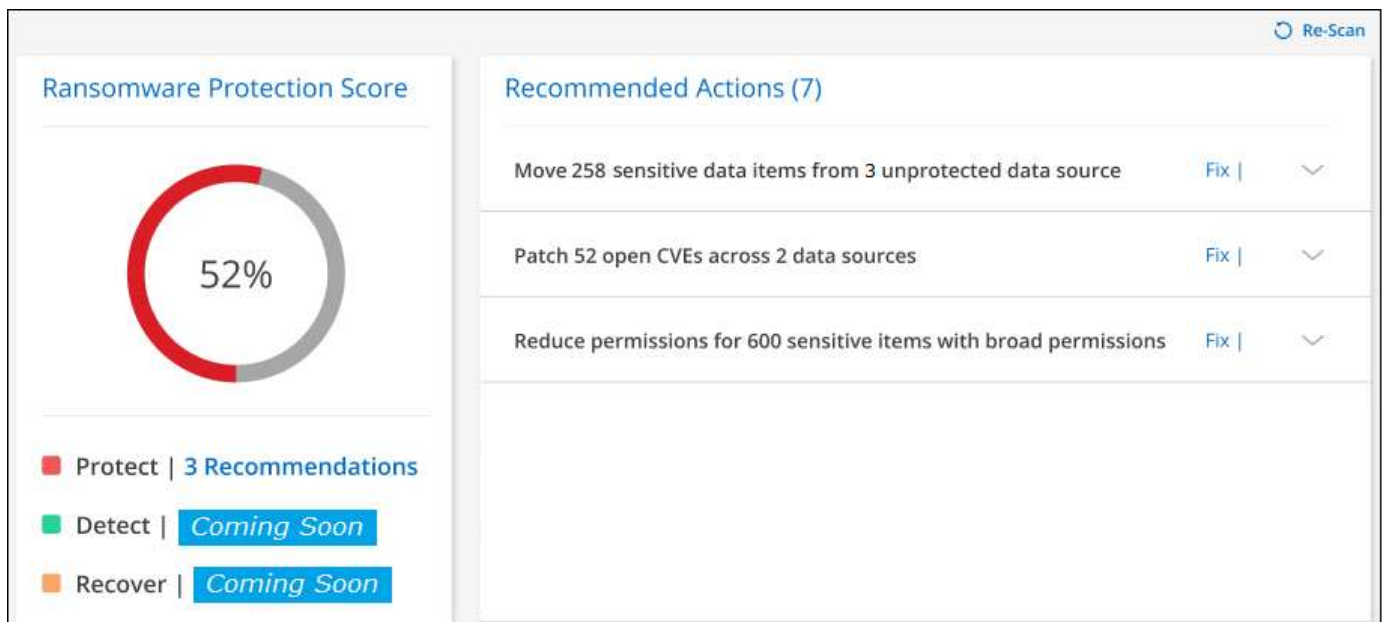
- Der Gesamtbewertung für Ihre Daten (0 – 100 % geschützt)

Die Bewertung basiert auf einer gewichteten Berechnung aller möglichen Empfehlungen.

- Wie viele empfohlene Maßnahmen sind verfügbar, um Ihren Schutz auf 100 % zu steigern, wenn Sie die Empfehlungen implementieren.

Die drei Arten der empfohlenen Maßnahmen entsprechen dem ["NIST-Framework für Cyber-Sicherheit"](#):

- Sichern
- Erkennen
- Recovery



Auf dieser Beispielseite gibt es sieben empfohlene Aktionen für die Kategorie „Schutz“. Die erste Empfehlung gilt für 258 Dateien.

Dieses Panel unterstützt Arbeitsumgebungen und Datenquellen, die dem Cloud Data Sense hinzugefügt wurden.

Beachten Sie, dass die Empfehlungen pro Datenquelle gelten. Wenn also dieselbe Empfehlung für 3 Datenquellen relevant ist, wird sie als 3 Empfehlungen gezählt.

Sie können auf klicken ▾ So erweitern Sie jede empfohlene Aktion wie unten gezeigt.

Recommended Actions (3)		
Move 258 sensitive data items from 3 unprotected data sources		
System Name	Items	
ONTAP123	200	Investigate
SystemAB	32	Investigate
SystemCD	26	Investigate

Um die detaillierte Liste der Daten zu sehen, die mit einer empfohlenen Aktion identifiziert wurden, klicken Sie auf die Schaltfläche **untersuchen** und Sie werden auf die Cloud Data Sense Untersuchungsseite mit der Liste aller Dateien weitergeleitet, die die Kriterien für die empfohlene Aktion erfüllen.

Dann können Sie entscheiden, ob Sie die empfohlene Aktion auf alle diese Dateien anwenden möchten, oder nur auf einigen von ihnen.

Nachdem Sie die empfohlene Aktion behoben haben, wird die nächste Aktualisierung der Ransomware Protection Score Panel (alle 5 Minuten) die Zahl für die Punktzahl anpassen. Sie können auch auf die Schaltfläche **Re-Scan** klicken, um die Seite jetzt zu aktualisieren.

Liste empfohlener Maßnahmen

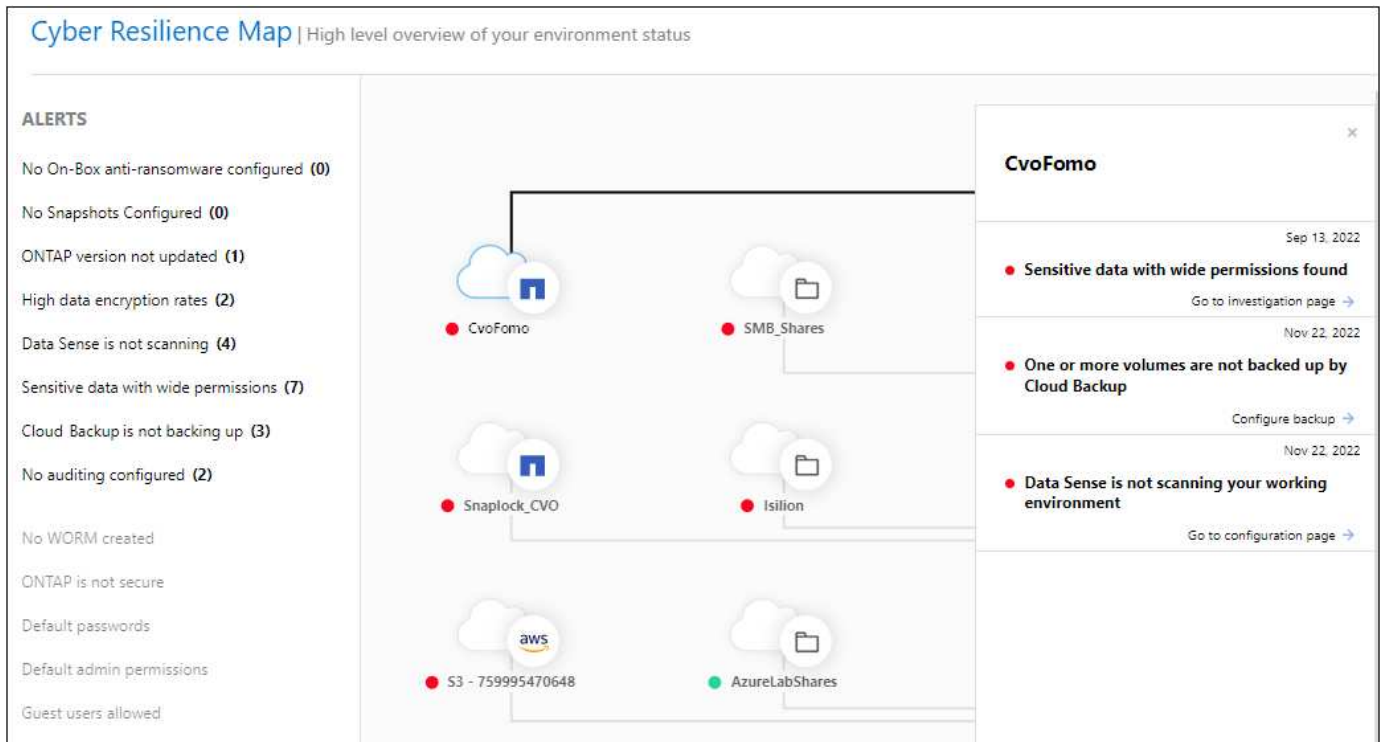
Hier handelt es sich um die derzeit aufgezeichneten Maßnahmen und Lösungsvorschläge.

Empfohlene Maßnahmen	Beschreibung	Mögliche Lösung
Reduzieren Sie die Berechtigungen für X-sensible Elemente mit breiten Berechtigungen	In Ihren Datenquellen von Cloud Data Sense finden Sie sensible Dateien mit offenen Berechtigungen. Dazu zählen alle sensiblen Daten (personenbezogene Daten und sensible personenbezogene Daten), die „offen für Unternehmen“ oder „öffentlich zugänglich“ sind.	Klicken Sie für jede Datenquelle auf die Schaltfläche untersuchen und Sie werden zur Seite Data Sense Investigation weitergeleitet, auf der Sie alle gefährdeten sensiblen Dateien anzeigen und weitere Maßnahmen ergreifen können, um dieses Risiko zu reduzieren. Dazu gehört auch, wie die breiten Berechtigungen auf diesen Dateien reduziert werden können.

Empfohlene Maßnahmen	Beschreibung	Mögliche Lösung
Verschieben Sie X-sensible Elemente von nicht geschützten Y-Datenquellen in sichere Speicherorte	Sensible Daten sind durch Cloud Data Sense in ungeschützten Datenquellen vorhanden. An diesen Orten kann die Ransomware-Datensicherungssoftware nicht schützen. In der Regel verfügen IT-Abteilungen über Richtlinien, die sensible Daten von bestimmten Unternehmensstandorten einschränken. Diese empfohlene Aktion ermöglicht es Ihnen, die Dateien mit sensiblen Daten zu identifizieren und sie in eine sicherere Datenquelle zu verschieben, wo sensible *gespeichert werden darf.	Mit Data Sense können Sie diese Dateien schnell in eine besser geschützte Datenquelle verschieben. Sie werden die Funktion „Data Sense“ nutzen "Quelldateien in eine NFS-Freigabe verschieben" .
Patch X Open CVEs über Y-Datenquellen hinweg	Nicht patched CVEs (allgemeine Schwachstellen und Exposé) wurden auf den On-Premises-ONTAP-Systemen und/oder Cloud Volumes ONTAP-Systemen gefunden. Diese Probleme werden nur erkannt, wenn das Produkt Digital Advisor (ehemals Active IQ Digital Advisor) in Ihre Speichersysteme integriert ist. Hierbei handelt es sich um bekannte Schwachstellen in NetApp Storage-Systemen, deren Behebung des CVE-Problems ermittelt wurde. NetApp CVEs sind im aufgeführt "Produktsicherheitsseite" .	Klicken Sie für jede Datenquelle auf die Schaltfläche Digital Advisor , und Sie werden im Digital Advisor zur Seite <i>Security Vulnerabilities</i> weitergeleitet. Dort werden die Details zu den geöffneten CVEs sowie die empfohlene Aktion zum Beheben der einzelnen CVE angezeigt. Häufig wird die Lösung auch auf ein Upgrade der ONTAP Software auf dem System ausgeführt. "Erfahren Sie mehr über die Seite Sicherheitslücke" .

Cyber Resilience Map

Die Cyber Resilience Map ist der Hauptbereich im Dashboard. Es ermöglicht Ihnen, alle Ihre Arbeitsumgebungen und Datenquellen visuell zu sehen und relevante Informationen zur Cyber-Ausfallsicherheit anzuzeigen.



Die Karte besteht aus drei Teilen:

Linker Bereich

Zeigt eine Liste der Warnungen an, für die der Service alle Datenquellen überwacht. Es gibt außerdem die Anzahl jeder bestimmten Warnung an, die in Ihrer Umgebung aktiv ist. Eine große Anzahl von Warnungen kann ein guter Grund sein, um zu versuchen, diese Warnmeldungen zuerst zu lösen.

Mittelplatte

Zeigt alle Datenquellen, Dienste und Active Directory in einem grafischen Format an. Gesunde Umgebungen weisen einen grünen Indikator auf, und Umgebungen mit einem Warnmeldungsanzeiger haben einen roten Indikator.

Rechte Abdeckung

Nachdem Sie auf eine Datenquelle geklickt haben, die eine rote Anzeige aufweist, zeigt dieses Fenster die Warnungen für diese Datenquelle an und gibt Empfehlungen zur Behebung der Warnmeldung aus. Die Alarme werden so sortiert, dass die letzten Warnmeldungen zuerst aufgeführt werden. Viele Empfehlungen führen Sie zu einem anderen BlueXP-Service, wo Sie das Problem lösen können.

Es handelt sich dabei um die derzeit nachverfolgten Warnungen und vorgeschlagenen Korrekturmaßnahmen.

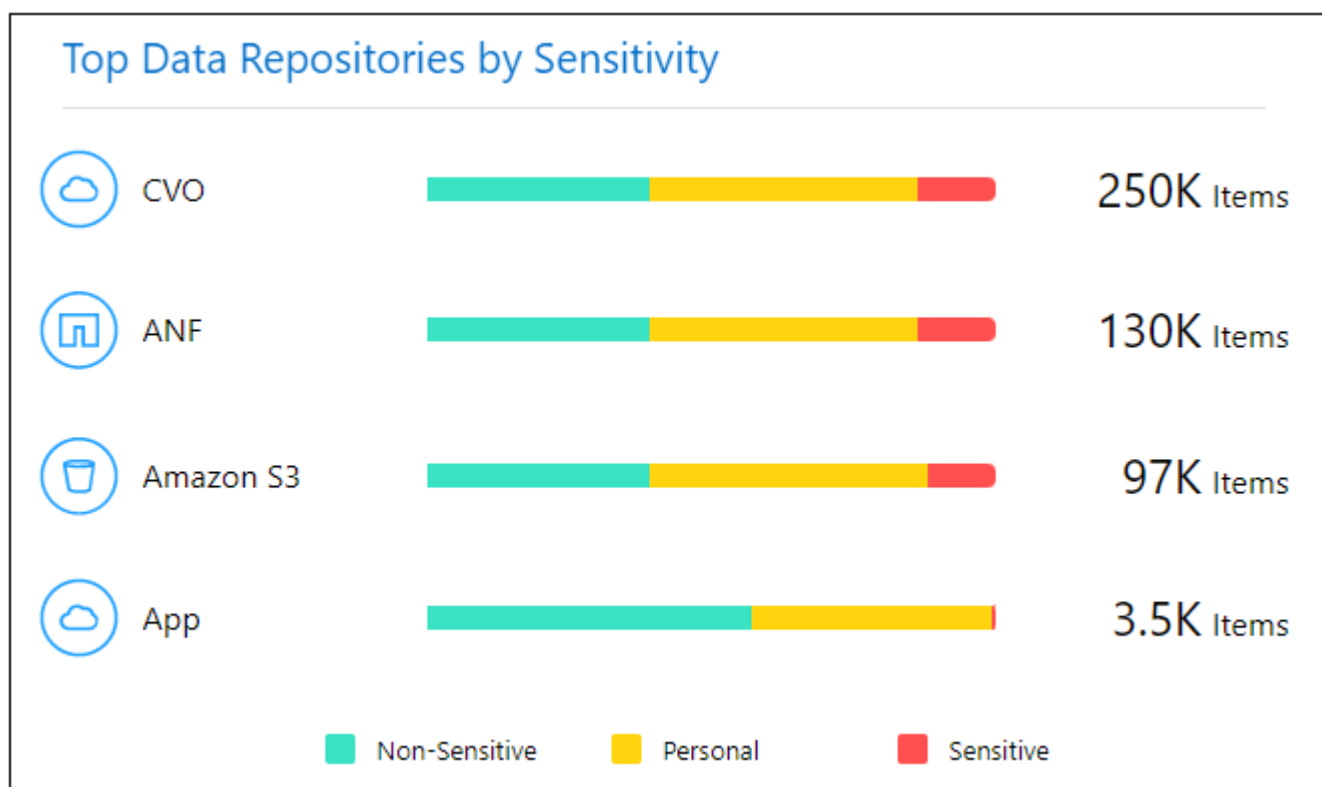
Alarm	Beschreibung	Korrekturmaßnahmen
Hohe Datenverschlüsselungsraten gefunden	Eine anormale Zunahme des Prozentsatzes der verschlüsselten Dateien oder beschädigten Dateien in der Datenquelle ist aufgetreten. Das bedeutet, dass der Prozentsatz der verschlüsselten Dateien in den letzten 7 Tagen um mehr als 20 % erhöht wurde. Wenn zum Beispiel 50 % der Dateien verschlüsselt sind, dann erhöht sich diese Zahl einen Tag später auf 60 %, Sie würden diese Warnung sehen.	Klicken Sie auf den Link, um das zu starten " Untersuchungsseite „Data Sense“ ". Dort können Sie die Filter für die spezifische <i>Arbeitsumgebung</i> und <i>Kategorie (verschlüsselt und beschädigt)</i> auswählen, um die Liste aller verschlüsselten und beschädigten Dateien anzuzeigen.
Sensible Daten mit breiten Berechtigungen gefunden	Sensible Daten werden in Dateien gefunden und die Zugriffsberechtigungen sind in einer Datenquelle zu hoch.	Klicken Sie auf den Link, um das zu starten " Untersuchungsseite „Data Sense“ ". Dort können Sie die Filter für die spezifische <i>Arbeitsumgebung</i> , <i>Sensitivity Level (Sensitive Personal)</i> und <i>Open Permissions</i> auswählen, um die Liste der Dateien anzuzeigen, die dieses Problem haben.
Ein oder mehrere Volumes werden mit Cloud Backup nicht gesichert	Einige Volumes in der Arbeitsumgebung werden nicht mit geschützt " Cloud-Backup ".	Klicken Sie auf den Link, um Cloud Backup zu starten. Dann können Sie die Volumes identifizieren, die nicht in der Arbeitsumgebung gesichert werden, und entscheiden, ob Sie Backups auf diesen Volumes aktivieren möchten.
Ein oder mehrere Repositorys (Volumes, Buckets usw.) in Ihren Datenquellen werden nicht nach Data Sense gescannt	Einige Daten in Ihren Datenquellen werden nicht mit gescannt " Cloud-Daten Sinnvoll " Um Compliance- und Datenschutzbedenken zu identifizieren und Optimierungsmöglichkeiten zu finden.	Klicken Sie auf den Link, um den Datensense zu starten und das Scannen und die Zuordnung für die nicht gescannten Elemente zu aktivieren.
On-box Anti-Ransomware ist nicht für alle Volumes aktiv	Einige Volumes im lokalen ONTAP-System haben die nicht " NetApp Funktion zur Bekämpfung von Ransomware " Aktiviert.	Klicken Sie auf den Link, und Sie werden zu weitergeleitet Härten Sie Ihre ONTAP Umgebung Panel Und in die Arbeitsumgebung mit dem Problem. Dort können Sie herausfinden, wie das Problem am besten behoben werden kann.
Die ONTAP-Version wurde nicht aktualisiert	Die auf Ihren Clustern installierte Version der ONTAP Software entspricht nicht den Empfehlungen von " NetApp Leitfaden zur verstärkte Sicherheit von ONTAP-Systemen ".	Klicken Sie auf den Link, und Sie werden zu weitergeleitet Härten Sie Ihre ONTAP Umgebung Panel Und in die Arbeitsumgebung mit dem Problem. Dort können Sie herausfinden, wie das Problem am besten behoben werden kann.

Alarm	Beschreibung	Korrekturmaßnahmen
Snapshots sind nicht für alle Volumes konfiguriert	Einige Volumes in der Arbeitsumgebung sind nicht durch die Erstellung von Volume Snapshots geschützt.	Klicken Sie auf den Link, und Sie werden zu weitergeleitet Härten Sie Ihre ONTAP Umgebung Panel Und in die Arbeitsumgebung mit dem Problem. Dort können Sie herausfinden, wie das Problem am besten behoben werden kann.
Das Auditing von Dateivorgängen ist nicht für alle SVMs aktiviert	Einige Storage-VMs in der Arbeitsumgebung sind nicht für das Filesystem-Auditing aktiviert. Es wird empfohlen, damit Sie die Benutzeraktionen auf Ihren Dateien verfolgen können.	Klicken Sie auf den Link, und Sie werden zu weitergeleitet Härten Sie Ihre ONTAP Umgebung Panel Und in die Arbeitsumgebung mit dem Problem. Dort können Sie herausfinden, ob Sie NAS-Prüfungen auf Ihren SVMs aktivieren müssen.

Wichtige Daten-Repositorys durch Sensibilität

Das Fenster *Top Data Repositories by Sensitivity Level* enthält bis zu den vier wichtigsten Daten-Repositorys (Arbeitsumgebungen und Datenquellen), die die sensibelsten Elemente enthalten. Das Balkendiagramm für jede Arbeitsumgebung ist in folgende Kategorien unterteilt:

- Nicht-sensible Daten
- Persönliche Daten
- Sensible personenbezogene Daten



Sie können mit der Maus auf jeden Abschnitt zeigen, um die Gesamtanzahl der Elemente in jeder Kategorie

anzuzeigen.

Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Seite „Data Sense Investigation“ anzuzeigen, damit Sie weitere Informationen finden können.

Domänenadministrator-Gruppenkontrolle

Das Fenster *Domain Administrator Group Control* zeigt die letzten Benutzer an, die zu Ihren Domänenadministratorgruppen hinzugefügt wurden, damit Sie sehen können, ob alle Benutzer in diesen Gruppen zugelassen werden sollen. Dieser muss unbedingt vorhanden sein ["Integration eines globalen Active Directory"](#) In Cloud Data Sense für dieses Panel aktiv sein.

Domain Administrative Groups control ⓘ	
User "marq markez" was added to "Administrators"	Jun 09, 2022
User "valentino rossi" was added to "Administrators"	Jun 07, 2022
User "Hatzil shum" was added to "Administrators"	Mar 15, 2022
Group "HR Application Users" was added to "Enterprise Admins"	Feb 16, 2022

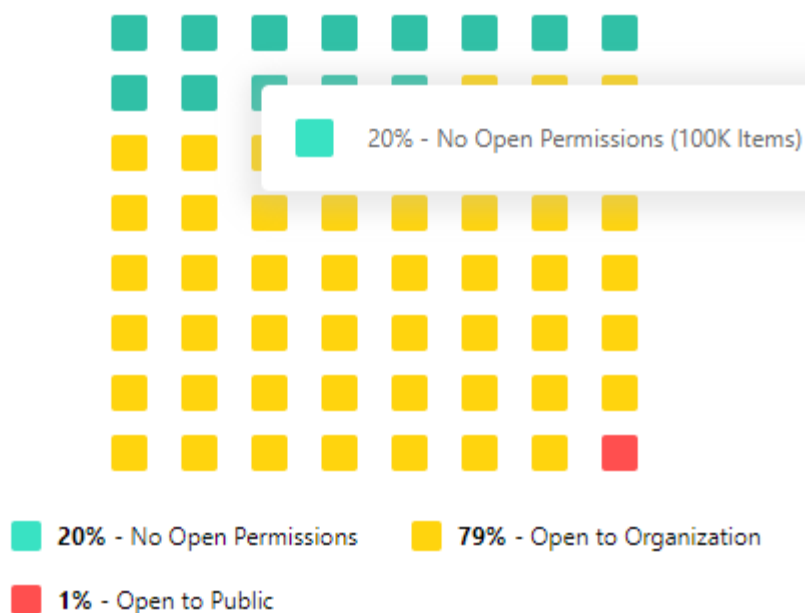
Zu den Standard-Administratorgruppen gehören „Administratoren“, „Domänen-Administratoren“, „Enterprise Admins“, „Enterprise Key Admins“ und „Key Admins“.

Daten, die nach Typen offener Berechtigungen aufgelistet sind

Im Fenster „_Öffnen“ wird der Prozentsatz für jeden Berechtigungstyp angezeigt, der für alle Dateien vorhanden ist, die gescannt werden. Das Diagramm wird aus Data Sense bereitgestellt und zeigt die folgenden Berechtigungstypen an:

- Kein Offener Zugriff
- Steht Unternehmen offen
- Öffentlich zugänglich
- Unbekannter Zugriff

Open Permissions



Sie können mit der Maus auf jeden Abschnitt zeigen, um den Prozentsatz und die Gesamtzahl der Dateien in jeder Kategorie anzuzeigen.

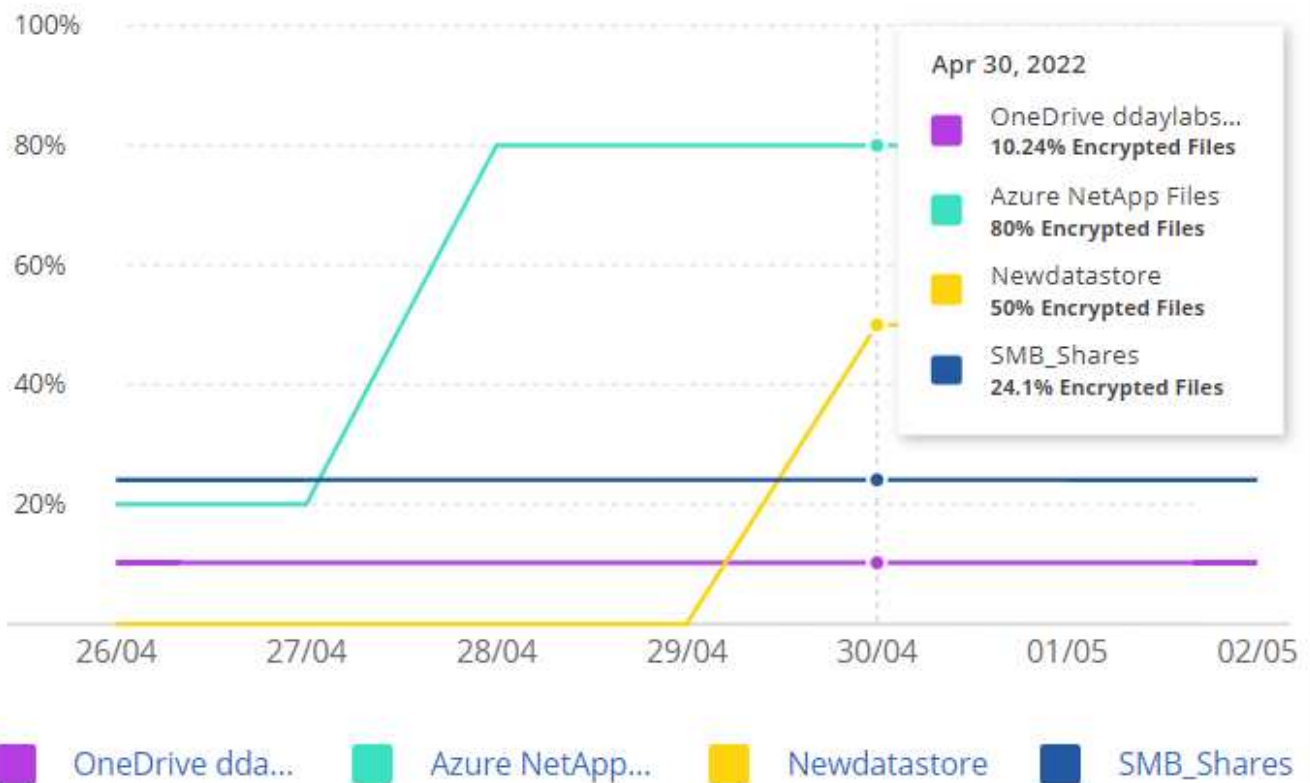
Klicken Sie auf die einzelnen Bereiche, um die gefilterten Ergebnisse auf der Seite „Data Sense Investigation“ anzuzeigen, damit Sie weitere Informationen finden können.

Daten, die in verschlüsselten Dateien aufgeführt sind

Das Fenster *verschlüsselte Dateien* zeigt die 4 wichtigsten Datenquellen mit dem höchsten Prozentsatz an Dateien an, die im Laufe der Zeit verschlüsselt sind. Dies sind in der Regel Elemente, die kennwortgeschützt waren. Dazu werden die Verschlüsselungsraten der letzten 7 Tage verglichen, um zu sehen, welche Datenquellen eine Zunahme von über 20 % haben. Eine Zunahme dieser Menge könnte bedeuten, dass Ransomware bereits Ihr System angegriffen wird.

Encrypted Files ⓘ

Rising percentages of encrypted files can be an indication of malicious activity



Klicken Sie auf eine Zeile für eine der Datenquellen, um die gefilterten Ergebnisse auf der Seite „Data Sense Investigation“ anzuzeigen, damit Sie weitere Untersuchungen durchführen können.




































Status der Erhöhung des Status der ONTAP Systemhärtung

Das Fenster *Harden Your ONTAP Environment* enthält den Status bestimmter Einstellungen in Ihren ONTAP-Systemen, die verfolgen, wie sicher Ihre Bereitstellung gemäß dem ist "[NetApp Leitfaden zur verstärkte Sicherheit von ONTAP-Systemen](#)" Und zum "[ONTAP Anti-Ransomware-Funktion](#)" Die ungewöhnliche Aktivitäten proaktiv erkennen und warnen.

Sie können die Empfehlungen prüfen und anschließend entscheiden, wie Sie potenzielle Probleme beheben möchten. Sie können die Schritte befolgen, um die Einstellungen auf Ihren Clustern zu ändern, die Änderungen auf ein anderes Mal zu verschieben oder den Vorschlag zu ignorieren.

Dieses Panel unterstützt derzeit On-Prem ONTAP, Cloud Volumes ONTAP und Amazon FSX für NetApp ONTAP Systeme.

Harden your ONTAP environments

Working Environment	ONTAP Anti Ransomware ⓘ	NAS Auditing ⓘ	ONTAP Version ⓘ	Snapshots ⓘ	
MY ONTAP1			 9.10.XX		  
ONTAP2			 9.10.XX		  
AccOI_ONTAP			 9.10.XX		  
CVO828			 9.8.XX		  
FSx			 9.8.XX		  

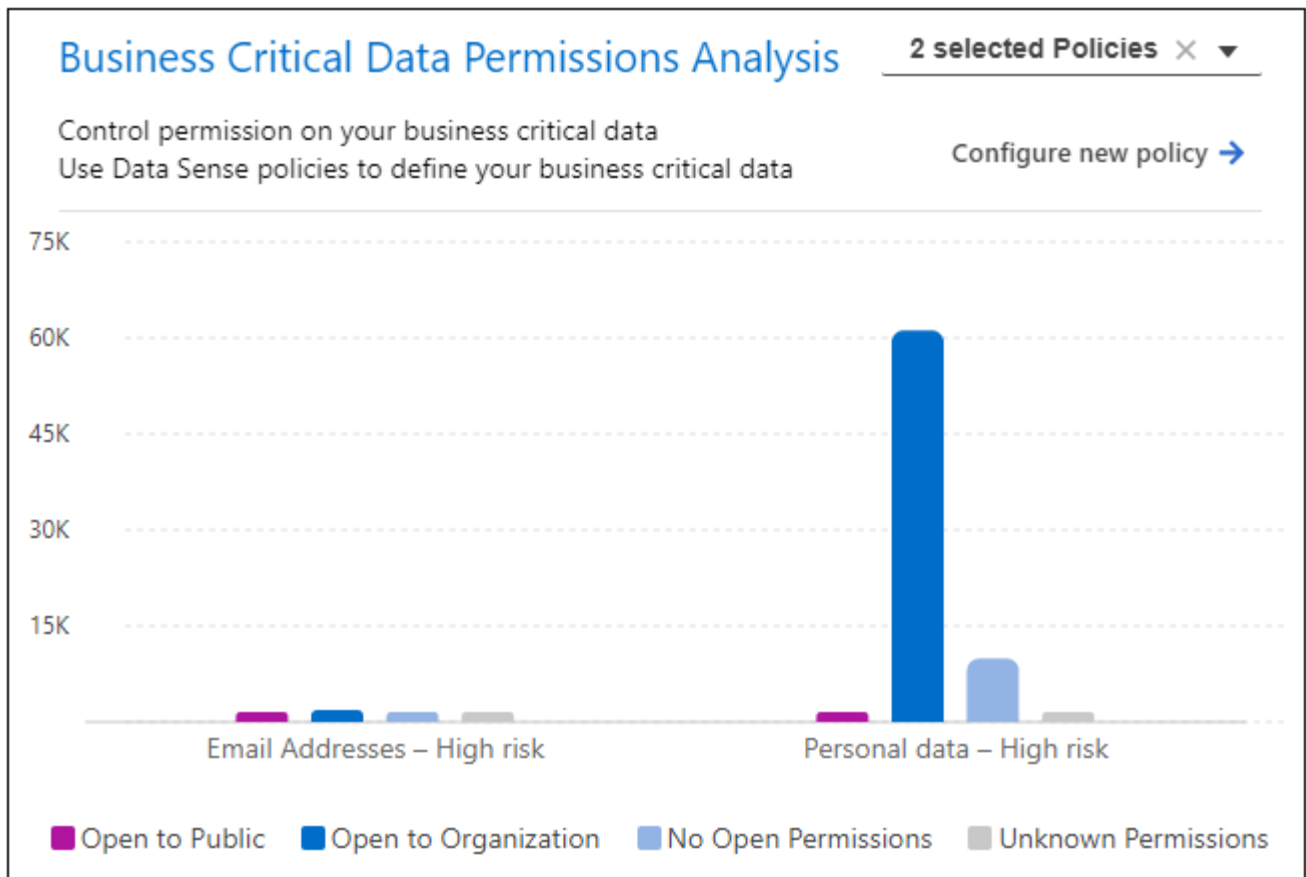
Folgende Einstellungen werden verfolgt:

Härtungsziel	Beschreibung	Korrekturmaßnahmen
ONTAP Anti-Ransomware	Der Prozentsatz der Volumes, für die integrierte Ransomware aktiviert ist. Nur für ONTAP-Systeme vor Ort gültig. Ein grünes Statussymbol zeigt an, dass > 85 % der Volumes aktiviert sind. Gelb gibt an, dass 40-85% aktiviert sind. Rot zeigt an, dass < 40 % aktiviert sind.	"Anti-Ransomware auf Ihren Volumes aktivieren" Verwenden von System Manager.
NAS-Auditing	Die Anzahl der Storage VMs, für die Dateisystemprüfungen aktiviert sind. Ein grünes Statussymbol zeigt an, dass bei > 85 % der SVMs die Prüfung des NAS-Filesystems aktiviert ist. Gelb gibt an, dass 40-85% aktiviert sind. Rot zeigt an, dass < 40 % aktiviert sind.	"Erfahren Sie, wie NAS-Audits auf SVMs möglich werden" Verwenden der CLI.

Härtungsziel	Beschreibung	Korrekturmaßnahmen
ONTAP-Version	Die auf den Clustern installierte Version der ONTAP Software. Ein grünes Statussymbol zeigt an, dass die Version aktuell ist. Ein gelbes Symbol zeigt an, dass der Cluster hinter 1 oder 2 Patch-Versionen oder 1 Minor-Version für On-Prem-Systeme oder hinter 1 Hauptversion für Cloud Volumes ONTAP steht. Ein rotes Symbol zeigt an, dass der Cluster hinter 3 Patch-Versionen steht, 2 Minor-Versionen, 1 Hauptversion für On-Prem-Systeme oder hinter 2 Hauptversionen für Cloud Volumes ONTAP.	"Für ein Upgrade von On-Premises-Clustern empfiehlt sich die beste Lösung" Oder "Ihre Cloud Volumes ONTAP Systeme".
Snapshots	Ist die Snapshot-Funktion für Daten-Volumes aktiviert und welcher Prozentsatz der Volumes Snapshot Kopien aufweisen. Ein grünes Statussymbol zeigt an, dass > 85 % der Volumes Snapshots aktiviert sind. Gelb gibt an, dass 40-85% aktiviert sind. Rot zeigt an, dass < 40 % aktiviert sind.	"Aktivieren Sie Volume-Snapshots in Ihren On-Premises-Clustern", Oder "Auf Ihren Cloud Volumes ONTAP Systemen", Oder "Auf Ihren FSX für ONTAP Systemen".

Status von Berechtigungen für Ihre kritischen Geschäftsdaten

Das Fenster *Analyse der Berechtigungen für geschäftskritische Daten* zeigt den Berechtigungsstatus von Daten an, die für Ihr Unternehmen von entscheidender Bedeutung sind. Damit können Sie schnell einschätzen, wie gut Sie Ihre geschäftskritischen Daten schützen.



In diesem Bereich werden zunächst Daten basierend auf den von uns ausgewählten Standardrichtlinien angezeigt. Sie können jedoch die 2 wichtigsten Daten Sense *Policies* auswählen, die Sie erstellt haben, um Ihre wichtigsten Geschäftsdaten anzuzeigen. Informieren Sie sich darüber "[Erstellen Sie Ihre Richtlinien mit Data Sense](#)".

Das Diagramm zeigt eine Berechtigungsanalyse aller Daten, die den Kriterien Ihrer Richtlinien entsprechen. Hier werden die Anzahl der Elemente aufgeführt, die:

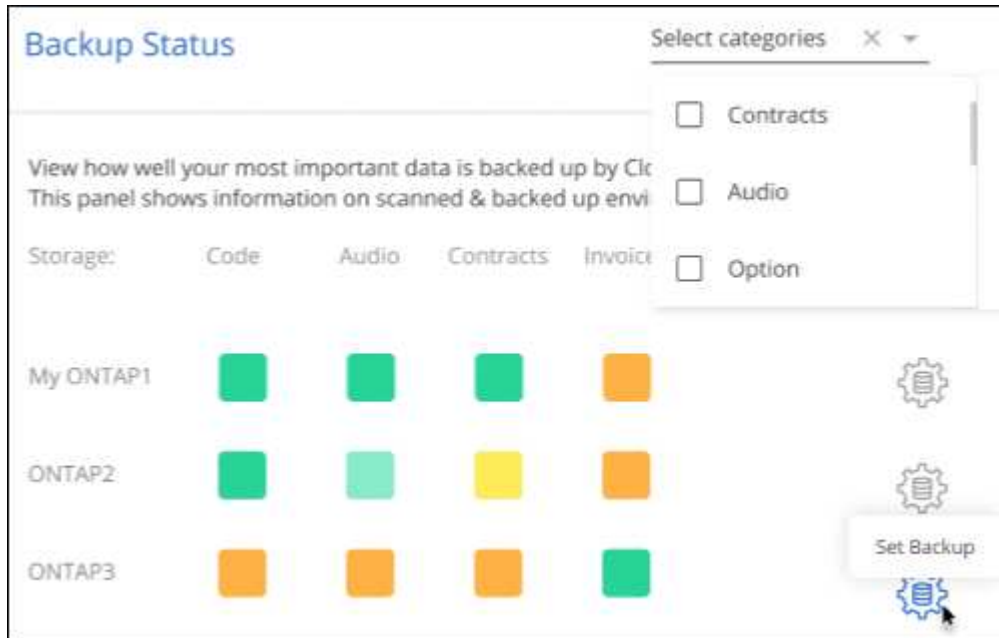
- Offen für öffentliche Berechtigungen - die Elemente, die Data Sense als offen für die Öffentlichkeit betrachtet
- Offen für Unternehmensberechtigungen – die Elemente, die von Data Sense als für Unternehmen offen erachtet werden
- Keine offenen Berechtigungen - die Elemente, die Data Sense als keine offenen Berechtigungen betrachtet
- Unbekannte Berechtigungen - die Elemente, die Data Sense als unbekannte Berechtigungen betrachtet

Bewegen Sie den Mauszeiger über die einzelnen Balken in den Diagrammen, um die Anzahl der Ergebnisse in jeder Kategorie anzuzeigen. Klicken Sie auf eine Leiste, und die Seite Data Sense Investigation wird angezeigt. So können Sie weitere Informationen darüber finden, welche Elemente über offene Berechtigungen verfügen und ob Sie Anpassungen an Dateiberechtigungen vornehmen sollten.

Backup-Status Ihrer geschäftskritischen Daten

Das Fenster *Backup Status* zeigt an, wie verschiedene Datenkategorien durch Cloud Backup geschützt werden. So finden Sie heraus, wie umfassend Ihre wichtigsten Daten-Kategorien gesichert werden, falls Sie eine Recovery aufgrund eines Ransomware-Angriffs durchführen müssen. Diese Daten stellen eine visuelle Darstellung dar, wie viele Elemente einer bestimmten Kategorie in einer Arbeitsumgebung gesichert werden.

In diesem Bereich wird nur On-Premises-ONTAP- und Cloud Volumes ONTAP-Arbeitsumgebungen angezeigt, die bereits über Cloud Backup *und* gescannt wurden, die über Cloud Data Sense verwendet werden.



Zunächst zeigt dieses Panel Daten basierend auf Standardkategorien, die wir ausgewählt haben. Sie können aber auch die Kategorien von Daten auswählen, die Sie nachverfolgen möchten; z. B. Codes von Dateien, Verträgen usw. Siehe die vollständige Liste von "[Kategorien](#)". Die sind von Cloud Data Sense für Ihre Arbeitsumgebungen verfügbar. Wählen Sie dann bis zu 4 Kategorien aus.

Wenn die Daten ausgefüllt sind, bewegen Sie den Mauszeiger über jedes Quadrat in den Diagrammen, um die Anzahl der Dateien anzuzeigen, die aus allen Dateien in derselben Kategorie in der Arbeitsumgebung gesichert werden. Ein grünes Quadrat bedeutet, dass 85 % oder mehr Ihrer Dateien gesichert werden. Ein gelbes Quadrat bedeutet, dass 40% bis 85% der Dateien gesichert werden. Und ein rotes Rechteck bedeutet, dass 40 % oder weniger Dateien gesichert werden.

Sie können am Ende der Zeile auf die Schaltfläche **Cloud Backup** klicken, um zur Cloud Backup-Schnittstelle zu wechseln, um Backups auf mehr Volumes in jeder Arbeitsumgebung zu ermöglichen.

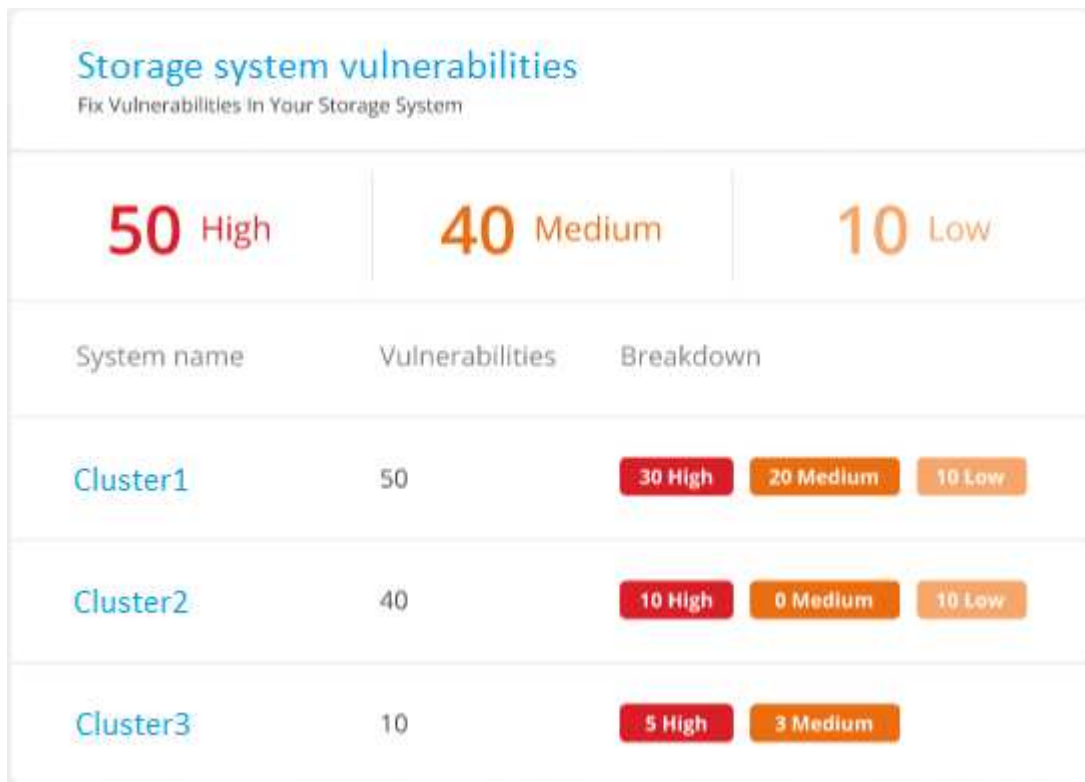
Schwachstellen im Storage-System

Das Fenster *Speichersystemschwachstellen* zeigt die Gesamtzahl der hohen, mittleren und niedrigen Sicherheitslücken, die das Active IQ Digital Advisor Tool auf jedem Ihrer ONTAP Cluster gefunden hat. Hohe Schwachstellen sollten sofort untersucht werden, um sicherzustellen, dass Ihre Systeme nicht für Angriffe geöffnet sind.

Voraussetzungen

- Der BlueXP Connector muss vor Ort installiert werden, nicht bei einem Cloud-Provider.
- Sie benötigen ein ONTAP Cluster vor Ort
- Das Cluster ist in Active IQ konfiguriert
- Sie müssen ein vorhandenes NSS-Konto in BlueXP registriert haben, um Ihre Cluster anzuzeigen und die Active IQ Digital Advisor-Benutzeroberfläche anzuzeigen.

Beachten Sie, dass Sie den Active IQ Digital Advisor direkt anzeigen können, indem Sie im BlueXP-Menü * Health > Digital Advisor* auswählen.



Klicken Sie auf die Art der Sicherheitsanfälligkeit (hoch, Mittel, Niedrig), die für einen der Cluster angezeigt werden soll, und Sie werden auf die Seite Sicherheitslücke in Active IQ Digital Advisor umgeleitet. (Mehr über diese Seite finden Sie im ["Active IQ Digital Advisor Dokumentation"](#).) Sie können die Sicherheitsanfälligkeiten anzeigen und anschließend die empfohlene Aktion befolgen, um das Problem zu beheben. Oftmals ist es dann die Lösung, ein Upgrade der ONTAP Software auf eine Point-Release- oder eine Vollversion durchzuführen, die die Sicherheitsanfälligkeit behebt.

Daten in Volumes, die mit SnapLock geschützt werden

Mit der NetApp SnapLock Technologie auf den ONTAP Volumes bleiben Dateien zu regulatorischen Zwecken in unveränderter Form erhalten. Sie können Dateien und Snapshot-Kopien auf WORM-Storage (Write Once, Read Many) festschreiben und Aufbewahrungszeiträume für diese WORM-geschützten Daten festlegen. ["Weitere Informationen zu SnapLock"](#).

Die `_kritische Unveränderlichkeit_Unveränderlichkeit_` zeigt die Anzahl der Elemente in Ihrer Arbeitsumgebung, die dank der ONTAP SnapLock Technologie vor Modifizierung und Löschung in WORM-Storage geschützt sind. So sehen Sie, wie viele Ihrer Daten eine unveränderliche Kopie haben, damit Sie ein besseres Verständnis Ihrer Backup- und Recovery-Pläne gegen Ransomware erhalten.

Voraussetzungen

- Der BlueXP Connector muss vor Ort installiert werden, nicht bei einem Cloud-Provider.
- Sie benötigen ein ONTAP Cluster vor Ort
- Sie müssen auf mindestens einem Knoten im Cluster eine **SnapLock**-Lizenz installiert haben

Critical data immutability

Make Sure You Are Creating Immutable Copies Of Your Business Critical Data Using SnapLock

2 selected Policies ▼

Configure Data Sense Policies →

 733

business critical items are
locked with SnapLock

Across 18 locked volumes

 1.3K

business critical items found in
all scanned environments
(locked volumes excluded)

Across 18 Working environments

In diesem Bereich werden zunächst Daten basierend auf den von uns ausgewählten Standardrichtlinien angezeigt. Sie können jedoch die 2 wichtigsten Daten Sense *Policies* auswählen, die Sie erstellt haben, um Ihre wichtigsten Geschäftsdaten anzuzeigen. Informieren Sie sich darüber ["Erstellen Sie Ihre Richtlinien mit Data Sense"](#).

Im Bereich werden die folgenden Informationen zu den Daten angezeigt, die den ausgewählten Richtlinien entsprechen:

- Die Anzahl der geschäftskritischen Dateien in allen gescannten Arbeitsumgebungen, die für die Verwendung von SnapLock konfiguriert sind.
- Die Anzahl der geschäftskritischen Dateien in allen gescannten Arbeitsumgebungen mit Ausnahme der für SnapLock konfigurierten Dateien. Beachten Sie, dass einige dieser Dateien mit einem anderen Mechanismus als SnapLock geschützt werden können.

Richtlinien für den Datensinn, die die folgenden Filter enthalten, sind in der Dropdown-Liste für ausgewählte Richtlinien nicht verfügbar, da sie wichtige Suchbereiche ausschließen:

- Name der Arbeitsumgebung
- Art der Arbeitsumgebung
- Storage Repository
- Dateipfad

Denken Sie also daran, Ihre wichtigen Geschäftsdaten über die Richtlinien zur Unveränderlichkeit kritischer Daten im Panel „_kritische Daten“ anzuzeigen.

Ransomware-Vorfälle auf Ihren Systemen erkannt

Ransomware-Vorfälle, die auf Ihren gemanagten Systemen erkannt wurden, werden als Warnmeldungen im Fenster „*Ransomware Incidents*“ angezeigt. Dazu gehören Verschlüsselungsprozesse, verdächtige Dateiendungen, Ransomware-Aktivitäten und böswillige Aktivitäten. Im Fenster wird die Art des Vorfalls angezeigt, und es wird angezeigt, ob automatische Aktionen ausgeführt wurden, um das Problem zu beheben. Beispielsweise könnte eine Volume Snapshot Kopie generiert und in die Cloud gesendet werden.

Ransomware Incidents (5)				
	Volume123	Multiple encryption (150) All automatic actions failed	Resolve	
	Volume345	Suspicious file extensions (75) No automatic action configured	Resolve	
	Volumeabc	Ransomware activity (120) Some automatic actions succeeded	Resolve	
	Volume999	Malicious activity (54) Snapshot sent to cloud via Cloud Backup	Resolve	
	Volume895	Multiple encryption (88) Snapshot taken	Resolve	

Aktuell werden ONTAP Cluster vor Ort unterstützt, auf denen Autonomous Ransomware Protection (ARP) ausgeführt wird. ARP nutzt Workload-Analysen in NAS-Umgebungen (NFS und SMB), um ungewöhnliche Aktivitäten, die auf einen Ransomware-Angriff hinweisen könnten, proaktiv zu erkennen und zu warnen. ["Hier erfahren Sie mehr"](#).

Sie können auf klicken Um einen Vorfall zu erweitern, um die Anzahl der verschlüsselten Dateien anzuzeigen, die im verdächtigen Volume identifiziert wurden, die Arten von Dateierweiterungen und den Zeitpunkt, zu dem der Angriff stattgefunden hat.

Ransomware Incidents (5)				
	Volume123	Multiple encryption All automatic actions failed	Resolve	
150	.docx, .jpg,	Autonomous ransomware ...	Snapshot taken	
No. encrypted files	Suspicious file extensions	Detect	Snapshot sent to cloud	
		Autonomous ransomware protection	Malicious IP blocked	
		ponses		April 07, 2022 21:45
				Date & time

Sie können auf die Schaltfläche **Auflösen** klicken, um den Vorfall von der Benutzeroberfläche zu entfernen. Ein Dialogfeld erscheint, um zu sehen, ob der gemeldete Vorfall ein echter Ransomware-Vorfall war oder nicht. Klicken Sie auf **Ja**, wenn das Problem ein echter Ransomware-Vorfall war. Klicken Sie auf **Nein**, wenn das Problem nicht ein echter Ransomware-Vorfall war.

Voraussetzungen

- Sie müssen über einen lokalen ONTAP-Cluster verfügen, der ONTAP 9.11 oder höher ausführt.
- Sie müssen die **Anti_Ransomware**-Lizenz (ONTAP 9.11.1 +) auf mindestens einem Knoten im Cluster installiert haben.
- NetApp Autonomous Ransomware Protection (ARP) muss 30 Tage lang zum ersten Mal Learning Period

(auch als „dry run“ bekannt) aktiviert sein, bevor er in den „aktiven Modus“ umgeschaltet wird. So hat es ausreichend Zeit, um Workload-Merkmale zu bewerten und mutmaßliche Ransomware-Angriffe korrekt zu melden.

Wissen und Support

Für den Support anmelden

Bevor Sie einen Support-Fall beim technischen Support von NetApp eröffnen können, müssen Sie BlueXP einen NetApp Support Site Account (NSS) hinzufügen und sich dann für den Support registrieren.

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren Ihres BlueXP-Konto-ID-Support-Abonnements (Ihre 20-stellige Seriennummer 960xxxxxxxxx auf der Seite Support-Ressourcen in BlueXP).

Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

Diese Seriennummern werden als *PAYGO Seriennummern* bezeichnet und werden zum Zeitpunkt der Cloud Volumes ONTAP Implementierung von BlueXP generiert.

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen.

Ihre Anmeldung hängt davon ab, ob Sie ein neuer oder bereits bestehender Kunde oder Partner sind.

- Bestehender Kunde oder Partner

Als bestehender NetApp Kunde oder Partner können Sie mit Ihrem NSS SSO-Konto (NetApp Support Site) die oben genannten Registrierungen durchführen. Im Support Dashboard stellt BlueXP eine **NSS Management**-Seite zur Verfügung, auf der Sie Ihr NSS-Konto hinzufügen können. Sobald Sie Ihr NSS-Konto hinzugefügt haben, registriert BlueXP diese Seriennummern automatisch für Sie.

[Erfahren Sie, wie Sie Ihr NSS-Konto hinzufügen.](#)

- Neu bei NetApp

Wenn Sie neu bei NetApp sind, müssen Sie eine einmalige Registrierung Ihrer BlueXP Account ID Seriennummer auf der Support-Registrierungsseite von NetApp abschließen. Sobald Sie diese Registrierung abgeschlossen und ein neues NSS-Konto erstellt haben, können Sie dieses Konto in BlueXP verwenden, um sich in Zukunft automatisch zu registrieren.

[Erfahren Sie, wie Sie sich mit NetApp anmelden können.](#)

Fügen Sie ein NSS-Konto zu BlueXP hinzu

Über das Support Dashboard können Sie Ihre NetApp Support Site Konten zur Verwendung mit BlueXP hinzufügen und managen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten

hinzufügen.

- Wenn Sie einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Klicken Sie auf **NSS Management > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Weiter**, um auf eine Microsoft-Login-Seite umgeleitet zu werden.

NetApp verwendet Microsoft Azure Active Directory als Identitäts-Provider für Authentifizierungsservices, die sich speziell für Support und Lizenzierung entscheiden.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

Beachten Sie Folgendes:

- Das Konto muss ein Kundenkonto auf Kundenebene sein (kein Gast- oder Temporkonto).
- Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern. Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet wird. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ... Menü.
- Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ... Menü. Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden.

Mit NetApp registrieren

Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

Bestandskunde mit NSS-Konto

Wenn Sie ein NetApp Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Wenn Sie dies noch nicht getan haben, fügen Sie Ihr NSS-Konto bei BlueXP hinzu.
3. Klicken Sie auf der Seite **Ressourcen** auf **für Support registrieren**.



Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits Kunde von NetApp mit vorhandenen Lizenzen und Seriennummern sind, aber *no* NSS Konto, müssen Sie nur ein NSS-Konto erstellen.

Schritte

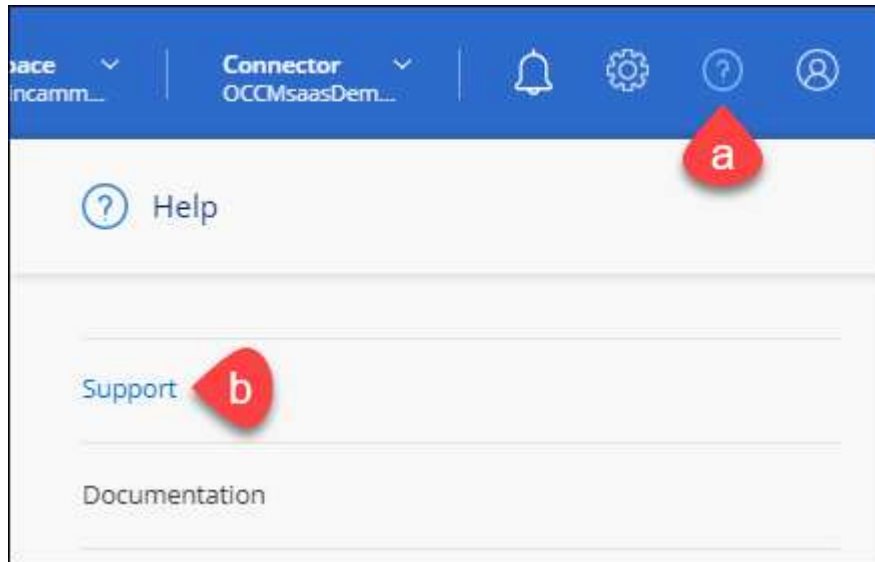
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen ["NetApp Support Site-Formular zur Benutzerregistrierung"](#)
 - a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
 - b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.

Neu bei NetApp

Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts in der BlueXP-Konsole auf das Hilfesymbol, und wählen Sie **Support**.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu ["Die Support-Registrierungs-Website von NetApp"](#) Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

7. Bestätigen Sie die Aktion in der E-Mail.

Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen ["NetApp Support Site-Formular zur Benutzerregistrierung"](#)
 - a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
 - b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Kontobearbeitung beschleunigt.

Nachdem Sie fertig sind

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Sobald Sie Ihren NetApp Support Site Account besitzen, können Sie im Portal BlueXP diesen NSS-Account für zukünftige Registrierungen hinzufügen.

Holen Sie sich Hilfe

NetApp bietet Unterstützung für BlueXP und seine Cloud-Services auf unterschiedliche Weise. Umfassende kostenlose Self-Support-Optionen stehen rund um die Uhr zur Verfügung, wie etwa Knowledge Base-Artikel (KB) und ein Community-Forum. Ihre Support-Registrierung umfasst technischen Remote-Support über Web-Ticketing.

Self-Support

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- ["Wissensdatenbank"](#)

Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- ["Communitys"](#)

Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu erstellen.

- Dokumentation

Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- [Mailto:ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)[Feedback email]

Wir wissen Ihre Vorschläge zu schätzen. Senden Sie uns Ihr Feedback, um BlueXP zu verbessern.

NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Bevor Sie beginnen

Um die * Case erstellen*-Fähigkeit zu verwenden, müssen Sie zuerst eine einmalige Registrierung Ihrer BlueXP Account ID-Seriennummer (dh 960xxxx) mit NetApp ["Erfahren Sie, wie Sie sich für Support registrieren"](#).

Schritte

1. Klicken Sie in BlueXP auf **Hilfe > Support**.
2. Wählen Sie eine der verfügbaren Optionen unter Technical Support:
 - a. Klicken Sie auf **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.
 - b. Klicken Sie auf **Case erstellen**, um ein Ticket mit einem NetApp Support-Experten zu öffnen:
 - **NetApp Support Site Account:** Wählen Sie das entsprechende NSS-Konto für die Person aus, die den Support-Case eröffnet. Diese Person ist der primäre Ansprechpartner bei NetApp, der Sie sich zusätzlich zu den unten aufgeführten zusätzlichen E-Mails mit anderen Kunden in Verbindung setzen kann.

Wenn Ihr NSS-Konto nicht angezeigt wird, können Sie im Support-Bereich von BlueXP zur Registerkarte **NSS Management** navigieren, um es dort hinzuzufügen.

- **Service:** Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
- **Arbeitsumgebung:** Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

Die Liste der Arbeitsumgebungen liegt im Bereich des BlueXP-Kontos, des Arbeitsbereichs und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Case Priority:** Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung:** Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen:** Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.

Create a Case

TESTCLOUD2NTAP

NetApp Support Site Account

Service

Cloud Manager
▼

Working Environment

Select...
▼

Case Priority

Low- General Guidance
▼

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional)

Attachment (Optional) Coming Soon

No files selected

Nachdem Sie fertig sind

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall und macht Sie umgehend mit.

Für eine Historie Ihrer Supportfälle können Sie auf **Einstellungen > Timeline** klicken und nach Aktionen mit dem Namen „Support Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Service zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Ihre Liste der NSS-Konten oben im **Case erstellen**-Formular überprüfen, um die richtige Übereinstimmung zu finden, oder Sie können Hilfe mit einer der folgenden Optionen suchen:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter <https://mysupport.netapp.com/site/help>

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

<http://www.netapp.com/us/legal/copyright.aspx>

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/us/media/patents-page.pdf>

Datenschutzrichtlinie

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

- ["Hinweis für BlueXP"](#)

Copyright-Informationen

Copyright © 2023 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 IRGEND EINER 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.