Versionshinweise

NetApp Ransomware Resilience

NetApp
February 11, 2026

Inhalt

Versionshinweise

Was ist neu bei NetApp Ransomware Resilience?

Informieren Sie sich über die Neuerungen bei NetApp Ransomware Resilience.

19. Januar 2026

Nicht unterstützte Volumes

Die Berichte zur Ransomware-Resilienz erfassen nun Informationen über unterstützte und nicht unterstützte Volumes im **Zusammenfassungsbericht**. Nutzen Sie diese Informationen, um zu diagnostizieren, warum Volumes in einem System möglicherweise nicht für den Ransomware-Schutz geeignet sind.

Weitere Informationen finden Sie unter "Berichte zum Thema Ransomware-Resilienz herunterladen".

12. Januar 2026

Snapshots in ONTAP replizieren

Ransomware Resilience unterstützt nun das Hinzufügen der Replikation von Snapshots zu einem sekundären ONTAP Standort. Mit Schutzgruppen, die eine Replikationsrichtlinie verwenden, können Sie für jede Arbeitslast an dasselbe Ziel oder an verschiedene Ziele replizieren. Sie können eine Ransomware-Schutzstrategie erstellen, die Replikation beinhaltet, oder die vordefinierte Strategie verwenden.

Weitere Informationen finden Sie unter "Workloads im Rahmen der Ransomware-Resilienz schützen".

Workloads von der Ransomware-Resilienz ausschließen

Ransomware Resilience unterstützt jetzt das Ausschließen bestimmter Workloads in einem System vom Schutz und vom Ransomware Resilience Dashboard. Sie können Workloads nach der Erkennung ausschließen und sie wieder einbeziehen, wenn Sie einen Ransomware-Schutz hinzufügen möchten. Für ausgeschlossene Arbeitslasten werden Ihnen keine Kosten in Rechnung gestellt.

Weitere Informationen finden Sie unter "Arbeitslasten ausschließen".

Benachrichtigungen als in Überprüfung markieren

Ransomware Resilience ermöglicht es Ihnen nun, Warnmeldungen als „In Prüfung“ zu markieren. Verwenden Sie das Label „In Prüfung“, um die Klarheit innerhalb Ihres Teams bei der Priorisierung und dem Management aktiver Ransomware-Bedrohungen zu verbessern.

Weitere Informationen finden Sie unter "Warnmeldungen in der Ransomware-Resilienz verwalten".

8. Dezember 2025

Die Blockierung von Erweiterungen ist auf Workload-Ebene aktiviert.

Wenn Sie die Erweiterungsblockierung aktivieren, erfolgt die Aktivierung nun auf Workload-Ebene und nicht mehr auf Ebene der Speicher-VM.

Benutzerverhaltenswarnungsstatus bearbeiten

Ransomware Resilience ermöglicht es Ihnen nun, den Status von Warnmeldungen zum Benutzerverhalten zu bearbeiten. Sie können Warnmeldungen manuell verwerfen und beheben.

Weitere Informationen finden Sie unter "Warnmeldungen in der Ransomware-Resilienz verwalten".

Unterstützung für mehrere Konsolenagenten

Ransomware Resilience unterstützt jetzt die Verwendung mehrerer Console-Agenten zur Verwaltung derselben Systeme.

Weitere Informationen zu Console-Agenten finden Sie unter"Erstellen eines Konsolenagenten" Die

10. November 2025

Diese Version enthält allgemeine Erweiterungen und Verbesserungen.

06. Oktober 2025

BlueXP ransomware protection heißt jetzt NetApp Ransomware Resilience

Der BlueXP ransomware protection wurde in NetApp Ransomware Resilience umbenannt.

BlueXP heißt jetzt NetApp Console

Die NetApp Console ermöglicht eine zentrale Verwaltung von Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene und liefert Einblicke in Echtzeit, schnellere Workflows und eine vereinfachte Verwaltung.

Einzelheiten zu den Änderungen finden Sie im "Versionshinweise zur NetApp Console" .

Erkennung von Datenschutzverletzungen

Ransomware Resilience umfasst einen neuen Erkennungsmechanismus, der in wenigen Schritten aktiviert werden kann, um anomale Benutzerlesevorgänge als Frühindikator für einen Datenverstoß zu erkennen. Ransomware Resilience sammelt und analysiert Lesevorgänge von Benutzern, indem es eine historische Basislinie erstellt, die ein Profil des erwarteten, normalen Verhaltens auf Grundlage der vergangenen Daten darstellt. Wenn die Aktivität eines neuen Benutzers erheblich von dieser festgelegten Norm abweicht (z. B. ein unerwarteter Anstieg der Lesevorgänge in Kombination mit verdächtigen Lesemustern), wird eine Warnung generiert. Ransomware Resilience umfasst ein KI-Modell zum Erkennen verdächtiger Lesemuster.

Anders als bei der Verschlüsselungserkennung durch ARP auf Speicherebene erfolgt die Erkennung der Anomalie des Benutzerverhaltens im Ransomware Resilience SaaS-Dienst durch das Sammeln von FPolicy-Ereignissen.

> Sie müssen die neue"Ransomware Resilience-Benutzerverhaltensadministrator und Ransomware Resilience-Benutzerverhaltensbetrachter" Rollen für den Zugriff auf Einstellungen zur Erkennung verdächtigen Benutzerverhaltens.

Weitere Informationen finden Sie unter"Aktivieren Sie die Erkennung verdächtiger Benutzeraktivitäten" Und"Anzeigen von anomalem Benutzerverhalten" .

Weitere Erkennungen verdächtiger Benutzeraktivitäten

Zusätzlich zur Erkennung von Datenschutzverletzungen erkennt Ransomware Resilience auch die folgenden Warnmeldungstypen basierend auf beobachteten verdächtigen Benutzeraktivitäten:

- **Datenzerstörung – potenzieller Angriff** – Eine Warnung mit der Schwere eines potenziellen Angriffs wird erstellt, wenn die Anzahl der Dateilöschungen die historische Norm überschreitet.
- **Verdächtiges Benutzerverhalten – potenzieller Angriff** – Eine Warnung mit dem Schweregrad eines potenziellen Angriffs wird erstellt, wenn Lese-, Umbenennungs- und Löschvorgänge in einer Sequenz beobachtet werden, die einem Ransomware-Angriff ähnelt.
- **Verdächtiges Benutzerverhalten – Warnung** – Eine Warnung mit dem Schweregrad „Warnung“ wird erstellt, wenn die Gesamtzahl der Dateiaktivitäten (Lesen, Löschen, Umbenennen usw.) die historische Norm überschreitet

Neue Benutzerrollen zur Erkennung von Datenschutzverletzungen

Um Warnmeldungen zu verdächtigen Benutzeraktivitäten zu verwalten, hat Ransomware Resilience zwei neue Rollen für Administratoren der Konsolenorganisation eingeführt, um Zugriff auf die Erkennung verdächtiger Benutzeraktivitäten zu gewähren: Ransomware Resilience-Benutzerverhaltensadministrator und Ransomware Resilience-Benutzerverhaltensbetrachter.

Sie müssen ein Benutzerverhaltensadministrator sein, um Einstellungen für verdächtiges Benutzerverhalten zu konfigurieren. Die Administratorrolle „Ransomware Resilience“ wird für die Konfiguration von Einstellungen für verdächtiges Benutzerverhalten nicht unterstützt.

Weitere Informationen finden Sie unter "Rollenbasierter Zugriff auf NetApp Ransomware Resilience" .

12. August 2025

Diese Version enthält allgemeine Erweiterungen und Verbesserungen.

15. Juli 2025

SAN-Workload-Unterstützung

Diese Version umfasst Unterstützung für SAN-Workloads im BlueXP ransomware protection. Sie können jetzt zusätzlich zu NFS- und CIFS-Workloads auch SAN-Workloads schützen.

Weitere Informationen finden Sie unter "Voraussetzungen für den BlueXP ransomware protection" .

Verbesserter Workload-Schutz

Diese Version verbessert den Konfigurationsprozess für Workloads mit Snapshot- und Backup-Richtlinien von anderen NetApp Tools wie SnapCenter oder BlueXP backup and recovery. In früheren Versionen erkannte der BlueXP ransomware protection die Richtlinien anderer Tools und ermöglichte Ihnen nur, die Erkennungsrichtlinie zu ändern. Mit dieser Version können Sie jetzt Snapshot- und Backup-Richtlinien durch BlueXP ransomware protection -Schutzrichtlinien ersetzen oder die Richtlinien anderer Tools weiterhin verwenden.

Weitere Einzelheiten finden Sie unter"Workloads schützen" .

E-Mail-Benachrichtigungen

Wenn der BlueXP ransomware protection einen möglichen Angriff erkennt, wird eine Benachrichtigung in den BlueXP Benachrichtigungen angezeigt und eine E-Mail an die von Ihnen konfigurierte E-Mail-Adresse gesendet.

Die E-Mail enthält Informationen zum Schweregrad, zur betroffenen Arbeitslast und einen Link zur Warnung auf der Registerkarte **Warnungen** des BlueXP ransomware protection .

Wenn Sie im BlueXP ransomware protection ein Sicherheits- und Ereignismanagementsystem (SIEM) konfiguriert haben, sendet der Dienst Warndetails an Ihr SIEM-System.

Weitere Einzelheiten finden Sie unter"Behandeln Sie erkannte Ransomware-Warnungen" .

9. Juni 2025

Aktualisierungen der Zielseite

Diese Version enthält Aktualisierungen der Zielseite für den BlueXP ransomware protection , die den Start der kostenlosen Testversion und die Entdeckung erleichtern.

Aktualisierungen der Bereitschaftsübung

Bisher konnten Sie eine Ransomware-Bereitschaftsübung durchführen, indem Sie einen Angriff auf eine neue Beispiel-Workload simulierten. Mit dieser Funktion können Sie den simulierten Angriff untersuchen und die Arbeitslast wiederherstellen. Verwenden Sie diese Funktion, um Warnbenachrichtigungen, Reaktionen und Wiederherstellungen zu testen. Führen Sie diese Übungen so oft wie nötig durch und planen Sie sie.

Mit dieser Version können Sie über eine neue Schaltfläche im BlueXP ransomware protection eine Ransomware-Bereitschaftsübung für eine Test-Workload ausführen. So können Sie Ransomware-Angriffe einfacher simulieren, ihre Auswirkungen untersuchen und Workloads effizient wiederherstellen – und das alles in einer kontrollierten Umgebung.

Sie können jetzt Bereitschaftsübungen zusätzlich zu NFS-Workloads auch für CIFS-Workloads (SMB) durchführen.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Aktivieren Sie BlueXP classification Klassifizierungsaktualisierungen

Bevor Sie die BlueXP classification innerhalb des BlueXP ransomware protection verwenden, müssen Sie die BlueXP classification aktivieren, um Ihre Daten zu scannen. Durch die Klassifizierung von Daten können Sie personenbezogene Daten (PII) finden, die das Sicherheitsrisiko erhöhen können.

Sie können die BlueXP classification auf einer Dateifreigabe-Workload innerhalb des BlueXP ransomware protection bereitstellen. Wählen Sie in der Spalte **Datenschutzgefährdung** die Option **Gefährdung identifizieren**. Wenn Sie den Klassifizierungsdienst aktiviert haben, identifiziert diese Aktion die Gefährdung. Andernfalls wird mit dieser Version in einem Dialogfeld die Option zum Bereitstellen der BlueXP classification angezeigt. Wählen Sie **Bereitstellen**, um zur Zielseite des BlueXP classification zu gelangen, wo Sie diesen Dienst bereitstellen können. W

Weitere Einzelheiten finden Sie unter "Stellen Sie die BlueXP classification in der Cloud bereit" und um den Dienst innerhalb des BlueXP ransomware protection zu nutzen, beziehen Sie sich auf "Scannen Sie mit der BlueXP classification nach personenbezogenen Daten" .

13. Mai 2025

Meldung nicht unterstützter Arbeitsumgebungen im BlueXP ransomware protection

Während des Erkennungsworkflows meldet der BlueXP ransomware protection weitere Details, wenn Sie mit der Maus über „Unterstützte“ oder „Nicht unterstützte Workloads“ fahren. Dies wird Ihnen helfen zu verstehen, warum einige Ihrer Workloads vom BlueXP ransomware protection nicht erkannt werden.

Es gibt viele Gründe, warum der Dienst eine Arbeitsumgebung nicht unterstützt. Beispielsweise könnte die ONTAP Version in Ihrer Arbeitsumgebung niedriger sein als die erforderliche Version. Wenn Sie mit der Maus über eine nicht unterstützte Arbeitsumgebung fahren, wird in einem Tooltip der Grund angezeigt.

Sie können die nicht unterstützten Arbeitsumgebungen während der ersten Erkennung anzeigen und dort auch die Ergebnisse herunterladen. Sie können die Ergebnisse der Erkennung auch über die Option **Workload-Erkennung** auf der Seite „Einstellungen“ anzeigen.

Weitere Einzelheiten finden Sie unter "Entdecken Sie Workloads im BlueXP ransomware protection" .

29. April 2025

Unterstützung für Amazon FSx for NetApp ONTAP

Diese Version unterstützt Amazon FSx for NetApp ONTAP. Diese Funktion hilft Ihnen, Ihre FSx für ONTAP -Workloads mit BlueXP ransomware protection zu schützen.

FSx für ONTAP ist ein vollständig verwalteter Dienst, der die Leistung des NetApp ONTAP -Speichers in der Cloud bereitstellt. Es bietet dieselben Funktionen, dieselbe Leistung und dieselben Verwaltungsfunktionen, die Sie vor Ort verwenden, mit der Agilität und Skalierbarkeit eines nativen AWS-Dienstes.

Am BlueXP ransomware protection -Workflow wurden die folgenden Änderungen vorgenommen:

- Discovery umfasst Workloads in FSx für ONTAP 9.15-Arbeitsumgebungen.
- Auf der Registerkarte „Schutz“ werden Workloads in FSx für ONTAP -Umgebungen angezeigt. In dieser Umgebung sollten Sie Sicherungsvorgänge mit dem FSx for ONTAP -Sicherungsdienst durchführen. Sie können diese Workloads mithilfe von BlueXP ransomware protection -Snapshots wiederherstellen.

  Sicherungsrichtlinien für eine auf FSx für ONTAP ausgeführte Workload können in BlueXP nicht festgelegt werden. Alle vorhandenen Sicherungsrichtlinien, die in Amazon FSx for NetApp ONTAP festgelegt sind, bleiben unverändert.

- Warnmeldungen zeigen die neue FSx for ONTAP Arbeitsumgebung.

Weitere Einzelheiten finden Sie unter "Erfahren Sie mehr über den BlueXP ransomware protection" .

Informationen zu den unterstützten Optionen finden Sie im "Einschränkungen des BlueXP ransomware protection" .

BlueXP -Zugriffsrolle erforderlich

Sie benötigen jetzt eine der folgenden Zugriffsrollen, um den BlueXP ransomware protection anzuzeigen, zu erkennen oder zu verwalten: Organisationsadministrator, Ordner- oder Projektadministrator, Ransomware-Schutzadministrator oder Ransomware-Schutz-Viewer.

"Erfahren Sie mehr über BlueXP -Zugriffsrollen für alle Dienste" .

14. April 2025

Bereitschaftsübungsberichte

Mit dieser Version können Sie Übungsberichte zur Vorbereitung auf Ransomware-Angriffe überprüfen. Mithilfe einer Bereitschaftsübung können Sie einen Ransomware-Angriff auf eine neu erstellte Beispiel-Workload simulieren. Untersuchen Sie dann den simulierten Angriff und stellen Sie die Beispiel-Arbeitslast wieder her. Mithilfe dieser Funktion können Sie durch das Testen von Warnbenachrichtigungen, Reaktions- und Wiederherstellungsprozessen sicherstellen, dass Sie im Falle eines tatsächlichen Ransomware-Angriffs vorbereitet sind.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Neue rollenbasierte Zugriffskontrollrollen und -berechtigungen

Bisher konnten Sie Benutzern basierend auf ihren Verantwortlichkeiten Rollen und Berechtigungen zuweisen, was Ihnen bei der Verwaltung des Benutzerzugriffs auf den BlueXP ransomware protection half. Mit dieser Version gibt es zwei neue Rollen speziell für den BlueXP ransomware protection mit aktualisierten Berechtigungen. Die neuen Rollen sind:

- Ransomware-Schutzadministrator
- Ransomware-Schutz-Viewer

Weitere Informationen zu Berechtigungen finden Sie unter "Rollenbasierter Zugriff auf Funktionen des BlueXP ransomware protection" .

Zahlungsverbesserungen

Diese Version enthält mehrere Verbesserungen des Zahlungsvorgangs.

Weitere Einzelheiten finden Sie unter "Einrichten von Lizenzierungs- und Zahlungsoptionen" .

10. März 2025

Simulieren Sie einen Angriff und reagieren Sie darauf

Simulieren Sie mit dieser Version einen Ransomware-Angriff, um Ihre Reaktion auf eine Ransomware-Warnung zu testen. Mithilfe dieser Funktion können Sie durch das Testen von Warnbenachrichtigungen, Reaktions- und Wiederherstellungsprozessen sicherstellen, dass Sie im Falle eines tatsächlichen Ransomware-Angriffs vorbereitet sind.

Weitere Einzelheiten finden Sie unter "Führen Sie eine Übung zur Vorbereitung auf Ransomware-Angriffe durch" .

Verbesserungen des Erkennungsprozesses

Diese Version enthält Verbesserungen der selektiven Erkennungs- und Neuerkennungsprozesse:

- Mit dieser Version können Sie neu erstellte Workloads entdecken, die den zuvor ausgewählten Arbeitsumgebungen hinzugefügt wurden.
- Sie können in dieser Version auch *neue* Arbeitsumgebungen auswählen. Mit dieser Funktion können Sie neue Workloads schützen, die Ihrer Umgebung hinzugefügt werden.

- Sie können diese Erkennungsprozesse während des Erkennungsprozesses zu Beginn oder innerhalb der Option „Einstellungen“ durchführen.

Weitere Einzelheiten finden Sie unter "Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Arbeitsumgebungen" Und "Konfigurieren von Funktionen mit der Option „Einstellungen“" .

Warnungen werden ausgelöst, wenn eine hohe Verschlüsselung erkannt wird

Mit dieser Version können Sie Warnmeldungen anzeigen, wenn bei Ihren Workloads eine hohe Verschlüsselung erkannt wird, auch ohne dass es zu starken Änderungen der Dateierweiterungen kommt. Diese Funktion, die ONTAP Autonomous Ransomware Protection (ARP) AI verwendet, hilft Ihnen, Workloads zu identifizieren, die einem Risiko von Ransomware-Angriffen ausgesetzt sind. Verwenden Sie diese Funktion und laden Sie die gesamte Liste der betroffenen Dateien mit oder ohne Erweiterungsänderungen herunter.

Weitere Einzelheiten finden Sie unter "Reagieren Sie auf eine erkannte Ransomware-Warnung" .

16. Dezember 2024

Erkennen Sie anomales Benutzerverhalten mit Data Infrastructure Insights Storage Workload Security

Mit dieser Version können Sie Data Infrastructure Insights Storage Workload Security verwenden, um anomales Benutzerverhalten in Ihren Speicher-Workloads zu erkennen. Diese Funktion hilft Ihnen, potenzielle Sicherheitsbedrohungen zu erkennen und potenziell böswillige Benutzer zu blockieren, um Ihre Daten zu schützen.

Weitere Einzelheiten finden Sie unter "Reagieren Sie auf eine erkannte Ransomware-Warnung" .

Bevor Sie Data Infrastructure Insights Storage Workload Security zum Erkennen anomalen Benutzerverhaltens verwenden, müssen Sie die Option mithilfe der Option **Einstellungen** des BlueXP ransomware protection konfigurieren.

Siehe "Konfigurieren Sie die BlueXP ransomware protection -Schutzeinstellungen" .

Auswählen von Workloads zum Erkennen und Schützen

Mit dieser Version können Sie jetzt Folgendes tun:

- Wählen Sie in jedem Connector die Arbeitsumgebungen aus, in denen Sie Workloads ermitteln möchten. Sie können von dieser Funktion profitieren, wenn Sie bestimmte Workloads in Ihrer Umgebung schützen möchten und andere nicht.
- Während der Workload-Erkennung können Sie die automatische Erkennung von Workloads pro Connector aktivieren. Mit dieser Funktion können Sie die Workloads auswählen, die Sie schützen möchten.
- Entdecken Sie neu erstellte Workloads für zuvor ausgewählte Arbeitsumgebungen.

Siehe "Workloads ermitteln" .

7. November 2024

Aktivieren Sie die Datenklassifizierung und suchen Sie nach personenbezogenen Daten (PII).

Mit dieser Version können Sie die BlueXP classification, eine Kernkomponente der BlueXP Familie, aktivieren, um Daten in Ihren Dateifreigabe-Workloads zu scannen und zu klassifizieren. Durch die Klassifizierung von Daten können Sie feststellen, ob Ihre Daten persönliche oder private Informationen enthalten, die das

Sicherheitsrisiko erhöhen können. Dieser Prozess wirkt sich auch auf die Wichtigkeit der Arbeitslast aus und hilft Ihnen sicherzustellen, dass Sie die Arbeitslasten mit dem richtigen Schutzniveau schützen.

Das Scannen nach PII-Daten im BlueXP ransomware protection ist im Allgemeinen für Kunden verfügbar, die die BlueXP classification eingesetzt haben. Die BlueXP classification ist als Teil der BlueXP Plattform ohne zusätzliche Kosten verfügbar und kann vor Ort oder in der Kunden-Cloud bereitgestellt werden.

Siehe "Konfigurieren Sie die BlueXP ransomware protection -Schutzeinstellungen" .

Um den Scanvorgang zu starten, klicken Sie auf der Seite „Schutz“ in der Spalte „Datenschutzgefährdung“ auf **Gefährdung identifizieren**.

"Scannen Sie mit der BlueXP classification nach personenbezogenen sensiblen Daten" .

SIEM-Integration mit Microsoft Sentinel

Sie können jetzt mithilfe von Microsoft Sentinel Daten zur Bedrohungsanalyse und -erkennung an Ihr Sicherheits- und Ereignismanagementsystem (SIEM) senden. Bisher konnten Sie den AWS Security Hub oder Splunk Cloud als Ihr SIEM auswählen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

Jetzt 30 Tage kostenlos testen

Mit dieser Version können neue Bereitstellungen des BlueXP ransomware protection jetzt 30 Tage lang kostenlos getestet werden. Zuvor war der BlueXP ransomware protection 90 Tage lang als kostenlose Testversion verfügbar. Wenn Sie bereits an der 90-tägigen kostenlosen Testversion teilnehmen, gilt dieses Angebot für die nächsten 90 Tage.

Wiederherstellen der Anwendungsarbeitslast auf Dateiebene für Podman

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie jetzt eine Liste der Dateien anzeigen, die möglicherweise von einem Angriff betroffen waren, und diejenigen identifizieren, die Sie wiederherstellen möchten. Wenn die BlueXP Konnektoren in einer Organisation (früher ein Konto) Podman verwendeten, war diese Funktion zuvor deaktiviert. Es ist jetzt für Podman aktiviert. Sie können die wiederherzustellenden Dateien vom BlueXP ransomware protection auswählen lassen, eine CSV-Datei hochladen, in der alle von einer Warnung betroffenen Dateien aufgelistet sind, oder manuell angeben, welche Dateien Sie wiederherstellen möchten.

"Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-Angriff" .

30. September 2024

Benutzerdefinierte Gruppierung von Dateifreigabe-Workloads

Mit dieser Version können Sie jetzt Dateifreigaben in Gruppen zusammenfassen, um Ihren Datenbestand einfacher zu schützen. Der Dienst kann alle Volumes einer Gruppe gleichzeitig schützen. Bisher mussten Sie jedes Volume einzeln schützen.

"Erfahren Sie mehr über die Gruppierung von Dateifreigabe-Workloads in Ransomware-Schutzstrategien" .

2. September 2024

Sicherheitsrisikobewertung von Digital Advisor

Der BlueXP ransomware protection sammelt jetzt Informationen über hohe und kritische Sicherheitsrisiken im Zusammenhang mit einem Cluster von NetApp Digital Advisor. Wenn ein Risiko erkannt wird, gibt der BlueXP ransomware protection im Bereich **Empfohlene Aktionen** des Dashboards eine Empfehlung aus: „Beheben Sie eine bekannte Sicherheitslücke im Cluster <Name>.“ Wenn Sie in der Empfehlung auf dem Dashboard auf **Überprüfen und beheben** klicken, wird vorgeschlagen, Digital Advisor und einen CVE-Artikel (Common Vulnerability & Exposure) zu überprüfen, um das Sicherheitsrisiko zu beheben. Wenn mehrere Sicherheitsrisiken bestehen, überprüfen Sie die Informationen im Digital Advisor.

Siehe "Digital Advisor -Dokumentation" .

Sichern Sie auf der Google Cloud Platform

Mit dieser Version können Sie als Sicherungsziel einen Bucket der Google Cloud Platform festlegen. Bisher konnten Sie Sicherungsziele nur zu NetApp StorageGRID, Amazon Web Services und Microsoft Azure hinzufügen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

Unterstützung für Google Cloud Platform

Der Dienst unterstützt jetzt Cloud Volumes ONTAP für Google Cloud Platform zum Speicherschutz. Zuvor unterstützte der Dienst nur Cloud Volumes ONTAP für Amazon Web Services und Microsoft Azure sowie lokales NAS.

"Erfahren Sie mehr über den BlueXP ransomware protection und die unterstützten Datenquellen, Sicherungsziele und Arbeitsumgebungen" .

Rollenbasierte Zugriffskontrolle

Sie können jetzt den Zugriff auf bestimmte Aktivitäten mit der rollenbasierten Zugriffskontrolle (RBAC) beschränken. Der BlueXP ransomware protection verwendet zwei Rollen von BlueXP: BlueXP Kontoadministrator und Nicht-Kontoadministrator (Viewer).

Einzelheiten zu den Aktionen, die jede Rolle ausführen kann, finden Sie unter "Rollenbasierte Zugriffskontrollberechtigungen" .

5. August 2024

Bedrohungserkennung mit Splunk Cloud

Sie können Daten zur Bedrohungsanalyse und -erkennung automatisch an Ihr Sicherheits- und Ereignismanagementsystem (SIEM) senden. Bei früheren Versionen konnten Sie nur den AWS Security Hub als Ihr SIEM auswählen. Mit dieser Version können Sie den AWS Security Hub oder Splunk Cloud als Ihr SIEM auswählen.

"Erfahren Sie mehr über die Konfiguration der BlueXP ransomware protection -Schutzeinstellungen" .

1. Juli 2024

Bringen Sie Ihre eigene Lizenz mit (BYOL)

Mit dieser Version können Sie eine BYOL-Lizenz verwenden, bei der es sich um eine NetApp -Lizenzdatei

(NLF) handelt, die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten.

"Weitere Informationen zum Einrichten der Lizenzierung" .

Wiederherstellen der Anwendungsarbeitslast auf Dateiebene

Bevor Sie eine Anwendungs-Workload auf Dateiebene wiederherstellen, können Sie jetzt eine Liste der Dateien anzeigen, die möglicherweise von einem Angriff betroffen waren, und diejenigen identifizieren, die Sie wiederherstellen möchten. Sie können die wiederherzustellenden Dateien vom BlueXP ransomware protection auswählen lassen, eine CSV-Datei hochladen, in der alle von einer Warnung betroffenen Dateien aufgelistet sind, oder manuell angeben, welche Dateien Sie wiederherstellen möchten.

> Wenn mit dieser Version nicht alle BlueXP Konnektoren in einem Konto Podman verwenden, ist die Funktion zur Wiederherstellung einzelner Dateien aktiviert. Andernfalls ist es für dieses Konto deaktiviert.

"Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-Angriff" .

Laden Sie eine Liste der betroffenen Dateien herunter

Bevor Sie eine Anwendungsarbeitslast auf Dateiebene wiederherstellen, können Sie jetzt auf die Seite „Warnungen“ zugreifen, um eine Liste der betroffenen Dateien in einer CSV-Datei herunterzuladen und dann die CSV-Datei über die Seite „Wiederherstellung“ hochzuladen.

"Erfahren Sie mehr über das Herunterladen betroffener Dateien vor der Wiederherstellung einer Anwendung" .

Schutzplan löschen

Mit dieser Version können Sie jetzt eine Ransomware-Schutzstrategie löschen.

"Erfahren Sie mehr über den Schutz von Workloads und die Verwaltung von Ransomware-Schutzstrategien" .

10. Juni 2024

Sperren von Snapshot-Kopien auf dem Primärspeicher

Aktivieren Sie diese Option, um die Snapshot-Kopien auf dem primären Speicher zu sperren, sodass sie für einen bestimmten Zeitraum nicht geändert oder gelöscht werden können, selbst wenn ein Ransomware-Angriff den Weg zum Sicherungsspeicherziel findet.

"Erfahren Sie mehr über den Schutz von Workloads und die Aktivierung der Backup-Sperre in einer Ransomware-Schutzstrategie" .

Unterstützung für Cloud Volumes ONTAP für Microsoft Azure

Diese Version unterstützt Cloud Volumes ONTAP für Microsoft Azure als System zusätzlich zu Cloud Volumes ONTAP für AWS und lokalem ONTAP NAS.

"Schnellstart für Cloud Volumes ONTAP in Azure"

"Erfahren Sie mehr über den BlueXP ransomware protection" .

Microsoft Azure als Backup-Ziel hinzugefügt

Sie können jetzt Microsoft Azure zusammen mit AWS und NetApp StorageGRID als Sicherungsziel hinzufügen.

"Erfahren Sie mehr über die Konfiguration von Schutzeinstellungen" .

14. Mai 2024

Lizenzierungsupdates

Sie können sich für eine 90-tägige kostenlose Testversion anmelden. In Kürze können Sie ein Pay-as-you-go-Abonnement beim Amazon Web Services Marketplace erwerben oder Ihre eigene NetApp -Lizenz mitbringen.

"Weitere Informationen zum Einrichten der Lizenzierung" .

CIFS-Protokoll

Der Dienst unterstützt jetzt lokales ONTAP und Cloud Volumes ONTAP in AWS-Systemen unter Verwendung der Protokolle NFS und CIFS. Die vorherige Version unterstützte nur das NFS-Protokoll.

Details zur Arbeitslast

Diese Version bietet jetzt mehr Details in den Workload-Informationen vom Schutz und anderen Seiten für eine verbesserte Bewertung des Workload-Schutzes. Anhand der Workload-Details können Sie die aktuell zugewiesene Richtlinie und die konfigurierten Sicherungsziele überprüfen.

"Erfahren Sie mehr über das Anzeigen von Workloaddetails auf den Schutzseiten" .

Anwendungskonsistenter und VM-konsistenter Schutz und Wiederherstellung

Sie können jetzt anwendungskonsistenten Schutz mit der NetApp SnapCenter -Software und VM-konsistenten Schutz mit dem SnapCenter Plug-in for VMware vSphere durchführen und so einen ruhigen und konsistenten Zustand erreichen, um einen möglichen späteren Datenverlust zu vermeiden, falls eine Wiederherstellung erforderlich ist. Wenn eine Wiederherstellung erforderlich ist, können Sie die Anwendung oder VM in einen der zuvor verfügbaren Zustände zurückversetzen.

"Erfahren Sie mehr über den Schutz von Workloads" .

Strategien zum Schutz vor Ransomware

Wenn für die Arbeitslast keine Snapshot- oder Sicherungsrichtlinien vorhanden sind, können Sie eine Ransomware-Schutzstrategie erstellen, die die folgenden Richtlinien enthalten kann, die Sie in diesem Dienst erstellen:

- Snapshot-Richtlinie
- Sicherungsrichtlinie
- Erkennungsrichtlinie

"Erfahren Sie mehr über den Schutz von Workloads" .

Bedrohungserkennung

Die Bedrohungserkennung ist jetzt über ein Sicherheits- und Ereignismanagementsystem (SIEM) eines Drittanbieters verfügbar. Das Dashboard zeigt jetzt eine neue Empfehlung zum Aktivieren der Bedrohungserkennung an, die auf der Seite „Einstellungen“ konfiguriert werden kann.

"Erfahren Sie mehr über das Konfigurieren von Einstellungsoptionen" .

Falsche positive Warnungen verwerfen

Auf der Registerkarte „Warnungen“ können Sie jetzt Fehlalarme verwerfen oder sich für eine sofortige Wiederherstellung Ihrer Daten entscheiden.

"Erfahren Sie mehr über die Reaktion auf eine Ransomware-Warnung" .

Erkennungsstatus

Auf der Seite „Schutz“ werden neue Erkennungsstatus angezeigt, die den Status der auf die Arbeitslast angewendeten Ransomware-Erkennung zeigen.

"Erfahren Sie mehr über den Schutz von Workloads und die Anzeige des Schutzstatus" .

CSV-Dateien herunterladen

Sie können CSV-Dateien* von den Seiten „Schutz“, „Warnungen“ und „Wiederherstellung“ herunterladen.

"Erfahren Sie mehr über das Herunterladen von CSV-Dateien vom Dashboard und anderen Seiten" .

Dokumentationslink

Der Link „Dokumentation anzeigen“ ist jetzt in der Benutzeroberfläche enthalten. Sie können auf diese Dokumentation über die Dashboard-Vertikale **Aktionen** zugreifen.  Option. Wählen Sie **Was ist neu**, um Details in den Versionshinweisen anzuzeigen, oder **Dokumentation**, um die Homepage der BlueXP ransomware protection anzuzeigen.

BlueXP backup and recovery

Der BlueXP backup and recovery muss auf dem System nicht mehr aktiviert sein. Sehen "Voraussetzungen" . Der BlueXP ransomware protection hilft bei der Konfiguration eines Sicherungsziels über die Option „Einstellungen“. Sehen "Konfigurieren der Einstellungen" .

Einstellungsoption

Sie können jetzt Sicherungsziele in den Einstellungen des BlueXP ransomware protection einrichten.

"Erfahren Sie mehr über das Konfigurieren von Einstellungsoptionen" .

5. März 2024

Schutzrichtlinienverwaltung

Zusätzlich zur Verwendung vordefinierter Richtlinien können Sie jetzt Richtlinien erstellen. "Weitere Informationen zum Verwalten von Richtlinien" .

Unveränderlichkeit auf sekundärem Speicher (DataLock)

Sie können das Backup jetzt mithilfe der NetApp DataLock-Technologie im Objektspeicher im Sekundärspeicher unveränderlich machen. "Weitere Informationen zum Erstellen von Schutzrichtlinien" .

Automatisches Backup auf NetApp StorageGRID

Zusätzlich zur Verwendung von AWS können Sie jetzt StorageGRID als Ihr Sicherungsziel auswählen. "Erfahren Sie mehr über die Konfiguration von Sicherungszielen" .

Zusätzliche Funktionen zur Untersuchung potenzieller Angriffe

Sie können jetzt weitere forensische Details anzeigen, um den erkannten potenziellen Angriff zu untersuchen. "Erfahren Sie mehr über die Reaktion auf eine Ransomware-Warnung" .

Wiederherstellungsprozess

Der Wiederherstellungsprozess wurde verbessert. Jetzt können Sie Volume für Volume oder alle Volumes für eine Arbeitslast wiederherstellen. "Erfahren Sie mehr über die Wiederherstellung nach einem Ransomware-Angriff (nachdem Vorfälle neutralisiert wurden)" .

"Erfahren Sie mehr über den BlueXP ransomware protection" .

6. Oktober 2023

Der BlueXP ransomware protection ist eine SaaS-Lösung zum Schutz von Daten, zur Erkennung potenzieller Angriffe und zur Wiederherstellung von Daten nach einem Ransomware-Angriff.

In der Vorabversion schützt der Dienst anwendungsbasierte Workloads von Oracle, VM-Datenspeichern und Dateifreigaben auf lokalem NAS-Speicher sowie Cloud Volumes ONTAP auf AWS (unter Verwendung des NFS-Protokolls) über BlueXP -Organisationen hinweg und sichert Daten im Amazon Web Services Cloud-Speicher.

Der BlueXP ransomware protection bietet die volle Nutzung mehrerer NetApp -Technologien, sodass Ihr Datensicherheitsadministrator oder Sicherheitsbetriebsingenieur die folgenden Ziele erreichen kann:

- Sehen Sie sich auf einen Blick den Ransomware-Schutz für alle Ihre Workloads an.
- Erhalten Sie Einblicke in Empfehlungen zum Schutz vor Ransomware
- Verbessern Sie Ihre Schutzlage basierend auf den Empfehlungen von BlueXP ransomware protection .
- Weisen Sie Ransomware-Schutzrichtlinien zu, um Ihre wichtigsten Workloads und Hochrisikodaten vor Ransomware-Angriffen zu schützen.
- Überwachen Sie den Zustand Ihrer Workloads und schützen Sie sie vor Ransomware-Angriffen, indem Sie nach Datenanomalien suchen.
- Bewerten Sie schnell die Auswirkungen von Ransomware-Vorfällen auf Ihre Arbeitslast.
- Erholen Sie sich intelligent von Ransomware-Vorfällen, indem Sie Daten wiederherstellen und sicherstellen, dass keine erneute Infektion von gespeicherten Daten aus erfolgt.

"Erfahren Sie mehr über den BlueXP ransomware protection" .

Bekannte Einschränkungen der NetApp Ransomware Resilience

Bekannte Einschränkungen kennzeichnen Plattformen, Geräte oder Funktionen, die von dieser Produktversion nicht unterstützt werden oder nicht ordnungsgemäß mit ihr zusammenarbeiten. Lesen Sie diese Einschränkungen sorgfältig durch.

Problem mit der Reset-Option für die Bereitschaftsübung

Wenn Sie für die Übung zur Vorbereitung auf Ransomware-Angriffe ein ONTAP 9.11.1-Volume auswählen, sendet Ransomware Resilience eine Warnung. Wenn Sie die Daten mit der Option „Auf Volume klonen“ wiederherstellen und den Drill zurücksetzen, schlägt der Rücksetzvorgang fehl.

Einschränkungen von Amazon FSx for NetApp ONTAP

Das Amazon FSx for NetApp ONTAP -System wird in Ransomware Resilience unterstützt. Für Amazon FSx für ONTAP gelten folgende Einschränkungen:

- Backup-Richtlinien werden für Amazon FSx für ONTAP nicht unterstützt. In dieser Umgebung sollten Sie Sicherungsvorgänge mit Amazon FSx für Sicherungen durchführen. Sie können diese Workloads mithilfe von Ransomware Resilience wiederherstellen.
- Wiederherstellungsvorgänge werden nur von Snapshots aus durchgeführt.