



Los geht's

Ransomware Protection

NetApp
January 09, 2023

Inhaltsverzeichnis

- Los geht's 1
 - Erfahren Sie mehr über Ransomware-Schutz 1
 - Monitoring des Status von Ransomware-Warnmeldungen 3

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 () 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.

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.