Über NetApp Antivirus-Schutz

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/antivirus/file-protection-virus-scanning-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Über NetApp Antivirus-Schutz . . . 1
- Informationen zu NetApp Virenscans mit ONTAP Vscan . . . 1
  - Funktionsweise der Virenprüfung . . . 1
  - ICAP-basiertes Vscan im Vergleich zum Antivirus Connector . . . 1
- Workflow für die Virenprüfung mit ONTAP Vscan . . . 3
- Antivirus Architektur mit ONTAP Vscan . . . 4
  - Vscan Server-Software . . . 5
  - Vscan ONTAP Einstellungen . . . 5
- ONTAP Vscan Partnerlösungen . . . 7

Über NetApp Antivirus-Schutz

Informationen zu NetApp Virenscans mit ONTAP Vscan

Vscan ist eine Antiviren-Scanlösung, mit der Sie Ihre Daten vor Viren und anderer Schadsoftware schützen können. Sie kombiniert von Partnern bereitgestellte Antivirensoftware mit ONTAP Funktionen und bietet Ihnen so die nötige Flexibilität, um Dateiscans zu managen.

Funktionsweise der Virenprüfung

Speichersysteme lagern Scanvorgänge an externe Server aus, auf denen Antivirensoftware von Drittanbietern gehostet wird.

Basierend auf dem aktiven Scanmodus sendet ONTAP Scananforderungen, wenn Clients über SMB auf Dateien zugreifen (On-Access) oder auf Dateien an bestimmten Speicherorten zugreifen, entweder nach einem Zeitplan oder sofort (On-Demand).

- Die *On-Access-Prüfung* kann verwendet werden, um Dateien beim Öffnen, Lesen, Umbenennen oder Schließen über SMB auf Viren zu überprüfen. Dateivorgänge werden ausgesetzt, bis der externe Server den Scanstatus der Datei meldet. Wurde die Datei bereits geprüft, erlaubt ONTAP die Dateioperation. Andernfalls wird eine Prüfung vom Server angefordert.

  On-access-Scanning wird für NFS nicht unterstützt.

- Die bedarfsgesteuerte Überprüfung kann verwendet werden, um Dateien sofort oder nach einem Zeitplan auf Viren zu prüfen. Es wird empfohlen, bedarfsgesteuerte Scans nur außerhalb der Spitzenzeiten auszuführen, um eine Überlastung der bestehenden Antiviren-Infrastruktur zu vermeiden, die normalerweise für die Prüfung bei Zugriff ausgelegt ist. Der externe Server aktualisiert den Scanstatus der geprüften Dateien, sodass die Zugriffsverzögerung über SMB reduziert wird. Wenn Dateiänderungen oder Software-Updates vorliegen, wird ein neuer Dateiscan vom externen Server angefordert.

  Sie können die On-Demand-Scanfunktion für jeden Pfad im SVM-Namensraum verwenden, auch für Volumes, die nur über NFS exportiert werden.

In der Regel werden sowohl der On-Access- als auch der On-Demand-Scanmodus auf einer SVM aktiviert. In beiden Modi ergreift die Antivirensoftware basierend auf Ihren Softwareeinstellungen Maßnahmen zur Behebung infizierter Dateien.

Der ONTAP Antivirus Connector, der von NetApp bereitgestellt und auf dem externen Server installiert wird, übernimmt die Kommunikation zwischen dem Storage-System und der Antivirensoftware. Ab ONTAP 9.20.1 unterstützt ONTAP einen ICAP-basierten Scanpfad (Internet Content Adaptation Protocol), sodass der Antivirus Connector nicht mehr erforderlich ist. Jede SVM verwendet entweder ICAP oder den Antivirus Connector, jedoch nicht beides.

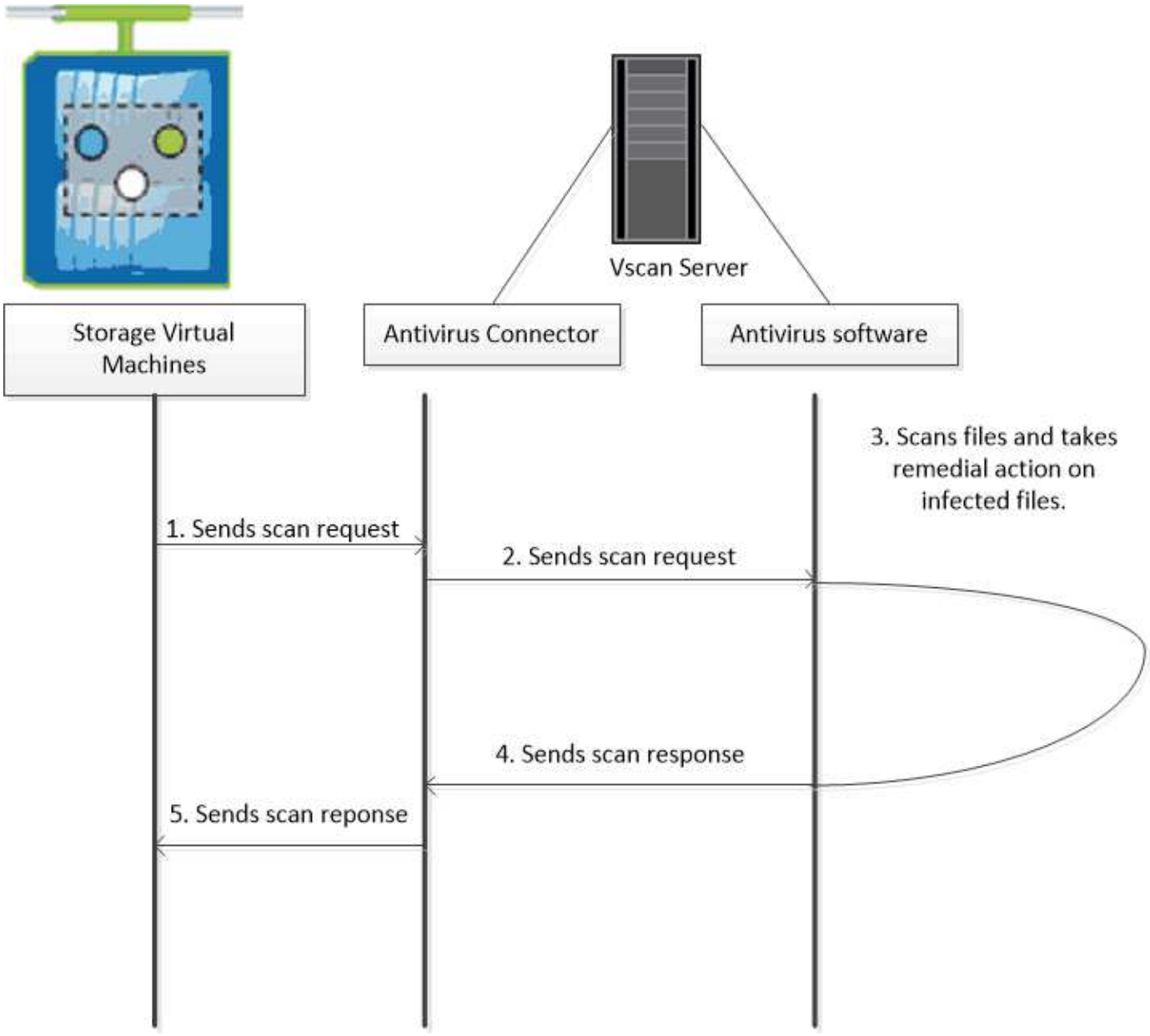
Vscan auf ICAP-Basis unterstützt nur das Scannen bei Dateizugriff.

ICAP-basiertes Vscan im Vergleich zum Antivirus Connector

Die folgende Tabelle fasst die Unterschiede zwischen dem Antivirus Connector und dem ICAP-basierten Vscan zusammen:

Funktion	Antivirus Connector	ICAP-basierter Vscan
Komponente	Auf einem Windows Server installierter ONTAP Antivirus Connector	Keine erforderlich; ONTAP verbindet sich direkt mit der Scan-Engine
Kommunikationsprotokoll	SMB Named Pipes und MS-RPC	ICAP über TCP
Infrastruktur	Dedizierter Vscan Verbindungsmanager	FPolicy Shared-Memory-Benachrichtigungspipeline
Unterstützte Betriebssysteme für Scan-Engines	Nur für Windows	Windows und Linux
Skalierbarkeit	Beschränkt auf 400 LIF Verbindungen pro Antivirus Connector Instanz	Nutzt FPolicy Verbindungspooling für höhere Skalierbarkeit
Erkennungsmechanismus	Polling-basierte Erkennung von SVMs und LIFs	Ereignisgesteuerte Verbindungsverwaltung über FPolicy

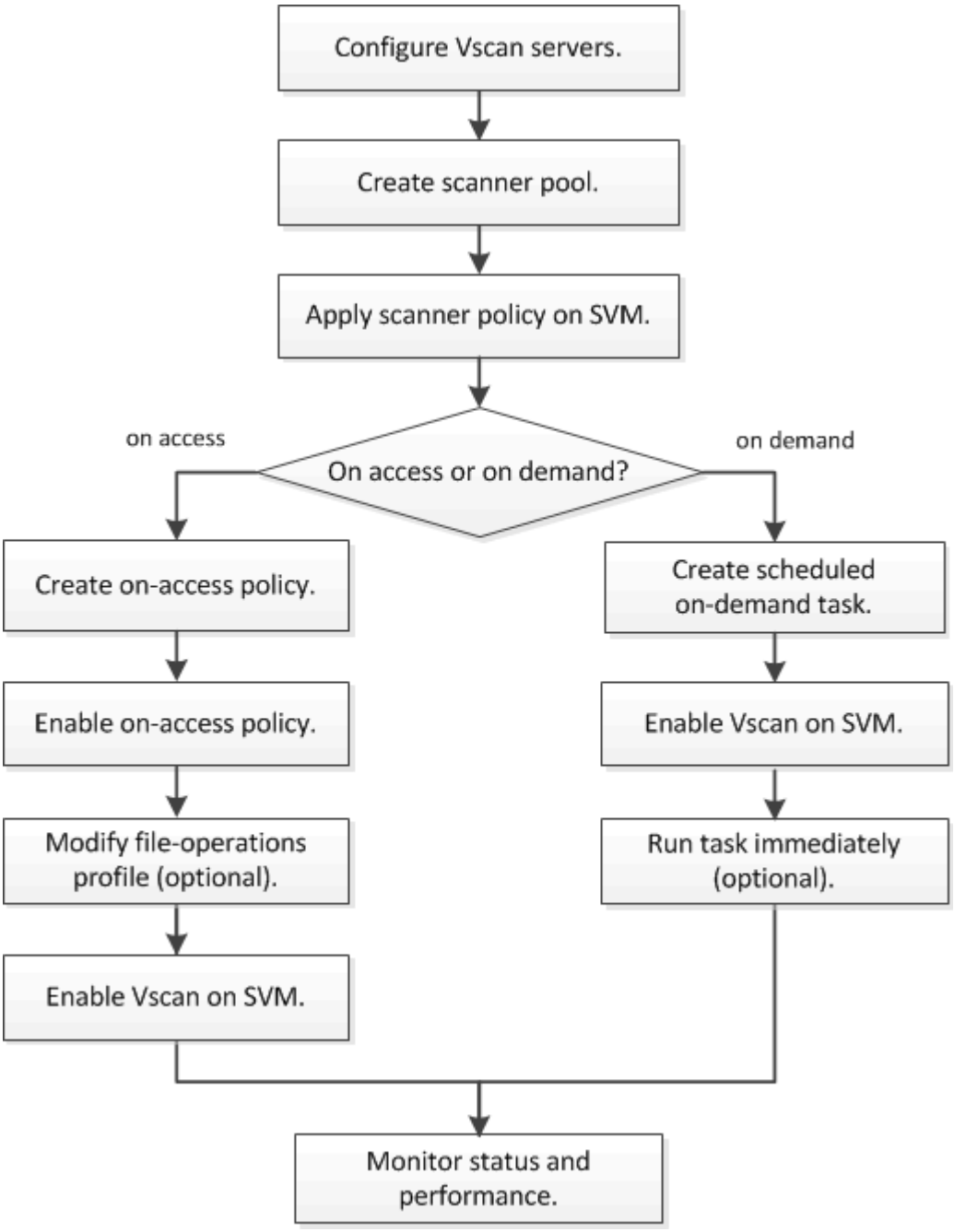
Das folgende Beispiel zeigt die Kommunikationsmethode von Antivirus Connector.



Workflow für die Virenprüfung mit ONTAP Vscan

Bevor Sie das Scannen aktivieren können, müssen Sie einen Scannerpool erstellen und eine Scannerrichtlinie anwenden. In der Regel werden sowohl der On-Access- als auch der On-Demand-Scanmodus auf einer SVM aktiviert.

Die CIFS Konfiguration muss abgeschlossen sein.



Um eine Aufgabe bei Bedarf zu erstellen, muss mindestens eine On-Access-Richtlinie aktiviert sein. Dies kann die Standardrichtlinie oder eine vom Benutzer erstellte On-Access-Richtlinie sein.

Nächste Schritte

- Einen Scannerpool auf einem einzelnen Cluster erstellen
- Eine Scannerrichtlinie auf einen einzelnen Cluster anwenden
- Eine On-Access-Richtlinie erstellen

Antivirus Architektur mit ONTAP Vscan

Die NetApp Antivirenarchitektur besteht aus Vscan Server-Software und den zugehörigen

Einstellungen.

Vscan Server-Software

Der ONTAP Antivirus Connector und die vom Partner bereitgestellte Antivirensoftware müssen auf demselben Vscan Server installiert sein.

- **ONTAP Antivirus Connector**

  Diese von NetApp bereitgestellte Software übernimmt die Kommunikation bezüglich Scananfragen und -antworten zwischen den SVMs und der Antivirensoftware. Sie kann auf einer virtuellen Maschine ausgeführt werden, für optimale Leistung wird jedoch ein physischer Rechner empfohlen. Diese Software ist auf der NetApp Support Site verfügbar (Anmeldung erforderlich).

- **Antivirensoftware**

  Hierbei handelt es sich um eine von einem Partner bereitgestellte Software, die Dateien auf Viren oder andere Schadsoftware überprüft. Bei der Konfiguration der Software wird festgelegt, welche Maßnahmen bei infizierten Dateien ergriffen werden.

Vscan ONTAP Einstellungen

Sie müssen die folgenden Vscan Einstellungen auf Ihrem ONTAP System konfigurieren.

- **scanner-pool**

  Diese Einstellung definiert die Vscan-Server und privilegierten Benutzer, die sich mit SVMs verbinden können. Sie legt außerdem eine Zeitüberschreitung für Scan-Anfragen fest, nach deren Ablauf die Scan-Anfrage an einen alternativen Vscan-Server gesendet wird, sofern einer verfügbar ist.

  > Die Zeitüberschreitungsperiode der Antivirensoftware auf dem Vscan Server sollte auf fünf Sekunden weniger als die scanner-pool Scan-Anforderungs-Zeitüberschreitungsperiode eingestellt werden. So werden Situationen vermieden, in denen der Dateizugriff verzögert oder vollständig verweigert wird, weil die Zeitüberschreitungsperiode der Software länger ist als die Zeitüberschreitungsperiode für die Scan-Anforderung.

- **Privilegierter Benutzer**

  Diese Einstellung ist ein Domänenbenutzerkonto, das ein Vscan-Server zur Verbindung mit der SVM verwendet. Das Konto muss in der Liste der privilegierten Benutzer im scanner-pool vorhanden sein.

- **Scannerrichtlinie**

  Diese Einstellung legt fest, ob ein scanner-pool aktiv ist. Scanner-Richtlinien sind systemdefiniert, daher können keine benutzerdefinierten scanner-pool-Richtlinien erstellt werden. Nur diese drei Richtlinien stehen zur Verfügung:

  - `Primary`gibt an, dass der scanner-pool aktiv ist.
  - `Secondary`Gibt an, dass der scanner-pool nur dann aktiv ist, wenn keiner der Vscan-Server im primären scanner-pool verbunden ist.
  - `Idle`gibt an, dass der scanner-pool inaktiv ist.

- **On-Access-Richtlinie**

Diese Einstellung definiert den Umfang eines On-Access-Scans. Sie können die maximale Dateigröße für den Scan, die Dateierweiterungen und Pfade, die in den Scan einbezogen werden sollen, sowie die Dateierweiterungen und Pfade, die vom Scan ausgeschlossen werden sollen, angeben.

Standardmäßig werden nur Lese-/Schreib-Volumes gescannt. Es können Filter angegeben werden, die das Scannen von schreibgeschützten Volumes ermöglichen oder das Scannen auf Dateien beschränken, die mit Ausführungsrechten geöffnet wurden:

- `scan-ro-volume` ermöglicht das Scannen von schreibgeschützten Volumes.
- `scan-execute-access`Beschränkt das Scannen auf Dateien, die mit Ausführungszugriff geöffnet wurden.

> „`Ausführungszugriff`“ ist etwas anderes als „`Ausführungsberechtigung.`“ Ein bestimmter Client hat nur dann „`Ausführungszugriff`“ auf eine ausführbare Datei, wenn die Datei mit „`execute intent.`“ geöffnet wurde.

Mit der `scan-mandatory`Option lässt sich `off` festlegen, dass Dateizugriff zulässig ist, wenn keine Vscan-Server für die Virenprüfung verfügbar sind. Im On-Access-Modus stehen diese beiden sich gegenseitig ausschließenden Optionen zur Auswahl:

- Erforderlich: Mit dieser Option versucht Vscan, die Scananfrage an den Server zu senden, bis die Zeitüberschreitung abgelaufen ist. Wird die Scananfrage vom Server nicht akzeptiert, wird die Zugriffsanfrage des Clients abgelehnt.
- Nicht obligatorisch: Bei dieser Option erlaubt Vscan immer den Clientzugriff, unabhängig davon, ob ein Vscan Server für den Virenscan verfügbar ist.

- **Auftrag auf Abruf**

Diese Einstellung definiert den Umfang eines bedarfsgesteuerten Scans. Sie können die maximale Dateigröße für den Scan, die Dateierweiterungen und Pfade, die in den Scan einbezogen werden sollen, sowie die Dateierweiterungen und Pfade, die vom Scan ausgeschlossen werden sollen, angeben. Dateien in Unterverzeichnissen werden standardmäßig gescannt.

Ein Cron-Schedule gibt an, wann die Aufgabe ausgeführt wird. Mit dem `vserver vscan on-demand-task run` Befehl lässt sich die Aufgabe sofort ausführen. Weitere Informationen zu `vserver vscan on-demand-task run` finden sich in der "ONTAP-Befehlsreferenz".

- **Vscan Dateioperationsprofil (nur Scannen bei Zugriff)**

Der `vscan-fileop-profile` Parameter für den `vserver cifs share create` Befehl definiert, welche SMB-Dateioperationen eine Virussuche auslösen. Standardmäßig ist der Parameter auf `standard` gesetzt, was der NetApp Best Practice entspricht. Dieser Parameter kann bei der Erstellung oder Änderung einer SMB-Freigabe angepasst werden.

- `no-scan`gibt an, dass für die Freigabe niemals Virenscans ausgelöst werden.
- `standard` gibt an, dass Virenscans durch Öffnungs-, Schließ- und Umbenennungsvorgänge ausgelöst werden.
- `strict`legt fest, dass Virusscans durch Öffnungs-, Lese-, Schließ- und Umbenennungsvorgänge ausgelöst werden.

  Das `strict` Profil bietet erhöhte Sicherheit für Situationen, in denen mehrere Clients gleichzeitig auf eine Datei zugreifen. Schließt ein Client eine Datei, nachdem er einen Virus hineingeschrieben hat, und

bleibt dieselbe Datei auf einem zweiten Client geöffnet, `strict` wird sichergestellt, dass ein Lesevorgang auf dem zweiten Client einen Scan auslöst, bevor die Datei geschlossen wird.

Sie sollten darauf achten, das `strict` Profil auf Freigaben zu beschränken, die Dateien enthalten, auf die voraussichtlich gleichzeitig zugegriffen wird. Da dieses Profil mehr Scan-Anfragen generiert, kann dies die Leistung beeinträchtigen.

- `writes-only` gibt an, dass Virenscans nur dann ausgelöst werden, wenn geänderte Dateien geschlossen werden.

Da `writes-only`weniger Scan-Anfragen generiert werden, wird die Leistung in der Regel verbessert. Bei Verwendung dieses Profils muss der Scanner so konfiguriert sein, dass nicht reparierbare, infizierte Dateien gelöscht oder unter Quarantäne gestellt werden, sodass kein Zugriff mehr möglich ist. Schließt beispielsweise ein Client eine Datei, nachdem er einen Virus hineingeschrieben hat, und wird die Datei nicht repariert, gelöscht oder unter Quarantäne gestellt, wird jeder Client, der auf die Datei `without` schreibt, infiziert.

Wenn eine Clientanwendung eine Umbenennung durchführt, wird die Datei mit dem neuen Namen geschlossen und nicht gescannt. Falls solche Vorgänge in Ihrer Umgebung ein Sicherheitsrisiko darstellen, empfiehlt sich die Verwendung des `standard` oder `strict` Profils.

Weitere Informationen zu `vserver cifs share create` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Vscan Partnerlösungen

NetApp arbeitet mit Trellix, Symantec, Trend Micro, Sentinel One, Deep Instinct und OPSWAT zusammen, um branchenführende Anti-Malware- und Anti-Virus-Lösungen bereitzustellen, die auf der ONTAP Vscan Technologie aufbauen. Diese Lösungen ermöglichen das Scannen von Dateien auf Malware und die Behebung betroffener Dateien.

Wie aus der folgenden Tabelle hervorgeht, werden die Interoperabilitätsdetails für Trellix und Trend Micro im NetApp Interoperability Matrix Tool verwaltet. Für alle anderen Partner, darunter Sentinel One, Symantec, Deep Instinct und OPSWAT, werden die Interoperabilitätsdetails auf den jeweiligen Partner-Websites verwaltet.

Partner	Lösungsdokumentation	Details zur Interoperabilität
Trellix (ehemals McAfee)	"Trellix Produktdokumentation"	• "NetApp Interoperabilitätsmatrix-Tool" • "NetApp Konfiguration auf Trellix ePO - Lokal verwaltete Endpunkte (trellix.com)"

Partner	Lösungsdokumentation	Details zur Interoperabilität
Symantec	"Symantec Protection Engine 9.0.0"	• "Support Matrix für Partnergeräte, die mit Symantec Protection Engine (SPE) für Network Attached Storage (NAS) 9.x.x zertifiziert sind" • Ab ONTAP 9.20.1 unterstützt das ICAP-basierte Vscan Symantec für On-Access-Scanning.
Trend Micro	"Dateisicherheit für NetApp ONTAP Vscan Support einrichten"	k. A.
Sentinel One	• "SentinelOne Singularity Cloud Data Security" • "Bedrohungserkennung für NetApp"	k. A.
Deep Instinct	Deep Instinct DSX für NAS • "Dokumentation und Interoperabilität" Für diesen Link ist eine Benutzeranmeldung erforderlich. Zugriff kann bei Deep Instinct angefordert werden. • "Datenblatt"	k. A.
OPSWAT	OPSWAT MetaDefender Storage Security • "MetaDefender Storage Security Integration mit NetApp" • "OPSWAT Partnerseite" • "Lösungsüberblick Integration"	Ab ONTAP 9.20.1 wird OPSWAT MetaDefender Storage Security durch ICAP-basiertes Vscan für On-Access-Scanning unterstützt.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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