Datenblatt

Sicherheitsfunktionen in ONTAP 9

Sicherheit für Ihre Daten – die wichtigste Ressource von Unternehmen

Wichtigste Vorteile

Verbessern von Datenvertraulichkeit, -integrität und -verfügbarkeit
Die ONTAP Data-Fabric-Sicherheitsfunktionen schützen die wichtigsten Ressourcen in Ihrem Unternehmen: die Daten.

Belastbare Sicherheit im Unternehmen
Errichten Sie eine sichere Grundlage für die Data-Fabric-Architektur Ihres Unternehmens und erhalten Sie einen Überblick über die Sichtbarkeits- und Sicherheitsfunktionen für eine sichere Infrastruktur.

Anwenden von NetApp und Branchen-Best-Practices für Sicherheit
Mit der Kompetenz und dem Branchen-Know-how von NetApp entsteht eine überprüfte Sicherheitsstruktur.

Einhalten von Governance- und Compliance-Anforderungen
Bewährte Sicherheits-Best-Practices werden angewendet, um Branchenvorgaben und Sicherheit-Compliance einzuhalten und zu unterstützen.

Die NetApp ONTAP Datenmanagement-Software entwickelt sich weiter und Sicherheit ist dabei ein integraler Bestandteil der Lösung. Die neueste Version von ONTAP 9 enthält viele neue Sicherheitsfunktionen, die für Ihr Unternehmen von unschätzbarem Wert sind, um die Daten in der gesamten Hybrid Cloud zu schützen und die Best Practices der Branche einzuhalten. Diese neuen Funktionen unterstützen Ihr Unternehmen außerdem dabei, sich weiter in Richtung eines Zero-Trust-Modells zu bewegen.

Weitere Informationen zur Erhöhung der Sicherheit in ONTAP 9 finden Sie im Dokument TR-4569: Security Hardening Guide for NetApp ONTAP 9.

Die Herausforderung

Moderne Unternehmen müssen sich heute der digitalen Transformation stellen. Es wird erwartet, dass sie Daten, die verteilt sind und immer unterschiedlicher und dynamischer werden, effektiv managen. Jeden Tag entstehen neue, komplexere Bedrohungen, die für IT-Umgebungen immer gefährlicher werden. Von Storage Engineers wird in ihrer Rolle als Administratoren und Betreiber der Datenbestände erwartet, dass sie die Daten während ihres gesamten Lebenszyklus sicher managen und aufbewahren.

Die Lösung

Die NetApp ONTAP 9 Software ist der Schlüssel zum Schutz Ihrer Daten und zur Erfüllung von Compliance-Anforderungen. Dieses Datenblatt und der Bericht TR-4569: Security Hardening Guide for NetApp ONTAP 9 stellen grundlegende Elemente zum Erreichen einer in der Branche bewährten Sicherheit für Ihre wichtigste Ressourcen dar: Ihre Daten.

NetApp®

Sicherheitsfunktionen in ONTAP 9

In Tabelle 1 werden die Sicherheitsfunktionen in ONTAP 9 vorgestellt.

Software oder Funktionen	Funktion	Auswirkungen
NetApp Volume Encryption (NVE)	NVE ist ein softwarebasierter Verschlüsselungsmechanismus, mit dem Sie Daten auf jeder beliebigen Festplatte mit einem eindeutigen Schlüssel pro Volume verschlüsseln können.	Verschlüsselung für Daten im Ruhezustand bleibt weiterhin ein wichtiges Thema in der Branche. NVE erfüllt dieses Anliegen und sorgt für umfangreiche Sicherheit in der gesamten Hybrid Cloud.
Sicheres Löschen mit NVE	Mit dieser Funktion erhalten Sie einen Befehl zum kryptografischen Schreddern gelöschter Dateien auf NVE Volumes. Dabei werden intakte Dateien verschoben und die Verschlüsselungsschlüssel von infizierten Dateien gelöscht.	Sie können Datenlecks online entgegenwirken, während das System betriebsbereit bleibt. Zudem profitieren Sie von der hochmodernen „Recht auf Löschung"-Funktionalität für die Datenschutz-Grundverordnung (DSGVO).
NetApp Aggregate Encryption (NAE)	NAE ist ein softwarebasierter Verschlüsselungsmechanismus, mit dem Sie Daten auf jedem beliebigen Laufwerkstyp mit eindeutigen Schlüsseln pro Aggregat, das von verschlüsselten Volumes gemeinsam genutzt wird, verschlüsseln können.	Wie NVE ermöglicht NAE auch die Verschlüsselung von Daten im Ruhezustand. Aggregatdeduplizierung ist bei NAE aktiviert, da die Volumes eines Aggregats dieselben Schlüssel verwenden und so bessere Storage-Effizienzfunktionen bieten.
Standardmäßige Verschlüsselung von Daten im Ruhezustand	Die Verschlüsselung von Daten im Ruhezustand ist standardmäßig aktiviert, wenn ein externer oder der integrierte Schlüsselmanager definiert werden. Dabei kommt die softwarebasierte Verschlüsselung von NVE oder NAE zum Einsatz. Wenn NSE Laufwerke Teil der Cluster-Konfiguration sind, ist die Verschlüsselung von Daten im Ruhezustand bereits gewährleistet und die softwarebasierte Verschlüsselung wird nicht standardmäßig aktiviert.	Die standardmäßige Verschlüsselung von Daten im Ruhezustand vereinfacht den Erhalt der umfangreichen Sicherheit in der gesamten Hybrid Cloud.
NetApp Storage Encryption (NSE)	NSE ist die NetApp Implementierung der vollständigen Festplattenverschlüsselung (Full Disk Encryption, FDE) unter Verwendung von Self-Encrypting Drives nach FIPS 140-2 Level 2. NSE bietet außerdem unterbrechungsfreie Verschlüsselungsimplementierung, die die gesamte Suite der NetApp Storage-Effizienztechnologien unterstützt.	Verschlüsselung für Daten im Ruhezustand bleibt weiterhin ein wichtiges Thema in der Branche. FDE von NSE kommt dieser Anforderung nach. In der NetApp Data Fabric bleibt lückenlos ein hohes Maß an Sicherheit gewahrt.
SMB-Verschlüsselung, beschleunigt durch Intel AES New Instructions (AES-NI)	Intel AES-NI verbessert den AES-Algorithmus und beschleunigt die Datenverschlüsselung mit unterstützten Prozessorfamilien.	Durch das Beschleunigen der Sicherheitsfunktionen wird die Effizienz gesteigert. Die effiziente Nutzung von Ressourcen ist ein entscheidender Aspekt für die erfolgreiche Bereitstellung von Sicherheitslösungen.
NetApp Cryptographic Security Module	Dieses Modul bietet nach FIPS 140-2 validierten kryptografischen Betrieb für ausgewählte SSL-basierte (Secure Sockets Layer) Managementservices.	Dedizierte Sicherheitsmodule verbessern die Ressourceneffizienz. Zudem ist FIPS 140-2 der anerkannte Branchenstandard für Kryptografieprodukte und -lösungen.
NetApp CryptoMod	Dieses Modul bietet nach FIPS 140-2 validierten kryptografischen Betrieb für NVE, NAE und den Onboard Key Manager (OKM).	FIPS 140-2 ist der anerkannte Branchenstandard für Kryptografieprodukte und -lösungen.
SHA-2 (SHA-512)-Support	Um die Passwortsicherheit zu verbessern, unterstützt ONTAP 9 die SHA-2-Passwort-Hash-Funktion und nutzt standardmäßig SHA-512, um neu erstellte oder geänderte Passwörter zu hashen.	SHA-2 ist inzwischen der Branchenstandard für Hash-Funktionen. Dies liegt an der wesentlich verbesserten Sicherheit gegenüber dem häufig kompromittierten SHA-1-Standard.
Sichere Protokollweiterleitung (Syslog über Transport Layer Security [TLS])	Die Protokollweiterleitungsfunktion unterstützt Ihre Administratoren dabei, Ziele so bereitzustellen, dass sie Syslog- und Audit-Informationen empfangen können. Aufgrund der Sicherheit der Syslog- und Audit-Informationen kann ONTAP 9 diese Informationen mithilfe der TCP-verschlüsselten Parameter sicher über TLS versenden.	Protokoll- und Audit-Informationen sind für Ihr Unternehmen im Hinblick auf Support und Verfügbarkeit von unschätzbarem Wert. Zudem handelt es sich bei den in Protokollen (Syslog) und Audit-Berichten enthaltenen Informationen in der Regel um sehr sensible Daten. Um Ihre Sicherheitskontrollen und Sicherheitsstatus aufrechtzuerhalten, müssen die Protokoll- und Audit-Daten sicher gemanagt werden.
TLS 1.1 und TLS 1.2	ONTAP 9 nutzt TLS 1.1 und TLS 1.2 für sichere Kommunikations- und Administrationsfunktionen.	NetApp rät von der Verwendung von TLS 1.0 ab, da es erhebliche Schwachstellen aufweist und somit Compliance -Standards wie PCI-DSS nicht erfüllt. NetApp empfiehlt die Verwendung von TLS 1.1 und TLS 1.2 aufgrund ihrer Stärke und Integrität.
Online Certificate Status Protocol (OCSP)	Dank aktiviertem OCSP können ONTAP 9 Applikationen, die TLS-Kommunikation wie LDAP oder TLS verwenden, einen digitalen Zertifikatsstatus erhalten. Die Applikation erhält eine signierte Antwort, die angibt, ob das angeforderte Zertifikat in Ordnung, annulliert oder unbekannt ist.	OCSP hilft, den aktuellen Status eines digitalen Zertifikats zu ermitteln. Dafür sind keine Certificate Revocation Lists (CRL, Zertifikatsannullierungslisten) erforderlich.
Onboard Key Manager (OKM)	OKM in ONTAP 9 bietet eine eigenständige Verschlüsselungslösung für Daten im Ruhezustand. OKM arbeitet mit NVE, die einen softwarebasierten Verschlüsselungsmechanismus bietet, mit dem Sie Daten verschlüsseln und beliebige Laufwerkstypen verwenden können. OKM nutzt auch NSE, die FDE mithilfe von Self-Encrypting Drives durchführt.	OKM bietet Verschlüsselungsmanagement für NSE und NVE. Zudem können Sie mithilfe der Verschlüsselungstechnologie in ONTAP 9 Daten im Ruhezustand sichern, was für jede Datensicherheitslösung von großer Bedeutung ist.
OKM Secure Boot	Diese Option erfordert nach dem Neustart eines Node gegebenenfalls eine Passphrase zum Entsperren von Laufwerken und Entschlüsseln von Volumes.	Wenn NSE und NVE den OKM verwenden, bietet der sichere Neustart Schutz vor Diebstahl des gesamten Storage-Arrays und nicht nur einzelner Laufwerke. Die Funktion ermöglicht außerdem einen sicheren physischen Transport von ganzen Clustern und die sichere Rückgabe von Geräten.

Tabelle 1) Sicherheitsfunktionen

Software oder Funktionen	Funktion	Auswirkungen
Externes Verschlüsselungskeymanagement	Das externe Verschlüsselungsmanagement wird von einem Drittanbietersystem in der Storage-Umgebung übernommen. Dieses Drittanbietersystem managt sicher die Authentifizierungsschlüssel und die Verschlüsselungsschlüssel, die von Verschlüsselungsfunktionen im Storage-System verwendet werden, z. B. von NSE, NVE oder NAE. Das Storage-System verwendet eine SSL-Verbindung, um den externen Verschlüsselungsmanagement-Server zu kontaktieren und Authentifizierungsschlüssel oder Volume-Datenverschlüsselungsschlüssel über das Key Management Interoperability Protocol (KMIP) zu speichern oder abzurufen.	Mit dem externen Verschlüsselungsmanagement zentralisieren Sie die Verschlüsselungsmanagement-Funktionen Ihres Unternehmens und bestätigen grundsätzlich, dass Schlüssel nicht in der Nähe der zugehörigen Assets gespeichert sind. Dieser Ansatz verringert das Risiko einer Kompromittierung.
Mandantenfähiges externes Verschlüsselungsmanagement	Mandantenfähiges externes Verschlüsselungsmanagement bietet die Möglichkeit, dass einzelne Mandanten oder Storage Virtual Machines (SVMs) ihre eigenen Schlüssel über KMIP für NVE aufbewahren können.	Mit dem mandantenfähigen externen Verschlüsselungsmanagement zentralisieren Sie die Verschlüsselungsmanagement-Funktionen Ihres Unternehmens nach Abteilung oder Mandanten und bestätigen grundsätzlich, dass Schlüssel nicht in der Nähe der zugehörigen Assets gespeichert sind. Dieser Ansatz verringert das Risiko einer Kompromittierung.
Verbessertes Filesystem-Auditing	ONTAP 9 erhöht die Anzahl der Auditing-Ereignisse und Details, die über eine Lösung hinweg berichtet werden. Die folgenden wichtigen Details werden bei der Erstellung von Ereignissen festgehalten: • Datei • Ordner • Zugriff auf Shares • erstellte, bearbeitete oder gelöschte Dateien • erfolgreicher Lesezugriff auf die Datei • fehlgeschlagene Versuche, Felder zu lesen oder Dateien zu schreiben • geänderte Ordnerrechte	NAS-Filesysteme haben einen größeren Fußabdruck in der heutigen Bedrohungslandschaft. Daher ist Sichtbarkeit durch die Audit-Funktionen weiterhin enorm wichtig und die erweiterte Audit-Funktion in ONTAP 9 bietet mehr CIFS-Audit-Details als je zuvor.
SMB-Signing and Sealing mit CIFS	SMB-Signaturen tragen dazu bei, die Sicherheit Ihrer Data Fabric zu steigern, indem der Datenverkehr zwischen den Storage-Systemen und den Clients vor Replay- oder Man-in-the-middle-Angriffen geschützt wird. Sie bestätigen zudem, dass SMB-Nachrichten über gültige Signaturen verfügen. Zusätzlich unterstützt ONTAP 9 SMB-Verschlüsselung, auch bekannt als Sealing.	Ein gängiger Bedrohungsvektor für Filesysteme und Architekturen ist das SMB-Protokoll. Das „Signing and Sealing“ ermöglicht eine uneingeschränkte Validierung des Verkehrs neben sicherem Datentransport auf einer Share-by-Share-Basis.
Kerberos 5 und krb5p-Support	ONTAP 9 unterstützt 128-Bit- und 256-Bit-AES-Verschlüsselung für Kerberos. Der Datenschutzservice umfasst die Verifizierung der Integrität von empfangenen Daten, Benutzerauthentifizierung und Datenverschlüsselung vor der Übertragung.	Krb5p-Authentifizierung schützt vor Datenmanipulation und -ausspähung durch das Verwenden von Prüfsummen, um den gesamten Verkehr zwischen Client und Server zu verschlüsseln.
SMB-Signing and Sealing mit Lightweight Directory Access Protocol (LDAP)	ONTAP 9 unterstützt das Signing and Sealing, um die Sitzungssicherheit bei Anfragen an einen LDAP-Server zu gewährleisten.	Das Signieren bestätigt die Integrität der LDAP-Nutzlastdaten mithilfe der Geheimschlüsseltechnologie. Das Sealing verschlüsselt die LDAP-Nutzlastdaten, um das Übertragen sensibler Informationen als unverschlüsselten Text zu vermeiden.
Ed25519- und NIST-Kurven in SSH (aktualisierte Algorithmen und Hash-basierte Methodenauthentifizierungscodes [HMACs])	ONTAP 9 bietet aktualisierte SSH-Chiffren und Schlüsselaustausch, einschließlich AES, 3DES, SHA-256 und SHA-512.	Die Bedrohungslandschaft entwickelt sich stetig weiter und die Stärke des Protokollalgorithmus, der Chiffren und des Schlüsselaustauschs ist entscheidend für die Integrität der Protokoll- und Produktfunktion.
Möglichkeit der Konfiguration der maximalen Anzahl nicht erfolgreicher SSH-Anmeldeversuche	ONTAP 9 bietet im Befehl „security ssh modify“ den Parameter „max-authentication-retry-count“, mit dem die maximale Anzahl von Anmeldeversuchen festgelegt werden kann. Das standardmäßige Maximum pro SSH-Verbindung liegt bei sechs, NetApp empfiehlt jedoch einen Wert von drei als Sicherheits-Best-Practice.	Diese Funktion unterstützt den Schutz vor „Brute Force“-Angriffen.
Multi-Faktor-Authentifizierung (MFA)	MFA ist für NetApp ONTAP System Manager und NetApp Active IQ Unified Manager für administrativen Web-Zugriff über Security Assertion Markup Language (SAML) und über externe Identitätsanbieter aktiviert. Administrativer Zugriff auf ONTAP über die Befehlszeile ist über lokale Zwei-Faktor-Authentifizierungsmethoden aktiviert. Die beiden Faktoren sind dabei Benutzerkennung/Passwort und ein öffentlicher Schlüssel. Sie können nsswitch mit öffentlichem Schlüssel als einen der beiden Faktoren für administrativen Zugriff über die SSH-Befehlszeile verwenden.	Schwache Anmeldedaten für administrativen Zugriff sind für die meisten Systemkompromittierungen verantwortlich. MFA macht es unmöglich, mit einfachen passwortbasierten Konten administrativen Zugriff zu erlangen.

Software oder Funktionen	Funktion	Auswirkungen
NetApp SnapLock Technologien mit NSE und NVE	ONTAP 9 unterstützt NSE und NVE mit der SnapLock Funktion, die Administration und Storage für WORM-Daten (Write Once, Read Many) bietet.	Die SnapLock Technologie erstellt dedizierte Volumes, in denen Dateien gespeichert und in einen schreib- und löschgeschützten Zustand versetzt werden können. SnapLock kann diesen Zustand unendlich lange oder für einen festgelegten Aufbewahrungszeitraum beibehalten, während die Sicherheit (Verschlüsselung) der NSE und NVE Lösungen gewahrt bleibt.
Validierung von Upgrade Images	Bei Upgrades für ONTAP wird bei der Durchführung überprüft, ob es sich um ein echtes ONTAP Image handelt.	Diese Validierung erkennt beschädigte oder gefälschte Images, wenn sie als Teil des Upgrade-Prozesses verwendet werden.
Unified Extensible Firmware Interface (UEFI) Secure Boot	Das Image wird bei jedem Systemneustart validiert.	Signierte ONTAP Images werden vom Boot-Loader überprüft, damit bei jedem Booten die Verwendung eines gefälschten Image verhindert wird.
Cluster-Peer-Verschlüsselung	Die Cluster-Peer-Verschlüsselung verwendet TLS 1.2 für die Verschlüsselung aller nicht über das Netzwerk zwischen Cluster Peers übertragenen Daten und die zugrunde liegenden ONTAP Funktionen, die Cluster Peering für die Datenreplizierung verwenden (NetApp SnapMirror, SnapVault, FlexCache).	Die Verschlüsselung von übertragenen Daten ist für ONTAP Funktionen verfügbar, die Daten replizieren. Außerdem können Unternehmen, die die Verschlüsselung von Daten im Ruhezustand (NVE/NSE) verwenden, die End-to-End-Verschlüsselung zwischen ONTAP Clustern mit Cluster-Peer-Verschlüsselung nutzen.
Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)	Die rollenbasierte Zugriffssteuerung in ONTAP gibt Administratoren die Möglichkeit, den administrativen Zugriff der Benutzer auf das Niveau zu beschränken, das für ihre Rolle festgelegt wurde. Mit dieser Funktion können Administratoren Benutzer anhand der ihnen zugewiesenen Rolle managen.	Zugriffssteuerung ist ein wesentliches Element für die Sicherheit. Funktionen wie die rollenbasierte Zugriffssteuerung bieten Ihrem Unternehmen die Möglichkeit, festzulegen, wer in welchem Umfang Datenzugriff erhält. Diese Funktion dämmt Schwachstellen und Exploit-Möglichkeiten ein, einschließlich Datenexfiltration und Eskalation von Berechtigungen.
Antivirus Connector (Virus-Scan)	Der Virus-Scan wird auf Vscan-Servern durchgeführt, die den Antivirus Connector und Virenschutzsoftware ausführen. In der Regel ist das System, das ONTAP ausführt, so konfiguriert, dass es Dateien scannt, wenn sie verändert wurden oder wenn ein Client darauf zugegriffen hat.	Bedrohungs- und Angriffsvektoren nehmen weiter zu. Daher schützt ein Inline-Virus-Scan von aufgerufenen oder geänderten Dateien die Integrität der Dateien Ihres Unternehmens.
Banner für Anmeldung und „Message of the Day“ (MOTD)	Anmeldebanner werden vor der Authentifizierung in der Ausgabe dargestellt. Diese Banner ermöglichen Ihrem Unternehmen und seinen Administratoren, mit den Systembenutzern zu kommunizieren.	Mithilfe von Anmeldebannern kann Ihr Unternehmen Bedienern, Administratoren und auch Benutzern mit eingeschränkten Berechtigungen die Bedingungen für eine akzeptable Nutzung eines Systems anzeigen. Diese Banner zeigen auch an, wer die Erlaubnis hat, auf das System zuzugreifen.
Festplattenbereinigung	Durch die Festplattenbereinigung können Sie Daten von einer Festplatte oder einer Reihe von Festplatten rückstandsfrei entfernen, sodass sie nie mehr wiederhergestellt werden können.	Sicherheitsprotokolle erfordern oft das irreparable Löschen von Daten von einer Festplatte. Die Funktion für die Festplattenbereinigung ermöglicht dies.
NetApp FPolicy Technologie	FPolicy ist eine Infrastrukturkomponente von ONTAP, mit der Partnerapplikationen Dateizugriffsberechtigungen überwachen und festlegen können. Dateirichtlinien können auf dem Dateityp basieren. FPolicy legt fest, wie das Storage-System Anfragen von einzelnen Client-Systemen für Vorgänge wie Erstellen, Öffnen, Umbenennen und Löschen verarbeitet. **Hinweis:** In ONTAP 9 wird das FPolicy Dateizugriffs-Benachrichtigungs-Framework durch Filterkontrollen und Ausfallsicherheit bei kurzen Netzwerkausfällen verbessert.	Die Zugriffssteuerung spielt eine wichtige Rolle bei der Sicherheit. Daher sind Sichtbarkeit und die Möglichkeit, auf Dateizugriff und Dateivorgänge zu reagieren, entscheidend, um die Sicherheit zu gewährleisten. Um Sichtbarkeit und Zugriffssteuerung zu ermöglichen, verwendet die ONTAP Lösung die FPolicy Funktion.

Tabelle 1) Sicherheitsfunktionen

Über NetApp

NetApp ist die Instanz für Daten in der Hybrid Cloud. Mit einem Portfolio an Hybrid Cloud Data Services, die das Management von Applikationen und Daten über Cloud- und On-Premises-Umgebungen hinweg vereinfachen, beschleunigt NetApp die digitale Transformation.

Gemeinsam mit Partnern hilft NetApp Unternehmen weltweit, das volle Potenzial ihrer Daten auszuschöpfen und damit ihren Kundenkontakt zu erweitern, Innovationen zu fördern und den Betrieb zu optimieren. Weitere Informationen finden Sie unter www.netapp.de. #DataDriven