

# NETAPP RANSOMWARE RESILIENCE

Erkennen Sie Ransomware-Angriffe in Echtzeit, verhindern Sie Datenverluste, stellen Sie die Daten schnell wieder her und minimieren Sie die Auswirkungen auf Ihr Unternehmen

## DAS PROBLEM

Ein entscheidender Aspekt bei der Vorbereitung auf einen Ransomware-Angriff besteht darin, geeignete Schutzmaßnahmen für Workload-Daten zu treffen und damit als letzte Instanz eine funktionierende Abwehr gegen Angreifer aufzubauen. Da die Angriffe immer ausgefeilter, automatisierter und kostspieliger werden, ist es unrealistisch, einen Ransomware-Angriff vollständig verhindern zu können. Sie müssen sich darauf einstellen, dass ein Angreifer in Ihr System eindringen könnte, und darauf vorbereitet sein.

Backups allein reichen nicht. Sie müssen außerdem in der Lage sein, das Risiko für Ihre kritischen Workload-Daten abzuschätzen, Bedrohungen zu erkennen und in Echtzeit darauf zu reagieren. Zusätzlich benötigen Sie Wiederherstellungspläne, die schnell und einfach ausführbar sind. Die Einrichtung eines wirksamen Schutzes gegen Ransomware-Angriffe stellt allerdings eine erhebliche Belastung für den Betrieb dar, wenn viele fehleranfällige manuelle Aufgaben ausgeführt werden müssen und zu wenig Personal über das nötige Fachwissen verfügt.

## DIE LÖSUNG

Mit dem NetApp Ransomware Resilience Service können Sie Ihr gesamtes Schutzprogramm schnell und einfach ausführen, von der Prävention über die Erkennung und Reaktion bis hin zur Wiederherstellung Ihrer Daten und Systeme.

Der Ransomware Resilience Service stellt eine zentrale Oberfläche zur intelligenten Orchestrierung Ihrer Workload-zentrierten Ransomware-Abwehr bereit. Mit wenigen Klicks können Sie Ihre schützenswerten Daten aus kritischen Workloads identifizieren und schützen. Automatisierung erkennt präzise potenzielle Angriffe, reagiert unmittelbar und begrenzt so die Auswirkungen. Und Sie können Ihre Workloads innerhalb von Minuten malwarefrei wiederherstellen. Damit schützen Sie Ihre wertvollen Daten und begrenzen Schäden sowie die Kosten von Geschäftsunterbrechungen auf ein Minimum.

## 7 Gründe, warum der Schutz und die Recovery von Workloads mit NetApp Ransomware Resilience noch effizienter, einfacher und schneller gelingt



1

**Weniger Zeit und Ressourcen:** Automatisieren Sie komplexe und zeitintensive manuelle Aufgaben.



2

**Höhere Konsistenz und Genauigkeit:** Vermeiden Sie Fehler mit automatisierten und geführten Maßnahmen.



3

**Frühzeitige Bedrohungserkennung:** Profitieren Sie von automatischer Überwachung und Warnung bei Anomalien im Datei- und Benutzerverhalten.



4

**Sofortige Reaktion:** Reagieren Sie sofort auf potenzielle Angriffe und begrenzen Sie Datenverluste. Integration in die gängigsten SIEM-Lösungen.



5

**Schnellere und einfachere Recovery:** Stellen Sie ganze Workloads schnell und malwarefrei wieder her und minimieren Sie so Geschäftsunterbrechungen, Kosten, Umsatzeinbußen und Image-Schäden.



6

**Geringere Ausgaben:** Optimieren Sie den ROI, indem Sie die Schutzrichtlinien anhand der Vertraulichkeit und Kritikalität der Workload-Daten festlegen.



7

**Höhere Effizienz:** Beschleunigen und verbessern Sie die Entscheidungsfindung und Maßnahmen mit dem Einsatz von KI.



**Der NetApp Ransomware Resilience Service berücksichtigt in seinen Maßnahmen alle sechs Komponenten, die im National Institute of Standards and Technology (NIST) Cybersecurity Frameworks abgedeckt sind: erfassen, sichern, erkennen, reagieren, wiederherstellen und verwalten.**

### Der richtige Umgang mit dem Risiko eines Ransomware-Angriffs

Identifizieren	Automatische Erfassung von Workloads und den zugehörigen Daten im NetApp Storage, Zuordnung der Daten zu Workloads und Ermittlung der Sensibilität, Kritikalität und des Risikos der Workload-Daten
Sichern	Empfehlungen für Workload-Schutzrichtlinien und deren Anwendung mit einem Klick
Erkennen	Echtzeit-Erkennung verdächtiger Anomalien im Datei- und Benutzerverhalten, die typischerweise auf einen Angriff hindeuten, und von Frühindikatoren für eine Kompromittierung (IoC), die auf einen potenziellen Versuch zur Datenexfiltration deuten.
Reagieren	Schutz der Workloads durch automatische Erstellung von Snapshot Kopien und Sperre der Anwender, wenn ein potenzieller Angriff vermutet wird. Der Service lässt sich außerdem in branchenführende Lösungen für Security Information and Event Management (SIEM) integrieren.
Wiederherstellen	Schnelle Wiederherstellung von Workloads und der zugehörigen Daten in einem einfachen, orchestrierten Recovery-Vorgang. Durch Nutzung der isolierten Recovery-Umgebung werden Ihre Daten sauber und malwarefrei wiederhergestellt.
Verwalten	Implementierung Ihrer eigenen Strategien und Richtlinien zum Schutz vor Ransomware und Überwachung der Ergebnisse

### Der NetApp Ansatz

## NetApp hat den sichersten Storage der Welt

### Umfassend

- Intelligentes Zusammenspiel der leistungsstarken, branchenführenden Cyberresilienz-Funktionen von NetApp ONTAP & den NetApp Data Services.
- Umfassender Schutz gegen Ransomware für Ihre Daten direkt auf der Ebene des Speichersystems. Geht über einfaches Backup hinaus und deckt alle sechs Komponenten des NIST-Frameworks für Cybersicherheit ab.
- Branchenführender Storage mit Ransomware-Schutz aus einer Hand.

### Benutzerfreundlich

- Automatische Identifizierung von Workloads; Vertraulichkeits-, Kritikalitäts- und Risikoanalysen; priorisierte, intelligente Empfehlungen für Schutzrichtlinien
- Automatische und geführte Maßnahmen für Schutz und Recovery von Daten-Workloads ohne Erfordernis spezieller Fähigkeiten oder zeitintensiver manueller Aufgaben
- Erfordert keine komplexen Konfigurationen, Optimierungen oder Integrationen

### Schnell

- Fortschrittliche KI zur Früherkennung und Reaktion auf potenzielle Angriffe
- Stellt komplette Workloads mit nur wenigen Klicks applikationskonsistent und schnell wieder her und minimiert so kostspielige Ausfallzeiten. Datenwiederherstellung optional granular nach Volume oder Datei.

**Erkennen Sie Ransomware-Angriffe in Echtzeit, verhindern Sie Datenverluste, stellen Sie die Daten schnell wieder her und minimieren Sie die Auswirkungen auf Ihr Unternehmen.**

### Weitere Ressourcen

**Testen Sie NetApp Ransomware Resilience gleich aus »**

Dieses Dokument wurde teilweise maschinell übersetzt und dient lediglich als Referenz. Im Zweifelsfall gilt die englische Version.



Kontakt

### Über NetApp

NetApp ist der Partner für intelligente Dateninfrastruktur. Mit Unified Storage sowie integrierten Data-, Management- und Workload-Services von NetApp minimieren Kunden Ineffizienzen und nutzen Umbrüche im Markt als Chance. Ergänzt um daten- und KI-basierte Analyse schaffen wir volle Transparenz über die gesamte Systemlandschaft und ermöglichen dadurch optimales Datenmanagement. Mit dem einzigen universalen Storage-Service auf Enterprise-Niveau in den führenden Public Clouds ist die Flexibilität von NetApp Lösungen unübertroffen: Unsere Data Services liefern starke Cyberresilienz, umfassende Governance und agile Applikationen; unsere Management- und Workload-Services optimieren fortlaufend die Performance und Ressourceneffizienz mit Hilfe künstlicher Intelligenz und telemetrischer Analyse. Egal welche Daten, Workloads und Umgebungen – NetApp transformiert Dateninfrastrukturen, damit Unternehmen ihr maximales Geschäftspotenzial ausschöpfen. [www.netapp.com](http://www.netapp.com)



© 2025 NetApp. Alle Rechte vorbehalten. NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> genannten Produktbezeichnungen sind Marken oder eingetragene Marken von NetApp Inc. in den USA und/oder in anderen Ländern. Alle anderen Marken- und Produktbezeichnungen sind möglicherweise Marken oder eingetragene Marken der jeweiligen Rechtsinhaber und werden hiermit anerkannt. NA-1087-0925-deDE