

NETAPP RANSOMWARE RESILIENCE



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

Sind Sie auf einen Ransomware-Angriff vorbereitet?

Ein entscheidender Aspekt der Vorbereitung auf einen Ransomware-Angriff ist der Schutz Ihrer Workload-Daten auf der Speicherebene – der letzten Verteidigungslinie. Da die Angriffe immer ausgefeilter, automatisierter und kostspieliger werden, ist es unrealistisch, einen Ransomware-Angriff zu verhindern. Sie müssen bereit sein, wenn Angreifer eindringen.

Backups allein reichen nicht aus. Sie müssen vielmehr in der Lage sein, das Risiko für Ihre kritischen Workload-Daten abzuschätzen, Bedrohungen zu erkennen und in Echtzeit darauf zu reagieren. Sie benötigen außerdem Wiederherstellungspläne, die schnell und einfach ausgeführt werden können. Die Erzielung wirksamer Resilienz gegen Ransomware-Angriffe ist allerdings eine erhebliche Belastung für den Betrieb, wenn viele fehleranfällige manuelle Aufgaben ausgeführt werden müssen und zu wenig Personal über das nötige Fachwissen verfügt.

Ohne ein geeignetes Schutzprogramm bleiben Angriffe auf Ihre Workloads lange unentdeckt und Sie reagieren erst spät. Die Wiederherstellung der Workloads wird dann komplex und durchschnittlich 7 Tage dauern¹ – und Ihre Daten können möglicherweise nicht einmal vollständig wiederhergestellt werden. Das ist nicht ausreichend und nicht rechtzeitig genug.

Umfassender Schutz für Ihre Daten direkt auf Storage-Ebene

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

Der Ransomware Resilience Service stellt eine zentrale Oberfläche zur intelligenten Orchestrierung Ihrer Workload-zentrierten Ransomware-Abwehr bereit. Mit wenigen Klicks können Sie gefährdete kritische Workload-Daten identifizieren und schützen. Der Dienst erkennt außerdem potenzielle Angriffe präzise und automatisch, reagiert darauf und begrenzt deren Auswirkungen. Und Sie können Workloads innerhalb von Minuten ohne Malware wiederherstellen, Ihre wertvollen Daten schützen und Schäden sowie die Kosten von Geschäftsunterbrechungen minimieren.

Ransomware Resilience vereint die leistungsstarken Funktionen der NetApp ONTAP® Software mit NetApp Data Services und ergänzt sie mit intelligenten Empfehlungen und Anleitungen sowie automatisierten Workflows zum:

- Identifizieren.** Identifizieren Sie automatisch Workloads (VMs, Dateifreigaben, gängige Datenbanken) und deren Daten in Ihrem NetApp Storage, ordnen Sie Daten den Workloads zu und bestimmen Sie die Sensibilität, Wichtigkeit und das Risiko der Daten.
- Schützen.** Erhalten Sie Empfehlungen für Workload-Schutzrichtlinien und wenden Sie diese mit einem Klick an.
- Erkennen.** Erkennen Sie verdächtige Datei- und Benutzeraktivitäten in Echtzeit, die auf potenzielle Datenexfiltrationsversuche sowie Dateiverschlüsselungs- und Massenlöschanträge hinweisen könnten.
- Reagieren.** Schützen Sie Workloads, indem Sie automatisch NetApp Snapshot™-Kopien erstellen und Benutzer blockieren, wenn ein potenzieller Angriff vermutet wird. Der Service lässt sich außerdem in branchenführende Lösungen für Security Information and Event Management (SIEM) integrieren.
- Wiederherstellen.** Stellen Sie Workloads und die zugehörigen Daten mithilfe eines einfachen, orchestrierten Wiederherstellungsprozesses schnell wieder her. Durch Nutzung der isolierten Recovery-Umgebung werden Ihre Daten sauber und malwarefrei wiederhergestellt.
- Verwalten.** Sie können Ihre eigenen Strategien und Richtlinien zum Schutz vor Ransomware implementieren und die Ergebnisse überwachen.

Bereiten Sie sich auf einen Angriff vor: Sparen Sie Zeit und verbessern Sie die Effektivität

Ransomware Resilience identifiziert automatisch die Datentypen in Ihrem NetApp Storage, ordnet die Daten bestimmten Workloads zu, bewertet die Sensibilität und Kritikalität der Daten und analysiert das Risiko. Dieser Prozess reduziert Ihre Abhängigkeit von komplizierten manuellen Analysen, zusätzlichen Tools von Drittanbietern und speziellem Fachwissen.

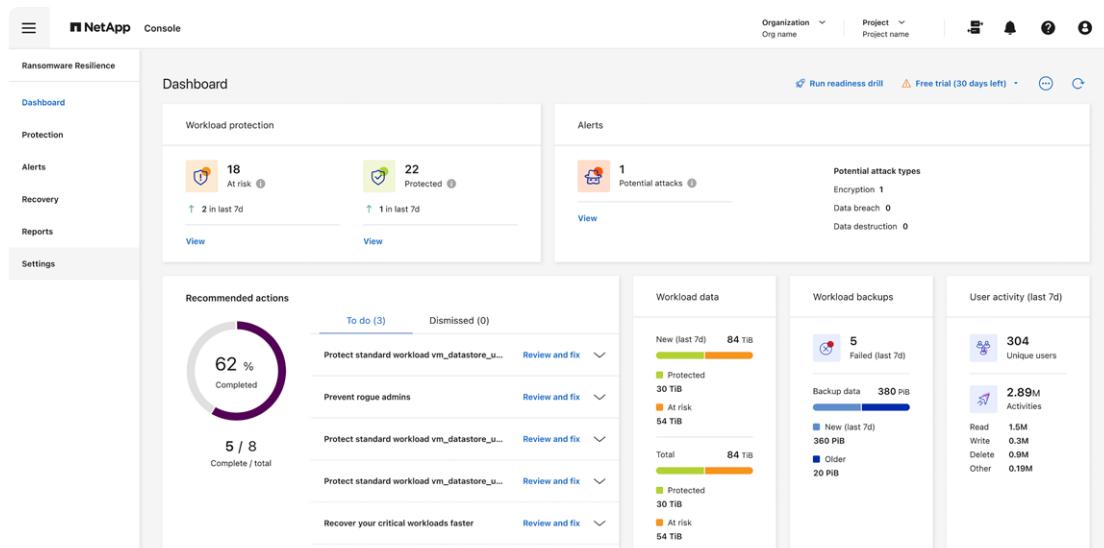


Abbildung 1: Der NetApp Ransomware Resilience Service bietet umfassenden, orchestrierten, Workload-zentrierten Ransomware-Schutz von der Erkennung bis zur Wiederherstellung über eine einzige Managementplattform.

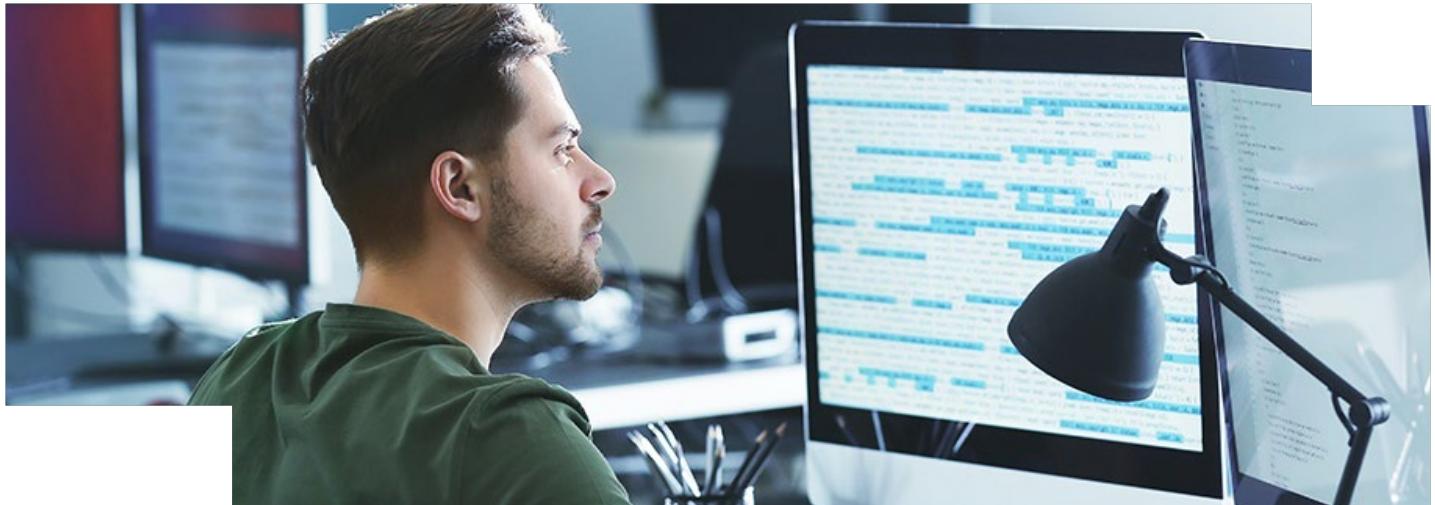
WESENTLICHE VORTEILE

Umfassender orchestrierter Schutz für Ihre Daten auf Ebene des Speichersystems

- Verschaffen Sie sich einen vollständigen Überblick über den Schutzstatus Ihrer Workloads.
- Erkennen Sie einen Angriff frühzeitig und verhindern Sie Datenverlust.
- Stellen Sie ganze Workloads schnell und Malware-frei wieder her, um Störungen, Kosten, Umsatzeinbußen und Geschäftsschäden zu minimieren.
- Erhalten Sie Daten für forensische Analysen und Empfehlungen zur Verbesserung Ihres Sicherheitsstatus.

Ransomware Resilience schlägt dann intelligente Schutzrichtlinien unter Verwendung von ONTAP Funktionen vor, darunter Anomalieerkennung über NetApp Autonomous Ransomware Protection mit AI (ARP/AI), Blockierung bösartiger FPolicy-Erweiterungen und manipulationssichere Snapshot-Kopien. Ransomware Resilience passt außerdem Schutzempfehlungen an die Sensibilität und Kritikalität Ihrer Datenbestände an.

Schutzrichtlinien werden mit nur einem Klick nahtlos und konsistent auf alle Workload-Daten angewendet. Ransomware Resilience arbeitet im Hintergrund, um die Funktionen von ONTAP und NetApp Data Services zu konfigurieren und Schutz-Workflows für jedes Datenvolumen zu orchestrieren, wodurch der Bedarf an sich wiederholenden manuellen Aufgaben reduziert wird.



Erkennen und reagieren Sie auf Bedrohungen in Echtzeit

Ransomware Resilience überwacht kontinuierlich verdächtige Dateien und Anomalien im Benutzerverhalten. Es kann Datenlecks erkennen, indem es frühzeitig Benutzerverhalten identifiziert, das auf einen möglichen Versuch der Datenexfiltration oder Dateiverschlüsselung und Massenlöschung hindeuten könnte. Bei Verdacht auf einen Angriff erstellt Ransomware Resilience eine Snapshot-Kopie, um Datenverlust zu verhindern. Außerdem aktiviert es die Blockierung des Benutzers, der den Angriff ausführt, um ihn zu stoppen und weitere Angriffe zu verhindern.

Dieser Dienst verwendet eine innovative, fortschrittliche KI-basierte Ransomware-Erkennung auf Ihrem primären Speicher. Durch diesen Ansatz können potenzielle Angriffe schnell erkannt und sofort abgewehrt werden.

Ransomware Resilience bietet Vorfallberichte zur Unterstützung der Forensik und lässt sich in die branchenführenden SIEM-Lösungen integrieren.

Einfache Wiederherstellung von Workloads innerhalb weniger Minuten

Ransomware Resilience orchestriert den Workflow für eine anwendungskonsistente Wiederherstellung aller zugehörigen Workload-Daten und bietet Ihnen Einblick in den Prozess und Status in Echtzeit. Snapshot-Kopien können auf Workload-Ebene oder granularer auf Volume- oder Dateiebene wiederhergestellt werden.

Als Teil des Wiederherstellungsprozesses bietet Ransomware Resilience eine isolierte Wiederherstellungsumgebung, die infizierte Workloads isoliert, Malware entfernt, einen Wiederherstellungspunkt empfiehlt und den Benutzer durch einen intuitiven Wiederherstellungsprozess führt. Dieser Ansatz ermöglicht eine saubere, malwarefreie Wiederherstellung und verhindert eine erneute Infektion Ihrer Daten.

Minimierung von Geschäftsunterbrechungen

Ransomware Resilience nimmt Ihnen die Last und Sorge ab, Ihre Workloads vor Ransomware-bedingten Ausfallzeiten und Datenverlusten zu schützen. Es bietet einen umfassenden Service, der Ihre Bereitschaft verbessert, auf Angriffe reagiert und Sie durch die Wiederherstellung führt. Mit NetApp können Sie darauf vertrauen, dass Sie im Falle eines Angriffs sofort alarmiert werden, Ihre wertvollen Workload-Daten geschützt sind, die Wiederherstellung schnell und einfach verläuft und die Unterbrechung Ihrer geschäftlichen Tätigkeit so minimal wie möglich ausfällt.

Testen Sie NetApp Ransomware Resilience gleich aus

¹ ESG, [2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](#), November 2023.

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



Kontakt

Über NetApp

NetApp ist das Unternehmen für intelligente Dateninfrastrukturen, das einheitliche Datenspeicherung, integrierte Daten sowie Betriebs- und Workload-Services kombiniert, um eine Welt voller Umbrüche für jeden Kunden in Chancen zu verwandeln. Ergänzt um daten- und KI-basierte Analyse schaffen wir volle Transparenz über die gesamte Systemlandschaft und ermöglichen dadurch optimales Datenmanagement. Mit dem einzigen nativen 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 Betriebs- und Workload-Services bieten eine kontinuierliche Optimierung der Leistung und Effizienz von Infrastruktur und Workloads durch Beobachtbarkeit und KI. Egal welche Daten, Workloads und Umgebungen – NetApp transformiert Dateninfrastrukturen, damit Unternehmen ihr maximales Geschäftspotenzial ausschöpfen. Mehr erfahren unter www.netapp.com oder folgen Sie uns auf [X](#), [LinkedIn](#), [Facebook](#), und [Instagram](#).

