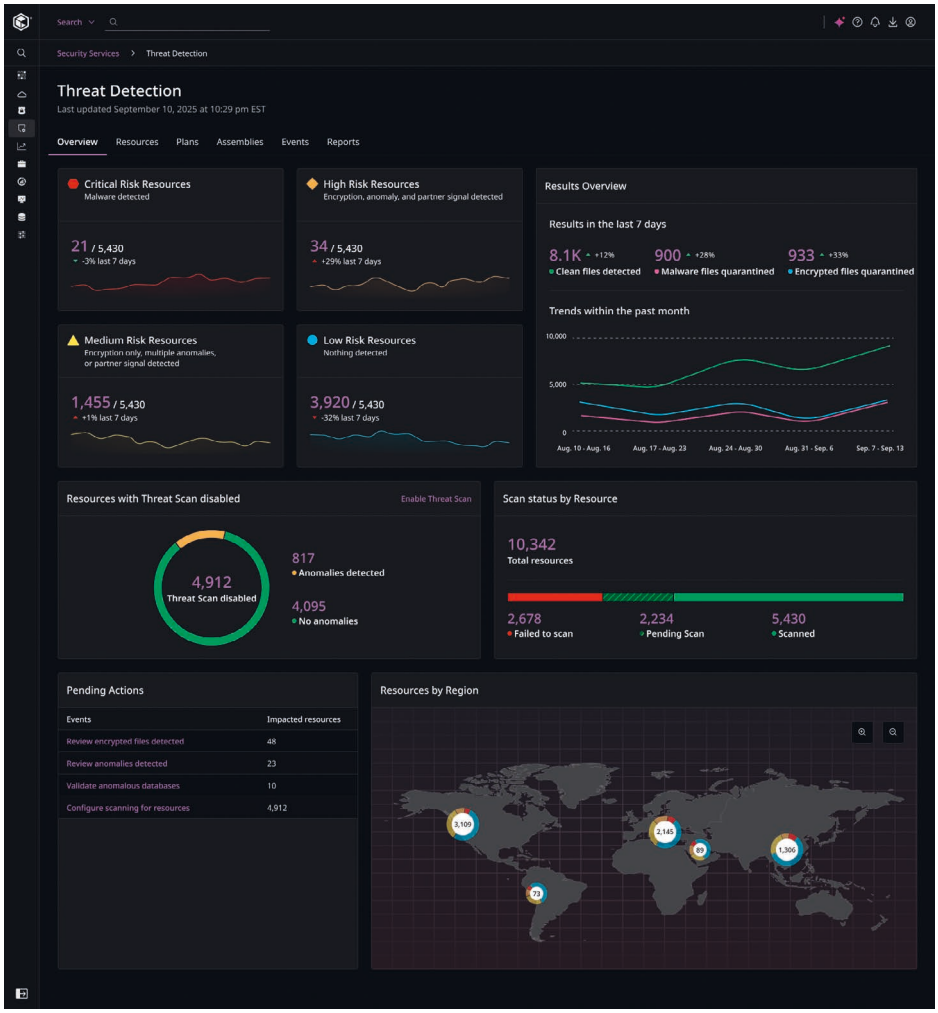
Cyberresilienz für sensible Daten

Wie Machine Learning und Künstliche Intelligenz Backup optimieren können



Angesichts von Cyberangriffen auf Backups ist eine Wiederherstellung sauberer Daten ein wichtiges Qualitätskriterium für ein Backup. Alle Bilder © Commvault

Autor:
Darren Thomson,
Vice President and Chief Technology Officer (Field) EMEAI
Commvault
www.commvault.com

Künstliche Intelligenz mit ihren neuen agentenbasierten Konzepten, höhere Anforderungen bei der Datensouveränität, Angriffe gegen Identitätssysteme: Disruptive Zeiten und Technologien wälzen auch Cyberresilienz, Datensicherheit und Backup um. Innovative Technologien, Ansätze und Bemessungsmethoden können in naher Zukunft eine neue Währung für Vertrauen in und durch Backup schaffen.

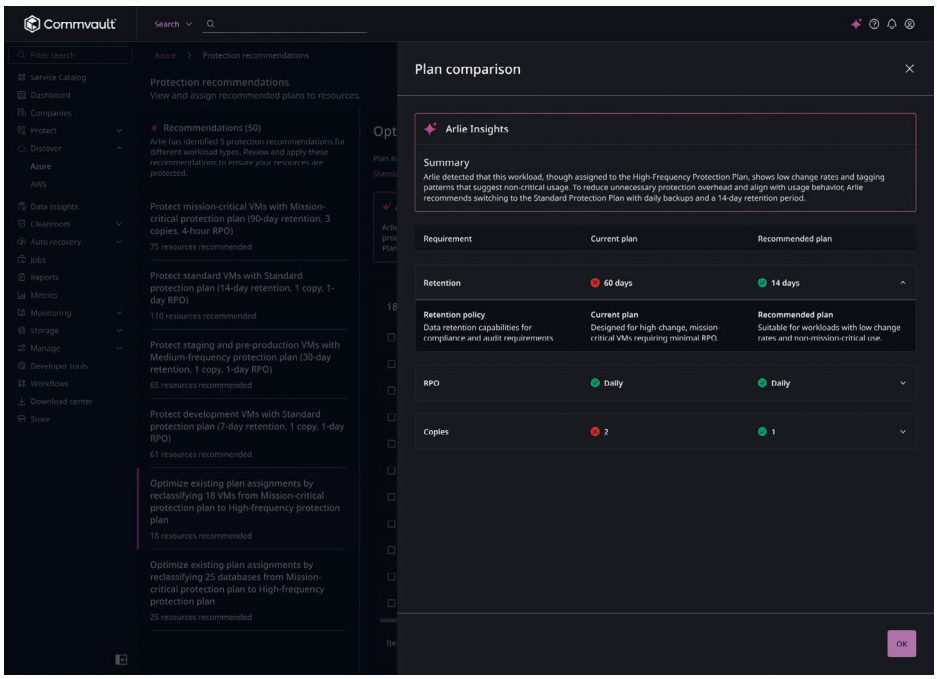
IT-Entscheider und Verantwortliche für Datensicherheit und IT-Betrieb stehen 2026 vor großen Herausforderungen, aber auch vor neuen Chancen. Die folgenden sechs Punkte helfen, die Verfügbarkeit von Daten, Systemen und Anwendungen im Alltag von KI und Cyberkriminalität aufrechtzuerhalten:

1. Vom Experiment zum Businessstandard

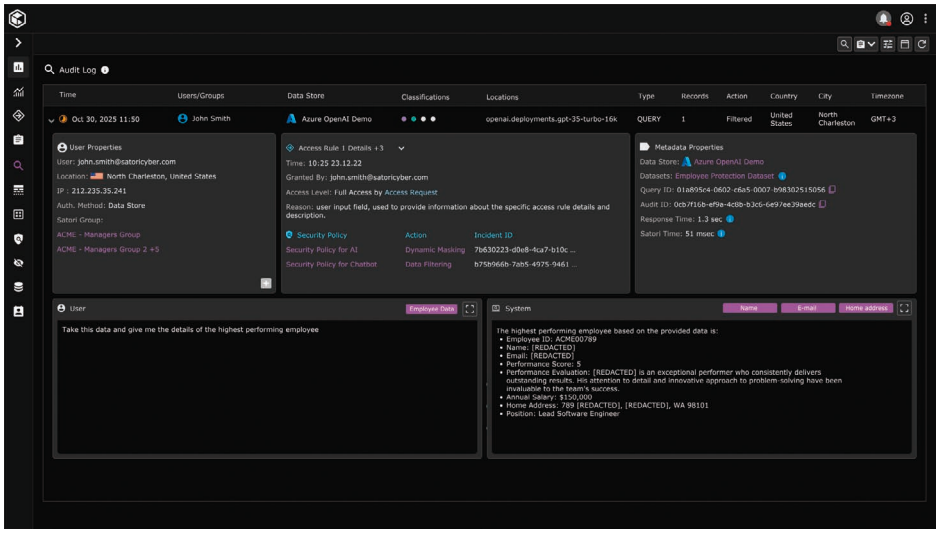
Die Integrität der KI und ihrer Daten wird essenziell für die Resilienz im Jahr 2026. Damit ist die Fähigkeit gemeint, die Ergebnisse in den Modellen des maschinellen Lernens nachzuverfolgen, zu überprüfen und Daten wiederherzustellen. Denn wenn die KI und die darunter liegenden Daten beschädigt sind, muss die Wiederherstellung über die Systeme hinausgehen und das Wissen selbst umfassen.

Intuitive Bedienung

KI hilft hierbei, denn inzwischen kann der User im KI-getriebenen Dialog die Cyberresilienz selbst stärken. Statt sich durch Dashboards und Skripte zu navigieren, können Teams ein-



Management von KI-Daten: Dashboards einer Cloud-Plattform liefern Informationen über KI-Daten und die jeweiligen Zugriffsrechte.



Mit digitalen Datenräumen können Unternehmen ihre vertrauenswürdigen Backup-Daten mit Plattformen für Künstliche Intelligenz oder internen Data Lakes verbinden.

fach - in natürlicher Sprache – Fragen stellen und Befehle erteilen, um ihre Workloads zu schützen, Richtlinien zu prüfen oder die Wiederherstellung ihrer Daten in SaaS-, Multi-Cloud- und Hybridumgebungen zu validieren. Die Innovation liegt nicht nur in der Automatisierung, sondern vor allem in der intuitiven Bedienung. User können ihre Resilienz einfach verwalten, indem sie der KI diese Aufgabe per Sprachbefehl mitgeben.

Sie können so operative Prozesse steuern und Maßnahmen zur Cyberabwehr und zum Schutz der Backups oder der zugehörigen Identitäten starten. Die KI wird ihren Mehrwert nicht nur ausspielen, indem sie Prozesse automatisiert, sondern den Usern erlauben, IT-Tools intuitiv zu bedienen.

2. Cloud-Souveränität als Flexibilitätsstrategie

Nicht nur dank der Richtlinien für Cyberresilienz wie NIS2 und dem EU Data Act hat das Thema Cloud-Souveränität an strategischem Gewicht gewonnen. So gehen die Analysten von Forrester davon aus, dass bis Ende nächsten Jahres die Hälfte der Unternehmen regionale Infrastrukturen priorisieren wird.

Digitale Souveränität bedeutet aber nicht Isolation, sondern Kontrolle und Wahlfreiheit. Angesichts verschiedener Clouds und Regionen benötigen die Unternehmen die Freiheit und Flexibilität, zu entscheiden, wo sie ihre Daten sichern – lokal, in einer Private Cloud, in einer lokalen Hyperscaler-Region oder in einer globalen Cloud.

Transparenz und Compliance

Gleichzeitig benötigen sie volle Transparenz über Zugriffsrechte und müssen diese grenzüberschreitend wiederherstellen können.

Die IT-Architekturen werden souveränitätsbewusst handeln und auf Verschlüsselung sowie Zugriffsrichtlinien über Grenzen und Clouds hinweg setzen, um die Compliance-Regeln für ihre Daten einzuhalten.

So wird Compliance als Folge digitaler Souveränität by Design 2026 zum Wettbewerbsvorteil werden. Denn die Kombination aus Souveränität und Wahlfreiheit erlaubt es Unternehmen, Daten und Workloads innerhalb vertrauenswürdiger Grenzen vorzuhalten.

3. Identität

Die unsichtbare Infrastruktur der Resilienz: Digitale Ökosysteme agieren zunehmend grenzübergreifend, weshalb die Identität in diesen offenen Infrastrukturen zum wichtigen Sicherheitsfaktor wird.

Jedes Privileg – gleich ob für Mensch oder Maschine – ist ein potenzielles Angriffsziel: Laut IDC werden Unternehmen daher Identitäten, Daten und Wiederherstellungsrichtlinien in einen Sicherheitsansatz vereinen: Recovery wird zur Vertrauensfrage.

Wer die Integrität der Identity-Systeme und der Nutzer-IDs verifizieren und diese wichtigen Daten wiederherstellen kann, wird die Resilienz seiner kritischen Workflows und Prozesse stärken. Dies wird noch mehr dort gelten, wo ausschließlich KI mit KI kommuniziert. Hier initiieren autonome Agenten Aktionen, teilen Daten und agieren selbstständig. KI-Systeme müssen wissen, mit wem sie interagieren, bevor sie handeln.

4. Datenräume

Geschützte Daten als vertrauenswürdige Basis der KI: Unternehmen werden erkennen, dass ihre KI-Initiativen nicht an fehlenden Daten scheitern, sondern an der Unfähigkeit, sicher auf vorhandene Daten zuzugreifen und diese aufzubereiten. Historische Daten sind bei verantwortungsvoller Nutzung nicht mehr nur eine Rückversicherung, sondern ein strategisches Informationsgut. Auf Unternehmenssouveränität ausgerichtete ausfallsichere Datenräume werden daher zum Erfolgsfaktor: Sie verbinden mit sicheren Umgebungen verwaltete Backup-Daten direkt mit KI-Plattformen und Data Lakes - ohne riskante, ad-hoc-ETL-Workflows. Informationen werden nun zu sauberen und KI-fähigen Daten. Sie sind klassifiziert, kompliant und ihre Herkunft ist bekannt.

5. Vertrauen wird zur Währung digitaler Infrastrukturen

Governance, Souveränität und Resilienz verschmelzen zu einem einzigen Auftrag: dem Nachweis von Vertrauenswürdigkeit. Vorstände und Führungsgremien werden von ihrer IT dafür Beweise verlangen: Klare Metriken für die Wiederherstellung, Audit-Trails und Validierungen in digitalen Reinräumen müssen zum Standard werden.

Diese Vertrauenswürdigkeit wird in der Zukunft zum Faktor der Wertschöpfung. Laut IDC wird bis 2030 die Hälfte des digitalen Werts in Europa von Unternehmen stammen, die KI verantwortungsvoll einsetzen und entsprechend skalieren.

Das Vertrauen darauf basiert auf drei Säulen:

- **Resilienz:** Gewährleistung der Integrität von KI und Datenpipelines
- **Souveränität:** Wahrung der rechtmäßigen Kontrolle über alle Datenflüsse; sowie
- **Quantenbereitschaft:** Schutz heutiger Informationen vor zukünftigen Bedrohungen etwa durch Postquanten-Computing-Attacken auf verschlüsselte Daten.

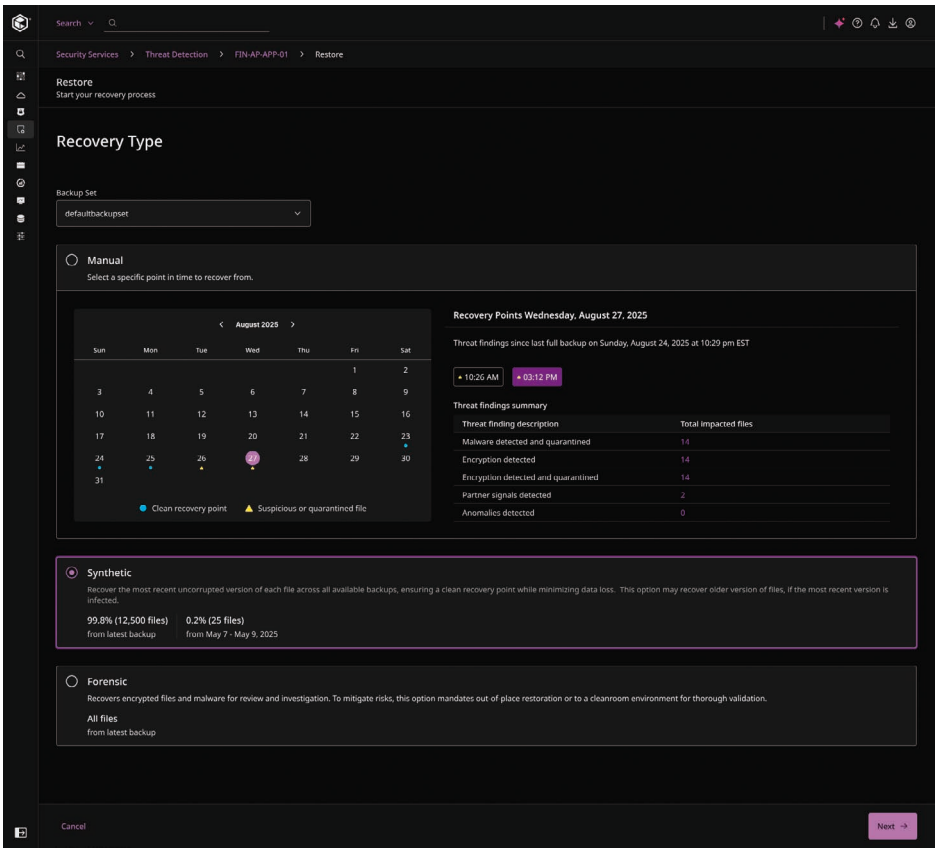
Die Architektur einer vertrauenswürdigen Autonomie bilden Systeme, die Entscheidungen treffen, sich erholen und zusammenarbeiten können, ohne die Kontrolle über ihre Integrität zu verlieren.

6. Neue Kennzahlen für Backup und Recovery

Wer Daten wiederherstellt, ohne deren Status zu untersuchen, erreicht vielleicht seine RTO- und RPO-Ziele. Eine saubere Wiederherstellung ist aber nicht garantiert. Außerdem könnte hierbei eine korrumpierte Datei wiederhergestellt werden, die Cyberkriminelle für einen erneuten Einbruch missbrauchen könnten. Ein herkömmlicher Ansatz führt also oft nur zu einem Teufelskreis aus sich wiederholenden Cybervorfällen und Ausfallzeiten.

Um dies zu vermeiden, sollten Teams Daten nicht sofort wiederherstellen, sondern Backups auf Integrität und Vertrauenswürdigkeit analysieren. Dieser zeit- und ressourcenintensive Vorgang kann aber selbst Tage und Wochen in Anspruch nehmen.

Angesichts von Cyberangriffen auf Backups ist eine Wiederherstellung sauberer Daten ein wichtiges Qualitätskriterium für ein Backup. Eine synthetische Recovery ermittelt automatisch den bestmöglichen Recovery Point in Time für eine Wiederherstellung möglichst aktueller und sauberer Daten.

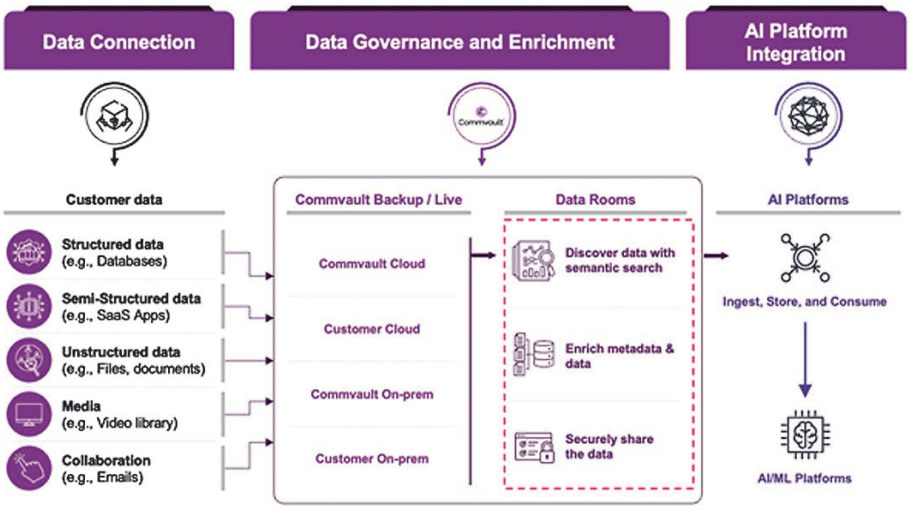


Künstliche Intelligenz unterstützt das Backupmanagement. Ein KI-Assistent bietet nicht nur ein Dialogfeld, sondern auch eine transparente Übersicht ihrer Tätigkeit.

Mean Time to Clean Recovery

Deshalb sind neue Kenngrößen für die Verfügbarkeit wie die Mean Time to Clean Recovery (MTCR) erforderlich: Gemeint ist die durchschnittlich notwendige Zeit, um nach einem Cyberangriff alle im Vorfeld als kritisch definierten Anwendungen sowie zugrundeliegende Systeme, Infrastrukturen und zugehörige saubere, validierte Daten wiederherzustellen.

Anhand dieses Parameters haben Führungskräfte eine neue Chance, Cyber-Recovery-Abläufe und die notwendige Vorabplanung neu zu gestalten. Sie können IT-Teams dazu bewegen, über die reine Recovery-Zeit hinauszudenken und stattdessen das Vertrauen in Daten, Systemintegrität und realistische Zeitpläne zu berücksichtigen. ◄



Eine wirksame Erkennung von Gefahren für Backups basiert auf KI.