Enterprise Strategy Group

WIRTSCHAFTLICHE VALIDIERUNG

Analyse der wirtschaftlichen Vorteile von Commvault Cleanroom Recovery und Cloud

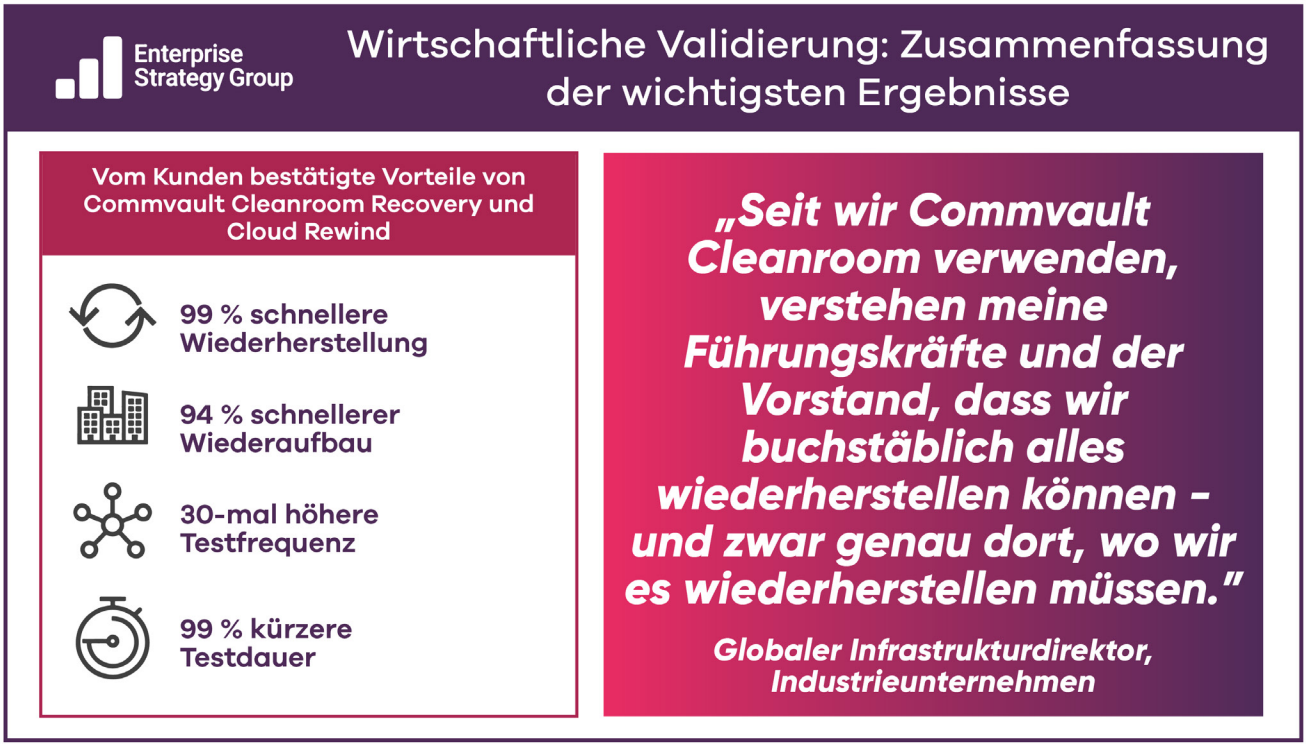
Modernisieren Sie Ihren Cyber-Wiederherstellungsplan und beschleunigen Sie Ihre Wiederherstellungsfähigkeit

Von Nathan McAfee, Principal Economic Validation Analyst
Enterprise Strategy Group
June 2025

Diese Economic Validation der Enterprise Strategy Group wurde im Auftrag von Commvault und Microsoft erstellt und wird unter Lizenz von TechTarget, Inc. veröffentlicht.

Commvault®

Inhalt



Einleitung

Diese Economic Validation von Enterprise Strategy Group konzentriert sich auf die quantitativen und qualitativen Vorteile, die Unternehmen durch die Einführung der Commvault Cleanroom Recovery- und Cloud Rewind-Technologien erwarten können.

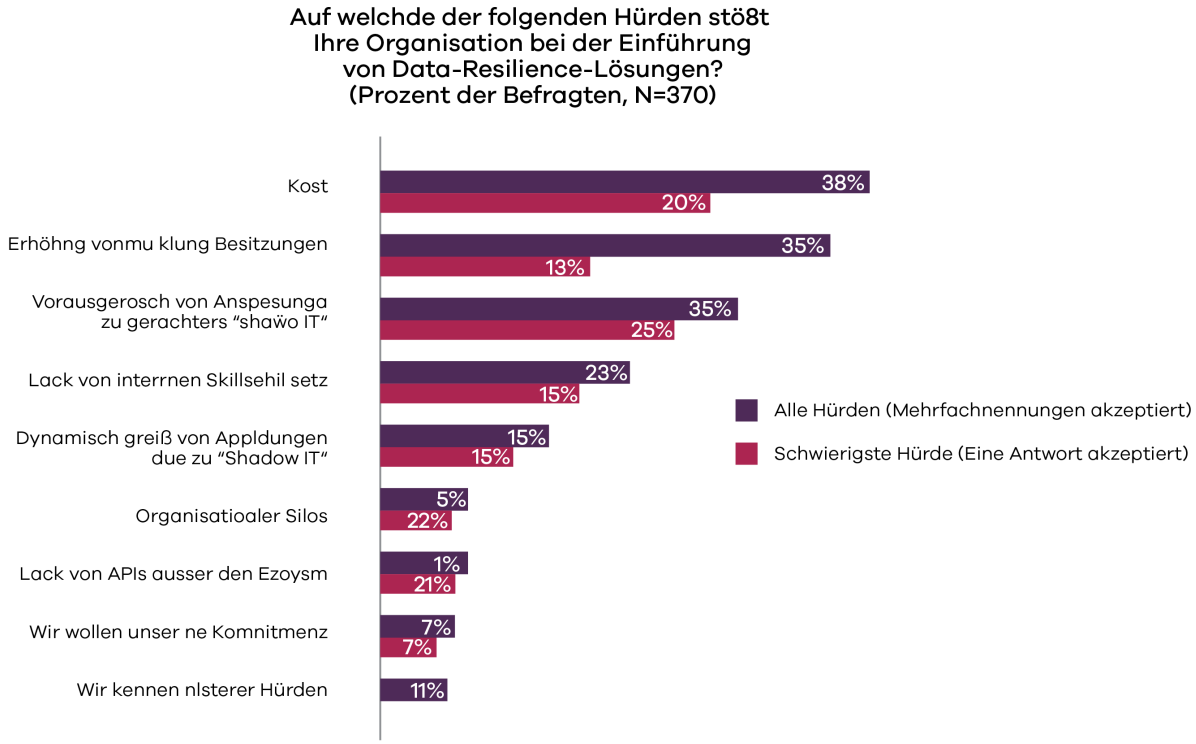
Die für diese Analyse befragten Kunden stammen aus verschiedenen globalen Branchen, darunter Energie, Gesundheitswesen, Fertigung, Bildung, Technologie, IT-Beratung, Finanzdienstleistungen, Einzelhandel und Regierung. Ihre jährlichen Umsätze liegen zwischen 2,4 Milliarden USD und 20,5 Milliarden USD. Obwohl jeder der Befragten einzigartige Anwendungsfälle für Commvault Cleanroom Recovery und Cloud Rewind hatte, stellten wir fest, dass die in unserem Finanzmodell dargestellten Vorteile auf Organisationen jeder Größe übertragbar sind, die analysiert wurden.

Herausforderungen

Die meisten erfahrenen IT-Fachleute kennen Geschichten über Wiederherstellungsvorfälle, bei denen Daten nicht in einen nutzbaren Zustand zurückversetzt werden konnten. Dies ist typischerweise das Ergebnis unzureichender Planung, mangelhafter Tools, fehlerhafter Implementierung oder Tests – oder eines allgemeinen Mangels an Fachwissen, um die Komplexität der heutigen hybriden IT-Umgebungen zu bewältigen. Die Forschung der Enterprise Strategy Group hat die größten Hürden identifiziert, mit denen Organisationen

bei der Datenausfallsicherheit konfrontiert sind, und diese als die wichtigsten Probleme herausgestellt (siehe Abbildung 1).[1]

Abbildung 1. Hindernisse bei der Einführung von Datenresilienzlösungen



Source: Enterprise Strategy Group, now part of Omdia

Im Rahmen unserer Analyse haben wir Kunden von Commvault Cleanroom und Cloud Rewind befragt, um einige der spezifischen Herausforderungen zu verstehen, mit denen sie in ihrer bisherigen Methodik und ihren Lösungen für Cyber-Resilienz konfrontiert waren. Diese waren in den meisten Interviews konsistent:

- **Fähigkeit zur vollständigen und konsistenten Wiederherstellung.** Die Möglichkeit, Daten zu sichern, ist weniger als die halbe Miete; die Fähigkeit, Daten und die zugehörige Infrastruktur effektiv wiederherzustellen, ist entscheidend, um die Auswirkungen eines Datenverlusts und Wiederherstellungsereignisses zu minimieren. Untersuchungen der Enterprise Strategy Group zeigten, dass nur 11 % der Befragten angaben, dass ihre Organisation regelmäßig in der Lage ist, alle Daten vollständig wiederherzustellen.[2]

- **Wiederherstellbarkeit des Plattformzustands.** Viele Organisationen bauen ihre Wiederherstellungspläne auf der Fähigkeit auf, Daten wiederherzustellen. Obwohl dies wichtig ist, ist es nur ein Teil der Lösung. Organisationen

[1] Source: Enterprise Strategy Group Research Report, Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance, September 2024.

[2] Source: Enterprise Strategy Group Research Report, Cloud Data Protection Strategies at a Crossroads, August 2023.

müssen außerdem in der Lage sein, das gesamte Ökosystem schnell wiederherzustellen – einschließlich Anwendungen, Treibern, Netzwerken und Verbindungen –, bevor die eigentliche Datenwiederherstellung überhaupt möglich wird. Darüber hinaus erfordern Abhängigkeiten beim Wiederaufbau der zugrunde liegenden Infrastruktur, dass die einzelnen Komponenten in einer bestimmten, schrittweisen Reihenfolge wiederhergestellt werden.

- **Komplexität und Kosten von Wiederherstellungstests.** Wiederherstellungspläne werden häufig erst dann vollständig getestet, wenn ein tatsächliches Wiederherstellungsereignis eintritt. Gespräche mit Kunden ergaben, dass nur wenige Unternehmen umfassende Wiederherstellungstests durchführen, während viele ihre Strategien auf jährliche Tests stützen, die nur einige ihrer geschäftskritischen Systeme abdecken. Diese Entscheidungen sind eine Folge der Kosten und Komplexität, die mit gründlichen Tests einer vollständigen Wiederherstellung verbunden sind, und führen dazu, dass Organisationen einem hohen Maß an selbstverschuldetem Risiko und potenzieller Gefährdung ausgesetzt sind.

- **Fehlende Möglichkeit, unerwünschte Wiederherstellungsänderungen rückgängig zu machen.** Für die meisten Organisationen ist es schwierig oder sogar unmöglich, Änderungen oder ineffektive Wiederherstellungsereignisse rückgängig zu machen. Solche Rücksetzungen können äußerst störend sein und führen häufig zu Datenverlusten und ungeplanten Ausfallzeiten.

- **Fähigkeit, Daten vor der Wiederherstellung zu prüfen und zu bereinigen.** Ein großes Problem bei der Wiederherstellung nach einem Ransomware-Angriff besteht darin, sicherzustellen, dass die Daten sauber sind, bevor sie wiederhergestellt werden. Herkömmliche Testumgebungen machen diese Aufgabe komplex, unsicher und oft unmöglich.

- **Wiederherstellbarkeit in isolierte Umgebungen.** Viele Organisationen sind darauf beschränkt, in dieselbe Umgebung wiederherzustellen, in der das Backup erstellt wurde, oder in eine andere Umgebung, die nicht zu 100 % als frei von potenziellen Infektionen verifiziert werden kann. In Fällen wie der Cyber-Wiederherstellung kann diese Umgebung beschädigt oder nicht verfügbar sein. Bei einer Cyber- oder Ransomware- Wiederherstellung benötigen Organisationen die Möglichkeit, in eine bedarfsgesteuerte, isolierte Umgebung wiederherzustellen, um sicherzustellen, dass die Daten sauber und frei von erneuter Infektion sind. Obwohl die meisten Organisationen Disaster Recovery (DR) und Cyber Recovery (CR) als denselben Prozess behandeln, scheitern sie oft katastrophal in einer Cyber-Recovery-Situation – mit karrierebeeinträchtigenden Folgen, wenn Ransomware zuschlägt.

- **Dedizierte Pläne für eine veränderte Bedrohungslandschaft.** Ein grundlegender Unterschied zwischen DR und CR besteht in der Anerkennung unterschiedlicher Bedrohungen. Traditionelle DR-Pläne decken die Komplexität eines Cyberangriffs, insbesondere von Ransomware, möglicherweise nicht ausreichend ab. Daher erfordert CR dedizierte Pläne, die sich auf die Wiederherstellung in eine isolierte und nachweislich saubere Umgebung konzentrieren.

- **Mangelnde Integration zwischen Datenresilienz- und Sicherheitsökosystemen.** Die von uns untersuchten Unternehmen stützten sich auf eine Vielzahl von Tools – viele davon mit über 15 verschiedenen Lösungen für DR und Cyberresilienz. Fehlende hochwertige APIs und mangelnde Interoperabilität führen zur Notwendigkeit dieser Vielzahl von Tools und verursachen hohe technische Schulden.

- **Prüfbarkeit und Verifizierung von Cyber-Wiederherstellungsplänen.** Die Enterprise Strategy Group stellte fest, dass die Prüfbarkeit von Wiederherstellungstests und -plänen für die untersuchten Organisationen eine Herausforderung darstellt. Diese Pläne sind entscheidend für die Unternehmensführung (einschließlich der Vorstände), erforderlich für bestimmte Compliance- und Regulierungsbehörden, notwendig zur Aufrechterhaltung von Geschäftsbeziehungen mit vielen Kunden und sogar, um die Kosten für Cyberversicherungen zu senken.

Die Bedeutung der Rückkehr zur Mindestfunktionsfähigkeit nach einem Cyberangriff

Die Auswirkungen von Ausfallzeiten können verheerend sein, und die Fähigkeit, nach einem Angriff oder einer Störung schnell wieder zu einem funktionsfähigen Betriebszustand zurückzukehren, ist entscheidend. Mindestfunktionsfähigkeit (Minimum Viability) bezeichnet die Fähigkeit, die minimal erforderlichen Funktionen (Anwendungen, Ressourcen, Prozesse, Personen) rasch und sauber wiederherzustellen, damit eine Organisation nach einem Angriff effektiv weiterarbeiten kann. Dies ist ein zentraler Bestandteil einer kontinuierlichen Geschäftspraxis. Eine Organisation muss Vertrauen in ihre Fähigkeit haben, schnell zu einem Zustand der Mindestfunktionsfähigkeit zurückzukehren, um die Unterbrechung des Geschäftsbetriebs zu minimieren – mit einem klar definierten Plan für die anschließende vollständige Wiederherstellung und verbesserte Resilienz.

Die Lösung: Commvault Cleanroom Recovery und Cloud Rewind

Um die Cyberresilienz zu stärken und die Wiederherstellung nach einem Sicherheitsvorfall oder Ransomware- Angriff zu beschleunigen, bietet Commvault Cleanroom Recovery an. Diese automatisierte, isolierte und sichere Cloud-Umgebung ermöglicht es Organisationen, Wiederherstellungsstrategien zu validieren und Bedrohungen mithilfe forensischer Analysen zu untersuchen. Zudem ermöglicht sie die schnelle Wiederherstellung von Betriebsumgebungen und trägt letztlich dazu bei, die Geschäftskontinuität während ungeplanter Ausfallzeiten, katastrophaler Ereignisse, Ransomware-Angriffe und anderer Bedrohungen aufrechtzuerhalten.

Commvault Cleanroom bietet folgende Funktionen:

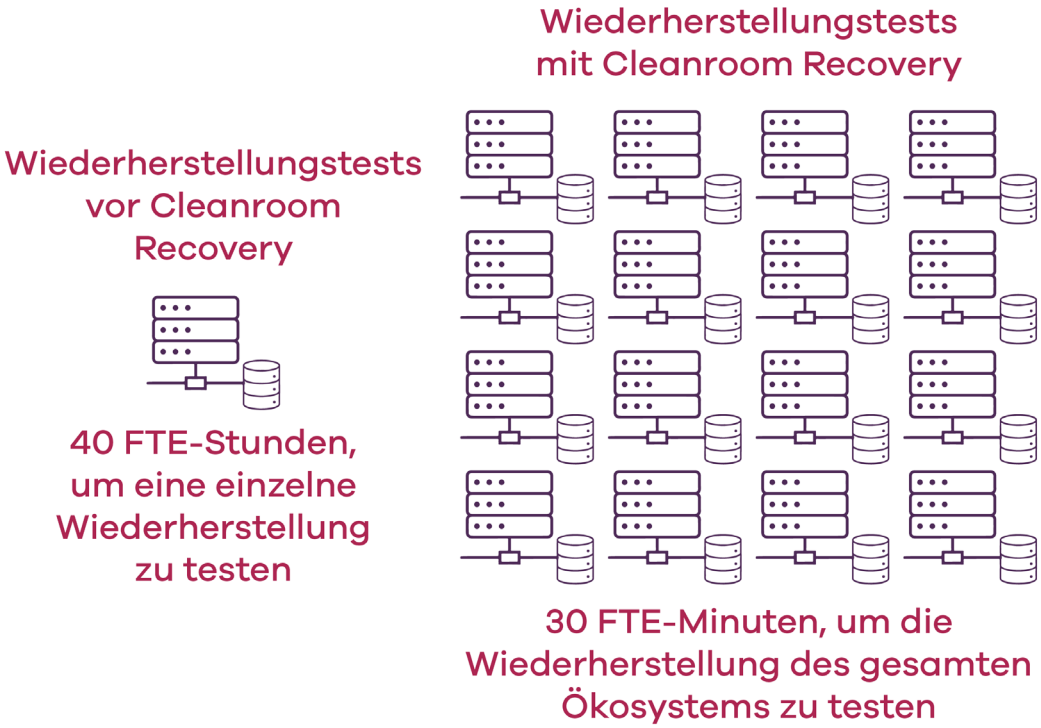
- **Aufbau eines effektiven Cyber- Wiederherstellungsplans**

Allzu oft führen Organisationen Wiederherstellungstests anhand einer Checkliste durch. Sie testen einen Teil des Wiederherstellungsprozesses nach dem anderen, bis alle Kästchen abgehakt sind. Doch dieser Plan zerfällt schnell im Chaos eines tatsächlichen Wiederherstellungsereignisses, wodurch die Organisation schlecht vorbereitet ist, um sich zu erholen und einen kontinuierlichen Geschäftsbetrieb sicherzustellen. Viele der von uns befragten Kunden betonten den hohen Wert ihrer Teilnahme an Commvaults praxisorientiertem „Minutes-to-Meltdown"-Erlebnis, einer immersiven Veranstaltung, die das Chaos eines echten Cyberangriffs realistisch nachstellt, sowie an Commvaults Cyber-Resilienz-Zertifizierungsprogrammen. Sie bezeichneten diese als entscheidend für die Bereitschaft ihrer Teams im Falle eines Cyberangriffs und für das Erreichen eines höheren Wiederherstellungsniveaus.

- **Cloudbasierte Isolation.** Cleanroom Recovery arbeitet in isolierten Cloud-Umgebungen wie Azure und ist darauf ausgelegt, in Verbindung mit Commvault Airgap Protect zu funktionieren. Airgap Protect bietet unveränderliche und unlöschbare Kopien der geschützten Daten, während Cleanroom Recovery eine vollständig sterile und isolierte Umgebung mit Zero-Trust-Zugriffskontrollen, schneller Bereitstellung und unbegrenzter Skalierung bei Bedarf bereitstellt. Airgap Protect hilft Organisationen, Ransomware-Risiken zu mindern, Datenkonformität aufrechtzuerhalten und die Wiederherstellungsbereitschaft im Falle eines Cybervorfalls oder Datenverlusts zu unterstützen.

- **Wiederherstellungstests.** Cleanroom Recovery ermöglicht Wiederherstellungstests in beliebigem Umfang und mit der Häufigkeit, die am besten zum Geschäftsmodell des Unternehmens passt. Darüber hinaus bietet Commvault Wiederherstellungsschulungen an, die das Chaos eines echten Wiederherstellungsereignisses simulieren und die Erkenntnisse und Erfahrungen fördern, die zu einem effektiven Cyber-Recovery-Plan und dessen Umsetzung führen. Wie in Abbildung 2 gezeigt, berichteten die analysierten Unternehmen, dass sie Wiederherstellungstests nur auf einem einzigen Server oder einer einzelnen Workload pro Monat durchführen, wobei jeder Test durchschnittlich 40 Vollzeitstunden (FTE) in Anspruch nahm. Tests mit Commvault Cleanroom Recovery können die für Wiederherstellungstests benötigte Zeit erheblich verkürzen. Während die Bereitstellung einer Cleanroom-Umgebung nur etwa 30 Minuten dauern kann, hängt die Gesamtdauer eines Tests vom Umfang und der Komplexität der Systeme und Daten ab, die wiederhergestellt werden. Dennoch bietet sie die Möglichkeit, Wiederherstellungstests für das gesamte Ökosystem innerhalb eines deutlich verkürzten Zeitrahmens durchzuführen – im Vergleich zu traditionellen Methoden, die oft Tage oder Wochen dauern und erhebliche FTE-Stunden erfordern. In dieser Analyse stellten wir fest, dass Resilienztests mit Commvault Cleanroom Recovery Wiederherstellungsstrategien ermöglichen, die das Risiko um 97 % reduzieren und gleichzeitig die Wiederherstellbarkeit erheblich verbessern.

Abbildung 2. Die Auswirkungen verstärkter Wiederherstellungstests mit Cleanroom Recovery



Source: Enterprise Strategy Group, now part of Omdia

- **Schnelle Bereitstellung.** Eine Cleanroom-Umgebung kann in wenigen Minuten erstellt und bereitgestellt werden. Dies verkürzt die Zeit bis zur Mindestfunktionsfähigkeit und ermöglicht es Unternehmen, nach einem Cyberangriff ihr Kerngeschäft schnell wiederherzustellen – und so den kontinuierlichen Betrieb sicherzustellen.

- **Forensische Analyse.** Cleanroom Recovery bietet eine isolierte, sichere Umgebung für die forensische Analyse infizierter Systeme, um die Ursache eines Angriffs zu identifizieren. Cleanroom Recovery kann außerdem eine infizierte Umgebung isolieren, um den Umfang und Ablauf einer Infektion sicher zu untersuchen und zu verstehen. Dies liefert wertvolle Erkenntnisse zur Verbesserung zukünftiger Prävention und Reaktionsbereitschaft bei Cyberangriffen.

- **KI-gestützte Wiederherstellung.** Commvault nutzt KI-gestützte Berichterstattung und Automatisierung im gesamten Wiederherstellungsprozess. Dadurch können der letzte bekannte saubere Wiederherstellungspunkt identifiziert und das gesamte Ökosystem in der erforderlichen Reihenfolge der Abhängigkeiten wieder aufgebaut werden.

- **Klare und detaillierte Audits und Berichte.** Commvault bietet umfangreiche Berichtsfunktionen, die für Aktivitäten wie Audits, Zertifizierungen zur Cyberversicherung, die Reduzierung von Versicherungsprämien sowie die Einhaltung lokaler und globaler Gesetze und Vorschriften genutzt werden. Laut vielen der befragten Kunden erfüllen diese detaillierten Berichte auch die Anforderungen von Vorstandsebenen als Nachweis der Cyberangriff-Bereitschaft.

Commvault Cloud Rewind bietet Wiederherstellungs- und Wiederaufbau-Funktionen, die speziell für cloudbasierte Anwendungen und Infrastrukturen entwickelt wurden. Es hilft Organisationen, sich schnell von Cyberangriffen, Ausfällen oder Katastrophen zu erholen, und ermöglicht es ihnen, Prioritäten darauf zu legen, was sie zuerst benötigen, um den kontinuierlichen Geschäftsbetrieb (d. h. Mindestfunktionsfähigkeit) aufrechtzuerhalten.

Die Funktionen von Commvault Cloud Rewind umfassen:

- **Schnelle Wiederherstellung von Cloud-Anwendungen und -Umgebungen.** Cloud Rewind kann automatisch eine Art „Zeitmaschine" für Anwendungsumgebungen erstellen, die es einer Organisation ermöglicht, Anwendungen und Infrastrukturen – zusammen mit den wesentlichen Elementen der Umgebung – zurückzuspulen, um zu dem Zeitpunkt vor einem schädigenden Cyberangriff zurückzukehren.

- **Erkennung von Cloud-Konfigurationen.** Cloud Rewind erkennt kontinuierlich Cloud-Service-Konfigurationen, um Abhängigkeiten zu kartieren und sich an die spezifische Cloud-Architektur und die Dienste einer Organisation anzupassen.

- **Reduziertes Risiko durch Cloud-Fehlkonfigurationen.** Die Automatisierung und Orchestrierung von Cloud Rewind verringern das Risiko von Anwendungsfehlern, indem sie vorhersehbare Wiederherstellungspfade und -prozesse bereitstellen und das Potenzial menschlicher Fehler begrenzen.

- **Kontinuierliche Cyberresilienz.** Hyperscale-Clouds erfordern Hyperscale-Resilienz. Cloud Rewind unterstützt die sofortige Wiederherstellung und den Wiederaufbau sowohl innerhalb derselben Zone als auch über verschiedene Zonen, Regionen und Konten hinweg – und bietet so maximale Flexibilität für schnelle Wiederherstellung und kontinuierlichen Geschäftsbetrieb.

- **Patentierte Dual-Vault-Cloud-Zeitmaschine.** Cloud Rewind verwendet sichere, unveränderliche Tresore für die sofortige Wiederherstellung von Anwendungen. Separate Tresore werden für Cloud-Konfigurationen und Anwendungsdaten genutzt, um schnellere Wiederherstellungen und einen ununterbrochenen Betrieb zu ermöglichen.

Wirtschaftliche Validierung der Enterprise Strategy Group

Die Enterprise Strategy Group führte eine quantitative wirtschaftliche Analyse durch, um zu verstehen, wie Commvault Cleanroom Recovery und Cloud Rewind einer Organisation helfen können, ihre IT- und Geschäftsziele zu erreichen. Unser Economic Validation-Prozess ist eine bewährte Methode, um den wirtschaftlichen Wert eines Produkts oder einer Lösung zu verstehen, zu validieren, zu quantifizieren und zu modellieren. Der Prozess nutzt die Kernkompetenzen der Enterprise Strategy Group in den Bereichen Markt- und Branchenanalyse, zukunftsorientierte Forschung sowie technische und wirtschaftliche Validierung. Wir führten ausführliche Interviews mit Commvault-Kunden, um zu verstehen, wie sich der Umstieg auf Cleanroom Recovery und Cloud Rewind auf ihre

Organisationen ausgewirkt hat – insbesondere in Bezug auf Wiederherstellungstests und die allgemeine Wiederherstellungsfähigkeit im Falle eines Cyber- oder Ransomware-Angriffs sowie anderer potenzieller Bedrohungen.

Die qualitativen und quantitativen Ergebnisse dienten als Grundlage für ein einfaches Wirtschaftsmodell, das die erwarteten Kosten und Vorteile einer verbesserten Wiederherstellbarkeit mit Cleanroom und Cloud Rewind vergleicht. Die befragten Organisationen repräsentieren eine Vielzahl globaler Branchen, darunter Energie, Gesundheitswesen, Fertigung, Industrieanlagen, Biomedizin, Bildung, Technologie, IT-Beratung, Finanzdienstleistungen, Einzelhandel und Regierung, mit jährlichen Umsätzen zwischen 2,4 Milliarden USD und 20,5 Milliarden USD.

Wirtschaftsanalyse von Commvault Cleanroom und Cloud Rewind

Die wirtschaftliche Analyse der Enterprise Strategy Group ergab, dass Organisationen, die Commvault Cleanroom Recovery und Cloud Rewind als Grundlage ihrer Test- und Wiederherstellungsstrategie einsetzen, folgende Vorteile genießen:

- **Verbesserte Geschäftskontinuität.** Schnelle, saubere und vollständige Wiederherstellbarkeit ist ein Eckpfeiler einer effektiven Strategie für Geschäftskontinuität. Die Enterprise Strategy Group stellte fest, dass Unternehmen, die Commvault Cleanroom Recovery und Cloud Rewind nutzen, eine deutlich höhere Wahrscheinlichkeit einer vollständigen Wiederherstellung haben.

- **Niedrigere Kosten für Wiederherstellung und Tests.** Wir stellten fest, dass die Kosten für Wiederherstellungstests erheblich reduziert wurden, wenn auf Cleanroom Recovery umgestellt wurde.

- **Reduzierte Komplexität und technische Schulden.** Cleanroom Recovery und Cloud Rewind sind Teil von Commvault Cloud – einer umfassenden Plattform für Datenschutz und Cyberresilienz, die für moderne hybride Umgebungen entwickelt wurde. Der Umstieg auf eine vereinfachte und hochintegrierte Lösung beseitigt jahrzehntelange technische Schulden und reduziert sowohl die Anzahl als auch das erforderliche Qualifikationsniveau des Personals, das für die Verwaltung und Skalierung der Commvault-Lösung benötigt wird.

Verbesserte Geschäftskontinuität

Datenresilienz ist für mehr als ein Drittel (36 %) der Organisationen die oberste IT-Priorität und gehört für 88 % zu den fünf wichtigsten Prioritäten. Interviews der Enterprise Strategy Group ergaben, dass die meisten Organisationen Schwierigkeiten haben, wirksame Strategien und Pläne für Cyberresilienz und Wiederherstellung zu entwickeln, umzusetzen und zu testen. Wir stellten fest, dass Commvault Cleanroom Recovery und Cloud Rewind aus vielen Gründen die Eckpfeiler eines Business-Continuity-Plans auf Unternehmensebene sind, darunter:

- **Ermöglichung von Wiederherstellungstests.** Obwohl die meisten Organisationen angaben, dass Datenresilienz oberste Priorität hat, verfügten nur wenige der für diese Analyse befragten Unternehmen vor der Einführung von Cleanroom Recovery über umfassende, regelmäßige und zuverlässige Testpläne.

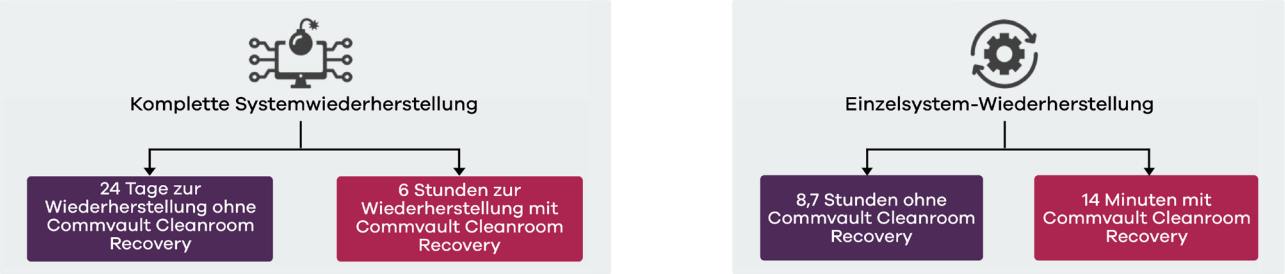
  Wir stellten fest, dass Cleanroom Recovery durch seine Flexibilität und Benutzerfreundlichkeit jede Form von Wiederherstellungstests ermöglicht, die den Anforderungen eines Unternehmens entspricht. Eine Umgebung kann schnell bereitgestellt werden, und Commvaults Metallic AI automatisiert große Teile des Testprozesses, ohne Produktionssysteme zu beeinträchtigen. Benutzer können Wiederherstellungssequenzen anpassen, um Daten in einer priorisierten und logischen Reihenfolge wiederherzustellen; zudem können Netzwerk, Speicher und Anwendungen mithilfe von Cloud Rewind wiederhergestellt werden, um ein vollständiges Cyber- Recovery-Szenario zu testen.

„Bevor wir Commvault Cleanroom Recovery eingeführt haben, führten wir jährliche Wiederherstellungstests auf einer unserer Serverfarmen durch. Wir mussten davon ausgehen, dass, wenn wir eine wiederherstellen konnten, alle wiederherstellbar wären. Jetzt, mit Cleanroom, führen wir monatliche Wiederherstellungstests für all unsere kritischen Assets durch und wissen, dass wir uns im Falle eines Cyberangriffs schnell wiederherstellen können."

– Direktor für Global IT, Dienstleistungs- und Lösungsanbieter

- **Nahezu sofortige Wiederherstellung.** Mit Cleanroom Recovery kann eine Wiederherstellungsumgebung in wenigen Minuten eingerichtet werden, was den gesamten Wiederherstellungsprozess erheblich beschleunigt. Vor der Einführung von Cleanroom Recovery dauerte die Wiederherstellung durchschnittlich 8,7 Stunden – in einigen Fällen sogar deutlich länger. Wie in Abbildung 3 zu sehen ist, erklärte der IT-Direktor eines Universitätssystems: **„Früher dauerte es 24–36 Stunden, um eine einzelne Serverinstanz wiederherzustellen, und bis zu 24 Tage, um sich von einem Cybereereignis zu erholen. Heute können wir alles in weniger als einer Stunde wiederherstellen."**

Abbildung 3. Vorteile bei der Wiederherstellungszeit

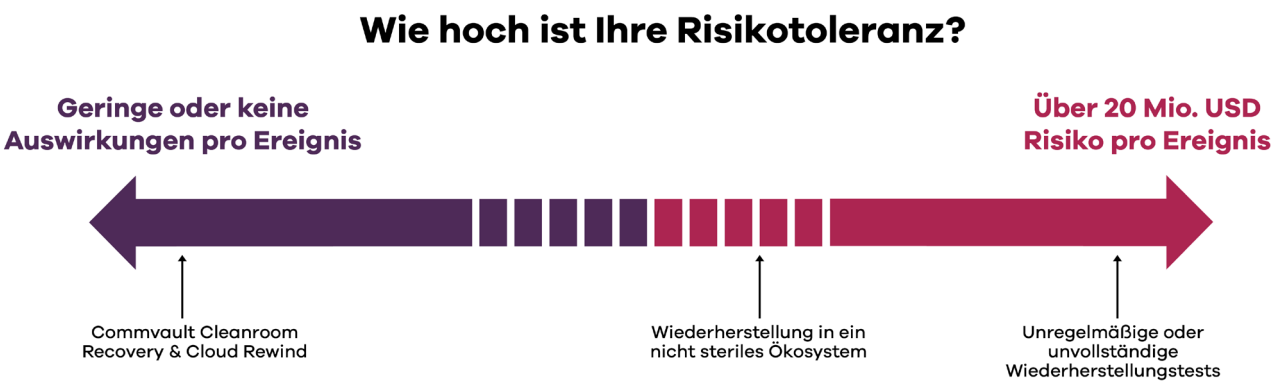


Source: Enterprise Strategy Group, now part of Omdia

Ein weiteres Beispiel stammt von einem Hersteller von Energieanlagen, der jeden Abend vollständige Wiederherstellungstests durchführt. Dadurch verfügt das Unternehmen über eine sofort verfügbare Umgebung, auf die im Falle eines

Ausfalls umgeschaltet werden kann. Der globale Infrastruktur-Direktor dieses Herstellers erklärte: **„Ich wache jeden Tag auf, überprüfe meinen Cleanroom-Recovery-Bericht über die Wiederherstellung der letzten Nacht und weiß, dass wir geschützt sind und uns erholen können. Ausfallzeiten sind in unserem Geschäft teuer – sowohl finanziell als auch in Bezug auf Kundenzufriedenheit. Wir haben Ausfallzeiten eliminiert, da wir uns immer von Cyberereignissen erholen können."** Angesichts von Kundenangaben über Kosten eines Cybervorfalls von rund 20 Millionen USD (mit jüngsten Beispielen in den Nachrichten von über 100 Millionen USD) sowie des immensen Reputationsschadens müssen Unternehmen ihre Risikotoleranz bewerten und sicherstellen, dass ihre Resilienzstrategie dieser entspricht (siehe Abbildung 4).

Abbildung 4. Verständnis der Korrelation zwischen Resilienzstrategie und Risiko



Source: Enterprise Strategy Group, now part of Omdia

- **Verbesserte Wiederherstellbarkeit.** Eine grundlegende Wahrheit der Datenresilienz lautet: Wenn kritische Daten und Infrastruktur nicht wiederhergestellt werden können, sollten sie niemals gesichert werden. Bei der Untersuchung der Ausgangssituation unserer Studienteilnehmer vor der Einführung von Commvault Cleanroom Recovery sahen wir zu viele Beispiele, in denen keine Gewissheit über die Wiederherstellbarkeit bestand. Der IT-Direktor für Infrastruktur eines weltweit tätigen Industriekonzerns fasste dies treffend zusammen: **„Mit Cleanroom kann ich absolut garantieren, dass mein letztes Backup wiederherstellbar ist. Früher war das nur Hoffnung und Theorie."**

- **Verlagerung der Expertise auf proaktives Denken.** Die KI-Funktionen von Cleanroom Recovery wurden häufig als bahnbrechend bezeichnet – aus drei Hauptgründen: die Geschwindigkeit und Vollständigkeit der Wiederherstellung, die Fähigkeit, Ursachen von Fehlern zu isolieren und zu identifizieren, sowie die Möglichkeit, dass IT-Mitarbeiter durch den Einsatz von Commvaults Metallic AI Automatisierungs- und Orchestrierungstools ihre Zeit freisetzen und sich stärker auf proaktive Aufgaben konzentrieren können. Der Direktor für IT-Lösungsengineering eines Krankenhausnetzwerks sagte: **„Seit wir auf Cleanroom Recovery und Cloud Rewind umgestiegen sind, konnte ich einige meiner besten Mitarbeiter auf zukunftsorientierte Aufgaben ansetzen, die es**

uns ermöglichen, Probleme zu lösen, die Ärzte und Patienten betreffen. Unsere Mitarbeitenden sind zufriedener und arbeiten besser zusammen, was zu einer verbesserten Patientenversorgung sowie höherer Kundenzufriedenheit und -bindung führt."

- **Isolierte Untersuchung.** Wenn ein Eindringen oder eine Infektion auftritt, kann die Untersuchung Monate dauern, um zu verstehen, wie das Problem in das IT-Ökosystem gelangt ist und wie es sich verbreitet hat. Darüber hinaus wurden über ein Drittel der Organisationen, die Opfer eines erfolgreichen Ransomware-Angriffs wurden, innerhalb von 12 Monaten erneut angegriffen. Unsere Gesprächspartner nannten als Hauptgrund die Komplexität, alle Aspekte einer Sicherheitsverletzung oder Infektion vor der Wiederherstellung zu identifizieren und zu beheben. Ein Sicherheits- und Wiederherstellungsexperte eines Unternehmens für Cyberresilienz fasste dies so zusammen: **„Wenn wir der Integrität der Daten während eines Wiederherstellungsereignisses nicht vertrauen können, können wir sie nicht in unsere Produktionsumgebung zurückspielen. Mit Cleanroom Recovery können wir die wiederhergestellte Umgebung isolieren und unser ‚Minimum Viable Company' tatsächlich darin betreiben. Dadurch können wir in einer geschützten und isolierten Umgebung weiterarbeiten."** Andere Befragte erwähnten Anforderungen, eine infizierte Umgebung zu Prüf- oder Versicherungszwecken verfügbar zu halten. Ein VP für Infrastruktur eines globalen Dienstleistungsunternehmens erklärte: **„Cleanroom ermöglicht es uns, unsere infizierte Umgebung in einer vollständig geschützten Instanz zu belassen, in der wir sie untersuchen und verstehen können, wie sie sich verbreitet hat. So erfüllen wir Versicherungs- und Compliance- Anforderungen, während wir gleichzeitig an anderer Stelle die Mindestfunktionsfähigkeit wiederherstellen und den Geschäftsbetrieb ohne Unterbrechung fortsetzen."**

„Wir treffen uns vierteljährlich mit Commvault, um unsere Wiederherstellungspläne zu überprüfen und Best Practices auszutauschen. Keiner unserer anderen IT-Anbieter macht das. Wir arbeiten mit über 100 Anbietern zusammen – Commvault steht eindeutig an der Spitze, wenn es darum geht, uns wie echte Partner zu behandeln."

– IT-Direktor, Universitätssystem

- **Unterstützung durch Commvault bei der Vorbereitung.** Die Qualität der Schulungs- und Lernprogramme von Commvault fiel besonders positiv auf, als wir die Kombination aus Technologie und Know-how untersuchten, die das Unternehmen bietet. Ein Kunde erklärte: **„Commvault glänzt besonders darin, uns dabei zu helfen, Wiederherstellbarkeit in einem chaotischen Zustand zu testen. Früher gingen wir einfach eine Checkliste durch und dachten, wir wären vorbereitet. Doch in einem echten Cybereregnis läuft nichts geordnet ab. Commvault hilft uns, dieses Chaos realistisch zu simulieren und uns auf das Unerwartete vorzubereiten."** Dies geschieht über Programme wie Commvault's Minutes-to-Meltdown, eine von Fachexperten geleitete Intensivsitzung, die den Teilnehmern hilft, moderne Ransomware-Angriffe zu verstehen. Dabei übernehmen die Teilnehmenden aktiv die Rollen von CISO, CIO und anderen Führungskräften, um einen Plan für verbesserte Cyber-Bereitschaft zu entwickeln. Commvault Recovery Range ist ein

praxisorientiertes Labor, das reale Cyberangriffe simuliert und sich auf erfolgreiche Wiederherstellung konzentriert. Die Teilnehmenden treten gegen die Zeit an, um ein großes Unternehmen unter Beschuss zu retten. Darüber hinaus bietet Commvault umfassende Cyberresilienz-Zertifizierungsprogramme für Kunden an.

- **Beseitigung von Komplexität während der Wiederherstellung** Wiederherstellung bedeutet weit mehr als das Zurückspielen von Daten. Mehrere Systeme müssen in einer bestimmten Reihenfolge wieder hochgefahren werden, um Abhängigkeiten zu erfüllen. Ein IT-Leiter eines globalen Backup-Anbieters erklärte: **„Unsere Wiederherstellungsmatrix umfasst über 20 verschiedene Ebenen, in denen Dienste in der richtigen Reihenfolge gestartet werden müssen. Mit Cleanroom Recovery automatisieren wir dies exakt in der Reihenfolge, die für den Erfolg erforderlich ist."**

- **Flexibilität bei Wiederherstellungsoptionen.** Die Wiederherstellung nach einem echten Cyberangriff kann eine Reparatur oder einen Wiederaufbau der zugrunde liegenden Infrastruktur oder sogar ganzer Standorte erfordern. Commvault Cleanroom Recovery und Cloud Rewind können innerhalb von Minuten eine Wiederherstellungsumgebung schaffen – völlig unabhängig von Hardware- oder Standortanforderungen.

- **Steigerung der Kundenzufriedenheit und des Unternehmenswachstums.** Auf die Frage nach den geschäftlichen Auswirkungen von Wiederherstellungstests berichteten mehrere Befragte, wie positiv ihre Kunden auf ihre verbesserten Fähigkeiten reagierten. Ein VP für Cloud Services sagte: **„Wenn ich meinen Kunden erkläre, dass wir monatliche statt jährliche Wiederherstellungstests durchführen können, wächst ihr Vertrauen in die Zusammenarbeit mit uns. So bieten wir ein Serviceniveau, das unsere Wettbewerber nicht erreichen können."** Er fügte hinzu: **„Wir halten unsere bestehenden Kunden zufriedener und gewinnen neue hinzu, weil wir unsere Bereitschaft zur Cyber-Wiederherstellung demonstrieren können. Unser Umsatz ist direkt um 3,5 % gestiegen, allein durch den Wechsel zu Commvault Cleanroom Recovery."**

Niedrigere Wiederherstellungs- und Testkosten

„Der Wechsel zu Commvault Cleanroom Recovery bedeutet nicht nur Kosteneinsparungen. Das Maß an Fachwissen, das erforderlich wäre, um tatsächlich eine saubere Wiederherstellungsumgebung zu schaffen, übersteigt unsere eigenen Fähigkeiten."

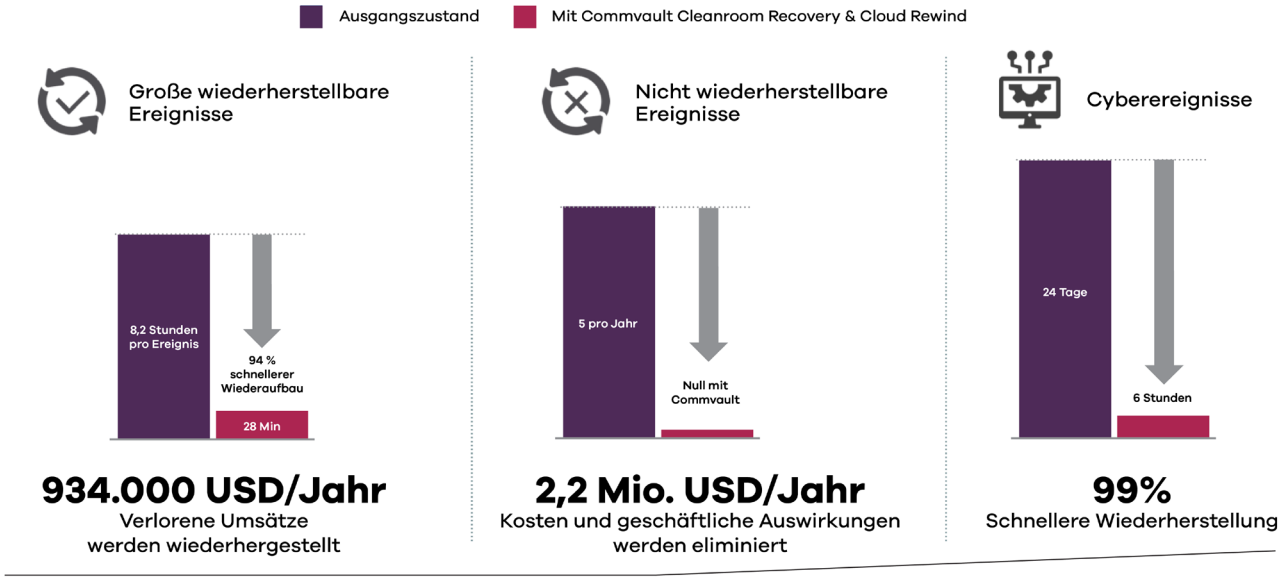
– Direktor für IT-Lösungsentwicklung, Globaler Cloud-Dienstleister

Der Vergleich der Kosten für Wiederherstellungstests vor und nach dem Wechsel zu Commvault Cloud ist schwierig, da sich die Art und Weise, wie Organisationen nach der Einführung von Commvault testen, dramatisch verändert. Die von uns untersuchten Unternehmen gingen von jährlichen Tests eines kleinen Teils ihres gesamten Ökosystems zu monatlichen Tests ihrer gesamten Daten-, Speicher- und Anwendungsplattformen über – darunter auch ein Unternehmen, das jede Nacht vollständige Wiederherstellungstests durchführt, um die potenziellen

Auswirkungen von Ausfallzeiten zu minimieren. Trotz der Unterschiede zwischen den einzelnen Fällen stellten wir fest, dass die folgenden Vorteile in allen untersuchten Organisationen konsistent auftraten:

- **Reduzierte Auswirkungen von Ausfallzeiten.** Bei der Untersuchung der Vorteile verbesserter Wiederherstellungsprozesse war die erste Kennzahl, die die meisten Organisationen nannten, die Veränderung der Ausfallzeiten durch beschleunigte Wiederherstellung. Wir stellten fest, dass Commvault Cloud Rewind die Anzahl kleinerer Wiederherstellungsereignisse pro Jahr reduzieren und die Auswirkungen jedes einzelnen Ereignisses verringern kann. Bei größeren Ereignissen erklärte keiner der Befragten, dass der frühere Zustand mit dem vollständig wiederherstellbaren Zustand von Commvault Cleanroom Recovery vergleichbar sei. Für unsere Modellberechnungen nahmen wir an, dass die wiederhergestellten Zustände gleichwertig waren, um die Auswirkungen verschiedener Wiederherstellungsszenarien auf unser Beispielunternehmen zu untersuchen (siehe Abbildung 5).

Abbildung 5. Vor und nach Commvault Cleanroom Recovery und Cloud Rewind



Zudem kann der geschäftliche Einfluss eines Cybereereignisses mehrere Millionen betragen

Source: Enterprise Strategy Group, now part of Omdia

„Wir erhalten Rabatte auf unsere Cyberversicherung dank der Verbesserungen, die Cleanroom Recovery bietet. Commvault macht es uns äußerst einfach, unseren Plan detailliert zu dokumentieren. Das spart uns über 100.000 USD pro Jahr."

– Globaler Infrastrukturdirektor, Industrieunternehmen

- **Beseitigung von Kostenbarrieren für Tests.** Die von uns befragten Organisationen nannten viele Gründe, warum ihre Wiederherstellungstestpläne nicht mit ihren Cyberresilienz-Zielen übereinstimmten. Der erste war die Kostenbelastung durch FTE-Zeit (Vollzeitäquivalente) für Tests, der zweite die Kosten und Komplexität bei der Erstellung und Aufrechterhaltung einer Testumgebung.
  Wir untersuchten Beispiele, bei denen Kunden bis zu 20 Millionen USD investierten, um eine Umgebung ähnlich wie Cleanroom Recovery zu schaffen – jedoch mit deutlich schlechteren Ergebnissen.
  Andere versuchten, cloudbasierte Wiederherstellungsumgebungen zu entwickeln, stellten jedoch fest, dass diese nicht die erforderliche Geschwindigkeit erreichten und die Ergebnisse unter den Erwartungen blieben. Der IT-Direktor eines Universitätssystems erklärte: **„Cleanroom ist 60 % günstiger als die Nutzung von VM- basierten Wiederherstellungsumgebungen, und wir können direkt aus einer Cleanroom-Umgebung heraus Mindestfunktionsfähigkeit erreichen. Es wäre unmöglich, unser Minimum Viable Company problemlos aus einer VM-Wiederherstellung zu betreiben.“**

- **Reduzierte FTE-Kosten für Planung und Test der Wiederherstellung.** Die durchschnittlichen Testkosten der untersuchten Unternehmen umfassten monatliche Tests, die fünf FTEs insgesamt 40 Stunden kosteten – was 141.864 USD pro Jahr entspricht. Nach der Umstellung auf Cleanroom sanken diese Kosten auf unter 11.000 USD pro Jahr. Gleichzeitig ergab unsere Analyse, dass die Testfrequenz von 12 Tests pro Jahr auf 365 Tests pro Jahr anstieg – jeweils durchgeführt von einer Person in nur einer halben Stunde pro Test.

- **Auswirkungen von KI-gestützter Anleitung und Best Practices.** Der IT-Direktor eines Cloud-Service-Unternehmens erklärte: **„Alles, was ich in meinem Test- und Wiederherstellungsprozess automatisieren kann, spart Zeit und Geld und erhöht die Wahrscheinlichkeit, dass wir im Falle eines Cyberangriffs erfolgreich und sauber wiederherstellen können. Commvault AI identifiziert kontinuierlich Verbesserungen und Best Practices, um unsere Wiederherstellungspläne zu optimieren und unsere Kosten zu senken.“**

- **Niedrigere Kosten für Cyber- und Geschäftsversicherungen.** Befragte berichteten, dass Cyber- und Geschäftsversicherungen leichter und zu niedrigeren Kosten zu erhalten waren – insbesondere aufgrund ihrer Investition in Commvault und ihrer Fähigkeit, detaillierte Test- und Wiederherstellungspläne sowie die erforderlichen Berichte für Compliance- und Regulierungsprüfungen vorzulegen.

„Wir vertrauen Commvault und Microsoft und schätzen ihre Partnerschaft sehr. Wir wissen, dass unsere Commvault Cloud- Lösung vollständig und sicher ist, und die Flexibilität ihrer Azure-Integration ermöglicht es uns, uns auf unser Kerngeschäft zu konzentrieren.”

– IT-Direktor, Universitätssystem

- **Abbau technischer Schulden.** Bei der Untersuchung des Zustands der Kunden vor der Einführung von Cleanroom Recovery stellten wir fest, dass zwischen ihren Anforderungen an Cyberresilienz und ihren tatsächlichen Fähigkeiten ein fundamentaler Widerspruch bestand. Wir fanden zusammengewürfelte, unvollständige und ungetestete Pläne, deren Kosten in keinem Verhältnis zu ihren Vorteilen standen. Viele Entscheidungen wurden aus Zwang oder aufgrund früherer Beschränkungen getroffen. Mit Cleanroom Recovery und Cloud Rewind können diese Kunden nun Testhäufigkeit und -umfang an ihre Resilienzziele anpassen und Wiederherstellungen in jeder benötigten Umgebung planen. So können sie schnell den Zustand der Mindestfunktionsfähigkeit wiedererlangen, der den Geschäftsbetrieb ohne Risiko von Umsatzverlusten oder Reputationsschäden ermöglicht.

Reduzierte Komplexität und geringere technische Schulden

Die Enterprise Strategy Group führte eine umfassende wirtschaftliche Analyse zu den Vorteilen von Commvault Cloud durch und stellte fest, dass die zusätzlich für diese Analyse befragten Kunden dieselben Vorteile erzielten:

- **Kosteneffizienz.** Commvault Cloud kann die Kosten senken und eine wesentlich vorhersehbarere Kostenstruktur im Vergleich zu alternativen Umgebungen bieten. Commvault ist ein Eckpfeiler, mit dem Unternehmen ihre Cloud-Umgebungen optimieren, die Gesamtausgaben reduzieren und gleichzeitig ihre Cyberresilienz und Cybersicherheit verbessern können.

- **Erhöhte Agilität.** Agilität – sowohl in der Arbeitsweise der Mitarbeitenden als auch in der Fähigkeit einer Organisation, ihre Daten in Zeiten rascher Veränderungen zu schützen – ermöglicht es Unternehmen, sich auf ihr Kerngeschäft zu konzentrieren, anstatt sich nach einem Cyberangriff oder anderen Bedrohungen um Datensicherheit und Wiederherstellung sorgen zu müssen. Ein wesentlicher Vorteil des Commvault-Ansatzes ist die branchenführende Tiefe und Breite der Workload-Abdeckung. Mehrere befragte Kunden beschrieben dies als die Sicherheit, die Commvault bietet, nämlich dass auf dem beschleunigten Weg in die Cloud keine Workload „zurückgelassen" wird – und zwar mit dem Ziel, die Cyber- und Datenresilienz zu verbessern, die Transformation zu optimieren und Kosten zu senken, während gleichzeitig die Agilität gesteigert wird.

- **Reduziertes Risiko.** Commvault bietet seit über 27 Jahren Datensicherung und ist seit der Einführung von **Microsoft Azure im Jahr 2010** in Microsofts Cloud-Lösung integriert – für einen ganzheitlichen, cloudnativen Ansatz. Im Jahr 2019 erweiterte Commvault seine Plattform um ein SaaS-Angebot, das auf derselben Technologie wie die Kernsoftware basiert. Dadurch können Daten unabhängig von ihrem Speicherort oder der gewählten Bereitstellungsmethode (On-Premises, Public Cloud oder SaaS) gesichert und geschützt werden. Dieser integrierte Ansatz ermöglichte es gemeinsamen Microsoft- und Commvault-Kunden, im Durchschnitt 15 bestehende Datensicherungslösungen durch den Wechsel zu Commvault Cloud auf Azure zu ersetzen – und dadurch ihr Risikoniveau in der gesamten Datenlandschaft erheblich zu senken.

Commvault Cloud vereint die SaaS-Lösung und die Softwarelösung von Commvault in einer einheitlichen Steuerungsebene, die erweiterte Funktionen und Benutzerfreundlichkeit im großen Maßstab bietet. Dadurch können Organisationen die Datensicherheits- und Cyber-Wiederherstellungsfunktionen nutzen, die sie von Commvault erwarten – ohne die Komplexität, die normalerweise mit Schutzlösungen auf Unternehmensebene einhergeht – und gleichzeitig einen klaren Fahrplan für eine nahtlose Transformation zu SaaS-basierter Datensicherung erhalten. Darüber hinaus verbessert Commvault Cloud die Cyberresilienz und die Datensicherheitslage einer Organisation erheblich.

Fazit

Die meisten Organisationen haben eine enorme Lücke zwischen ihren Anforderungen an Cyberresilienz und ihrer tatsächlichen Fähigkeit, sich nach einem Cyberangriff schnell zu erholen. Die Kosten und die Komplexität von Tests übersteigen häufig Budget und Ressourcen, und das echte Chaos, das mit einem großen Wiederherstellungsereignis einhergeht, lässt sich in Tests nur schwer nachbilden. Während die Forschung der Enterprise Strategy Group bestätigt, dass Cyberresilienz für 88 % der Organisationen zu den fünf wichtigsten Prioritäten gehört, haben wir Großunternehmen befragt, um ihre Strategien für Wiederherstellungstests zu verstehen. Dabei stellten wir fest, dass die meisten nur teilweise und seltene Tests durchführten – eher eine Checkliste als ein belastbarer Plan, der eine vollständige Wiederherstellung ermöglicht. Unsere Kundeninterviews zeigten, dass die Kosten von Ausfallzeiten zwischen 10.000 USD pro Stunde und mehreren Millionen USD pro Minute lagen. Wir stellten außerdem fest, dass zu viele Organisationen in Cyberresilienz investieren, als wäre das Risiko das Problem anderer – und dass das akzeptierte Risikoniveau vieler Unternehmen als inakzeptabel gelten sollte.

Wir analysierten die Auswirkungen, die Commvault Cleanroom Recovery und Commvault Cloud Rewind auf die Verbesserung von Wiederherstellungstests sowie auf Cyberresilienz und Wiederherstellung insgesamt haben können. Wir stellten fest, dass Cleanroom Recovery nicht nur eine Wiederherstellungsumgebung bietet, die weit über das hinausgeht, was die meisten Organisationen selbst schaffen könnten, sondern auch sterile, KI-gestützte Umgebungen, in denen eine Wiederherstellung auf Mindestfunktionsfähigkeit oft innerhalb von Minuten – statt Stunden, Tagen, Wochen oder Monaten – möglich ist, wodurch Ausfallzeiten nahezu auf null reduziert werden. Wir fanden heraus, dass Cloud Rewind Anwendungen und zugehörige Infrastrukturen in der Cloud schnell wiederherstellen kann, indem es zu einem früheren Zeitpunkt vor dem Cyberangriff zurückkehrt. Darüber hinaus sind wir der Ansicht, dass die Partnerschaft zwischen Commvault und Microsoft im Bereich Cyberangriffs- Bereitschaft und Wiederherstellung den zusätzlichen Vorteil bietet, Organisationen eine robuste Grundlage zu geben, um das gesamte Spektrum potenzieller Störungen zu bewältigen und gleichzeitig eine schnelle Wiederherstellung auf Mindestfunktionsfähigkeit zu planen.

Darüber hinaus glauben wir, dass Commvault den „Code für Wiederherstellbarkeit geknackt“ hat – mit von Kunden berichteten Ergebnissen von 94 % schnellerem Wiederaufbau (Cloud Rewind) und 99 % schnellerer Wiederherstellung (Cleanroom Recovery). Dies ermöglicht es Organisationen, kritische Systeme und Daten im Falle einer Cyberstörung schnell wiederherzustellen. Wir kamen zu dem Schluss, dass die Vorteile eines Cyberresilienz-Plans, der Commvault Cleanroom

Recovery und Commvault Cloud Rewind umfasst, den Unterschied zwischen erheblichen Geschäftsverlusten und langanhaltendem Markenschaden ausmachen können – im Vergleich zu Cybereereignissen, die mit minimaler oder gar keiner Geschäftsunterbrechung behoben werden, wenn der Wiederherstellungsplan Commvault Cloud integriert mit Microsoft Azure beinhaltet.

Commvault Cleanroom Recovery und Cloud Rewind sind die Grundpfeiler eines effektiven und modernen Cyberresilienzplans. Die Enterprise Strategy Group empfiehlt nachdrücklich, dass jede Organisation, bei der eine Diskrepanz zwischen ihren Resilienzfähigkeiten und der Fähigkeit besteht, einen bewährten Cyberresilienzplan umzusetzen, prüfen sollte, was Commvault und seine langjährige Partnerschaft mit Microsoft tun können, um entscheidende Schritte in Richtung echter Cyber-Sicherheit und Wiederherstellungsfähigkeit zu ermöglichen und zu beschleunige.