



# Modernisierung der Datensicherung in der Hybrid Cloud



Behalten Sie die Kontrolle und schützen Sie Ihre  
Daten vor Unterbrechungen

# Inhalt

## **3      Kurzfassung**

---

## **3      Moderne Workloads sind modernen Bedrohungen ausgesetzt**

---

## **4      Reibungsloses Arbeiten dank optimierter Abläufe und erhöhter Sicherheit**

---

## **5      Modernisieren Sie Ihre Datensicherung mit Zerto, a Hewlett Packard Enterprise company**

5 Abschwächen neuartiger Bedrohungen

5 Weniger Unterbrechungen und Ausfallzeiten

6 Erstellung kosteneffizienter sicherer Architekturen

---

## **6      Datenorientiert in die Zukunft**

---

## **7      Über HPE**

## Kurzübersicht

Herkömmliche Datensicherungsmethoden sind den Anforderungen der heutigen verteilten Anwendungen und Daten nicht gewachsen. Angesichts des exponentiellen Datenwachstums und fortschrittlicher Cyber-Bedrohungen wie Ransomware, behördlicher Auflagen, Risiken durch Naturkatastrophen, menschliches Versagen und Hardware-Ausfälle stehen Unternehmen vor immer größeren Herausforderungen. Die Lösung dieser Probleme ist unerlässlich, um geschäftskritische Systeme zu schützen, einen nahtlosen Betrieb in unterschiedlichen Umgebungen zu gewährleisten und kostspielige Ausfallzeiten und Datenverluste zu vermeiden.

Dieses Whitepaper soll Unternehmen bei der Bewältigung der Herausforderungen helfen, die mit dem Schutz ihrer Daten vor Unterbrechungen, Verlusten und der ständigen Bedrohung durch Cyber-Angriffe in ihren wachsenden hybriden Umgebungen verbunden sind. Darin werden die wichtigsten Herausforderungen untersucht, die sich aus der Cloud-übergreifenden Datensicherung ergeben. Dabei wird die Bedeutung moderner Ansätze hervorgehoben, die die Business Continuity ohne Unterbrechungen aufrechterhalten.

## Moderne Workloads sind modernen Bedrohungen ausgesetzt

Im heutigen digitalen Zeitalter nehmen das Volumen und die Bedeutung von Daten für moderne Unternehmen exponentiell zu, sodass eine robuste Datensicherung dringender denn je ist.

Herkömmliche Methoden zur Sicherung und Wiederherstellung können mit den steigenden Datenmengen häufig nicht Schritt halten. Unternehmen setzen daher häufig auf eine Mischung aus Speicher- und Softwarelösungen, was zu Datensilos führt. Dieser Ansatz verschlingt nicht nur erhebliche Bandbreiten und Budgets, sondern macht auch die Verwaltung und den Schutz von Daten in Hybrid Cloud-Umgebungen komplexer.

Die Hybrid Cloud wird bevorzugt, weil sie die Flexibilität der Public Cloud mit der Sicherheit der On-Premises-Infrastruktur kombiniert. Diese Kombination erfordert jedoch moderne Datensicherungsmaßnahmen, um zu gewährleisten, dass vertrauliche Informationen sicher und zugänglich bleiben und immer neue Vorschriften einhalten.

Zur Liste der Herausforderungen für die Datensicherung kommt noch die weitere Zunahme von Cybersicherheitsbedrohungen hinzu. In diesem Jahr haben Bedrohungsakteure zunehmend auf künstliche Intelligenz gesetzt, um raffiniertere Angriffe zu starten. Diese reichen von Deepfakes bis hin zu Bots mit Einmal-Passwörtern, mit denen Unternehmensdaten kompromittiert werden sollen. Da immer mehr Daten an den Edge verlagert werden, können die durch eine Kompromittierung der Umgebung entstehenden Kosten beträchtlich sein. Ein Beispiel dafür sind die finanziellen Folgen für Unternehmen, die von einer Sicherheitsverletzung bei IOT-Geräten (Internet der Dinge) betroffen sind. Jüngsten Berichten zufolge meldeten diese Unternehmen eher kumulative Kosten in Höhe von 5 bis 10 Millionen US-Dollar bei Sicherheitsverletzungen als Unternehmen, die Cyberangriffe auf Geräte außerhalb des IoT<sup>1</sup> verzeichneten.

Es sollte daher nicht überraschen, dass zwei Drittel (66 %) der Führungskräfte in der Technologiebranche Cyber-Bedrohungen als das größte Risiko einstufen, das es im Jahr 2024 zu minimieren gilt.<sup>2</sup> Oder dass für Cloud-Sicherheit im Jahr 2024 ein Wachstum von 24 % prognostiziert wird,<sup>3</sup> womit sie das höchste Wachstum aller Segmente des globalen Markts für Sicherheit und Risikomanagement aufweist. Schließlich beeinträchtigt ein Cyberangriff nicht nur kurzfristig den Betrieb. Er kann auch noch lange nach der Behebung des Angriffs und sogar nach der Wiederherstellung der Daten dem Ruf eines Unternehmens erheblich schaden.

Um den Herausforderungen zunehmender Bedrohungen für Ihre Daten und deren zunehmenden Volumen gerecht zu werden und Ihre Hybrid-Cloud-Umgebungen reibungsloser zu verwalten, benötigen Sie einen besseren, moderneren Ansatz zur Datensicherung.

**Ein Cyberangriff wirkt sich nicht nur kurzfristig auf den Betrieb aus, er kann auch dem Image des Unternehmens schaden.**

<sup>1</sup> „The Top Trends In IoT Security In 2024“, Forrester, März 2024

<sup>2</sup> „Only 2% of businesses have implemented firm-wide cyber resilience, even as cybersecurity concerns are top-of-mind and the average data breach exceeds US\$3M: PwC 2025 Global Digital Trust Insights“, PwC, September 2024

<sup>3</sup> „The Expanding Enterprise Investment in Cloud Security“, Gartner, Juni 2024

## Bewältigung typischer Herausforderungen bei der Datensicherung

**Längere Unterbrechungen:** Unter den aktuellen Arbeitssystemen dauert die Wiederherstellung nach Unterbrechungen zu lange. Unternehmen benötigen einen schnelleren Weg, um nach Unterbrechungen wieder betriebsbereit zu werden, ohne die Business Continuity zu beeinträchtigen.

**Kostspielige Ausfallzeiten:** Viele Unternehmen können sich keine Ausfallzeiten für kritische Workloads leisten, stellen jedoch fest, dass die Datenverfügbarkeit mit den aktuellen Tools weiterhin unzuverlässig ist.

**Bedenken hinsichtlich der Compliance:** Compliance und Sicherheit bereiten allen Unternehmen weiterhin große Sorgen, insbesondere wenn vertrauliche Daten in mehreren Umgebungen verteilt sind.

**Stillstand der Innovation:** Die Unterbrechung der Business Continuity, explodierende Kosten und der Versuch, mit der Bedrohung durch Datenschutzverletzungen Schritt zu halten, beeinträchtigen die Innovationsfähigkeit eines Unternehmens. Diese Stolpersteine machen Unternehmen unflexibler und erschweren die rasche Nutzung neuer Chancen.

Es liegt auf der Hand, dass der aktuelle Ansatz zur Datensicherung nicht mehr funktioniert. Es muss ein neuer Weg eingeschlagen werden, um den Geschäftsanforderungen im datenorientierten Zeitalter gerecht zu werden.

## Reibungsloses Arbeiten dank optimierter Abläufe und erhöhter Sicherheit

Zur Verringerung von Betriebsunterbrechungen und zur Vereinfachung der Komplexität benötigen Unternehmen Lösungen, die für reibungslosere Workloads und die Sicherheit der Daten sorgen – ganz gleich, wo sie sich befinden.

Die Antwort von HPE auf die moderne, hybride Datensicherung hat zwei Ziele: die Beseitigung von Altlasten und die Vereinheitlichung der Verwaltung vom Edge bis zur Cloud. Dieser Ansatz bietet eine schnellere und zuverlässigere Leistung für kritische Anwendungen und trägt gleichzeitig dazu bei, Datenverluste und Ausfallzeiten zu minimieren und den sich ständig verändernden Anforderungen an Sicherheit und Compliance gerecht zu werden.

Bei Unterbrechungen ermöglicht die kontinuierliche Datensicherung (Continuous Data Protection, CDP) von Hewlett Packard Enterprise eine Wiederherstellung innerhalb von Minuten mit branchenführenden RPOs und RTOs.

Ferner sind die HPE Lösungen so konzipiert, dass sie Unternehmen dabei helfen, die Compliance einzuhalten und den sich ständig ändernden Anforderungen an Daten und Vorschriften einen Schritt voraus zu sein, einschließlich detaillierter Berichte, Prüfprotokolle und globaler Multisite-Dashboards. Integrierte Komplettlösungen ermöglichen dabei eine schnelle Air-Gap-Wiederherstellung mit erstklassigen Speicher-, Rechen-, Netzwerk- und Softwarefunktionen.

### Drei Überlegungen für einen reibungslosen Ablauf der Workloads

Unternehmen, die ihre Hybrid-Cloud-Erfahrung hinsichtlich der Datensicherung verbessern möchten, müssen drei Faktoren berücksichtigen.

- **Aufrechterhaltung des Always-on-Geschäfts** durch Optimierung des Schutzes, der Wiederherstellung und der Mobilität von Anwendungen vor Ort und in der Cloud
- **Minimierung von Datenverlusten und Ausfallzeiten** durch CDP mit Wiederherstellung in Minutenschnelle mit branchenführenden RPO und RTO
- **sicherer Schutz** für kritische Daten mit einer dezentralen Zero-Trust-Architektur

## Modernisieren Sie Ihre Datensicherung mit Zerto, a Hewlett Packard Enterprise company

Zerto ermöglicht Unternehmen einen kontinuierlichen Geschäftsbetrieb und vereinfacht den Schutz, die Wiederherstellung und die Mobilität von Daten für eine kontinuierliche Verfügbarkeit in Private, Public und Hybrid Cloud-Bereitstellungen.

Durch die Reduzierung des Risikos und der Komplexität der Modernisierung und Cloud-Einführung können sich Unternehmen verstärkt auf ihre geschäftlichen Innovationen konzentrieren, anstatt Sicherheitsbedrohungen abzuwehren oder sich Sorgen über die Nichteinhaltung von Compliance-Anforderungen zu machen.

### Minimieren neuartiger Bedrohungen

- fortschrittliche Lösungen zur Erkennung und Bekämpfung von Sicherheitsbedrohungen, die Ransomware und andere Malware in Echtzeit identifizieren und neutralisieren können
- on demand-Sandboxen zur Durchführung einfacher Patchtests, forensischer Analysen oder Cybersicherheitsübungen an nahezu exakten Kopien der Produktion
- sichere, lokal installierte, vom Kunden kontrollierte Lösung, die eine isolierte Offline-Wiederherstellungsumgebung mit einem unveränderlichen Datentresor kombiniert, der sogar bei den schlimmsten Ransomware-Angriffen als letzte Verteidigungslinie dienen kann

### Weniger Unterbrechungen und Ausfallzeiten

- CDP für die Wiederherstellung Ihrer Daten innerhalb von Minuten mit branchenführenden RPOs und RTOs
- Automatisierte Failover- und Failback-Prozesse zur Reduzierung von Ausfallzeiten und Aufrechterhaltung der Business Continuity, unabhängig davon, ob einzelne Dateien oder ganze virtualisierte Anwendungen wiederhergestellt werden



## Erstellung kosteneffizienter, sicherer Architekturen

- Nutzen Sie Lösungen, die automatisierte und unterbrechungsfreie Tests für eine robuste und sichere Architektur ohne übermäßige Kosten ermöglichen.
- Halten Sie die Compliance ein und seien Sie den sich ständig weiterentwickelnden Daten- und Regulierungsanforderungen einen Schritt voraus, einschließlich detaillierter Berichte, Prüfprotokolle und globaler Multisite-Dashboards
- Profitieren Sie von integrierten Komplettlösungen, die eine schnelle Air-Gap-Wiederherstellung mit erstklassigen Speicher-, Rechen-, Netzwerk- und Softwarefunktionen ermöglichen.

Sollte alles andere fehlschlagen, bietet Ihnen der Zerto Cyber Resilience Vault eine Zero-Trust-Architektur, die isoliert und offline ist und unveränderliche Datenkopien sicher aufbewahrt.

## Datenorientiert in die Zukunft

Sowohl die Hybrid Cloud als auch exponentiell wachsende Datenmengen sind ein fester Bestandteil unserer datenorientierten Welt. Doch selbst angesichts anhaltender Bedrohungen müssen sie weder ein Hindernis für die Business Continuity noch für weitere Innovationen darstellen.

Die Sicherung und der Schutz kritischer Daten werden auch heute, morgen und in Zukunft von entscheidender Bedeutung sein. Mit den richtigen Tools und modernen Ansätzen können Unternehmen diese Herausforderung selbstbewusst angehen und sich darauf verlassen, dass ihr datenorientiertes Unternehmen gut aufgestellt ist, um in den kommenden Jahren und Jahrzehnten erfolgreich zu sein.



# Über HPE

HPE ist das Edge-to-Cloud-Unternehmen, das Unternehmen weltweit durch eine optimale Wertschöpfung aus allen ihren Daten bei schnelleren Ergebnissen unterstützt. Basierend auf jahrzehntelangem Engagement für eine Neugestaltung der Zukunft und Innovationen, die unsere Lebens- und Arbeitsweise verbessern, bietet HPE einzigartige, offene und intelligente Technologielösungen mit einer konsistenten Erfahrung über alle Clouds und Edges hinweg, um Kunden dabei zu helfen, neue Geschäftsmodelle zu entwickeln, neue Wege zu beschreiten und die operative Leistung zu steigern.

**Weitere Informationen finden Sie unter**

[HPE.com/Zerto](https://hpe.com/Zerto)

Visit HPE.com

## [Chat mit Vertrieb](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Neben der gesetzlichen Gewährleistung gilt für Produkte und Services von Hewlett Packard Enterprise ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Services explizit genannt wird. Die hier enthaltenen Informationen stellen keine zusätzliche Garantie dar. Hewlett Packard Enterprise haftet nicht für technische oder redaktionelle Fehler oder Auslassungen.

a50011803DEE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://hpe.com)

