

Nach dem Angriff ist es zu spät

Warum Immutable Storage
heute Pflicht ist

Monika Kahle | Director, Inside Sales, Arcserve



Ransomware-Vorfälle bestimmen die Schlagzeilen

Geschätzter Umsatzverlust von **350–400 Millionen US-Dollar** bei einem US-amerikanischen Naturkostunternehmen nach einem Cyberangriff – die Wiederherstellung dauerte mehrere Tage

20 % Umsatzrückgang im Jahresvergleich bei einer japanischen Brauerei nach einem Angriff im September 2025 – Beeinträchtigungen dauerten bis Februar 2026 an

700 Mitarbeitende verloren ihren Arbeitsplatz, nachdem ein britisches Transportunternehmen den Betrieb einstellen musste – das Unternehmen konnte weder das Lösegeld zahlen noch Daten aus Backups wiederherstellen

State of Data Resilience 2026*



Jetzt für den Bericht
anmelden – Coming
Soon! [ENG]

52%

Gaben an, dass die eigene Organisation bereits Opfer eines Ransomware-Vorfalles geworden ist

4%

Hatten innerhalb des letzten Monats einen Ransomware-Angriff erlebt

49%

Verfügt über einen immutable Backup-Speicher – eine grundlegende Sicherheitsmaßnahme, die verhindert, dass Angreifer Backup-Daten verschlüsseln oder löschen können

*Arcserve 2026 Market Study

Unternehmensdaten in immutable Speicher schützen

Finanzdaten

Kundendaten

Geistiges Eigentum

(Intellectual property)



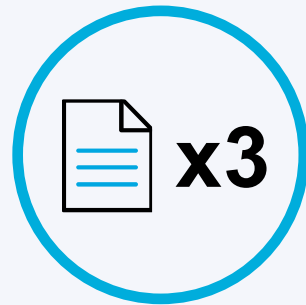
Regulatorische und
Compliance Dokumente

Betriebs- und
Prozessdaten

Mitarbeiterdaten

Backup-Konzepte benötigen eine 3-2-1-1-0-Strategie

Moderne Best Practices für Datensicherung basieren heute auf dem 3-2-1-1-0-Prinzip:



3 Kopien Ihrer Daten erstellen
(1 Produktivkopie und 2 Backup-Kopien)



2 Kopien lokal speichern – auf mindestens 2 unterschiedlichen Speichermedien (lokale Festplatte, NAS, Tape, etc.)



1 Kopie extern speichern (in sicherem Offsite-Storage oder in der Cloud etc.)



1 Kopie in unveränderbarem („immutable“) Speicher ablegen (Object Lock, WORM Medien, Air-Gap-Lösungen)



Zero Backup Fehler (durch automatische Verifizierung erfolgreicher Backups mit UDP Assured Recovery)

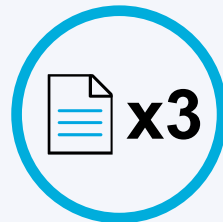
Herausforderungen bei der Einführung von Immutable Storage



Herausforderungen bei der Einführung von Immutable Storage mit Arcserve lösen



Unterstützung bei der Umsetzung der 3-2-1-1-0-Backup-Strategie



3 Kopien Ihrer Daten



2 unterschiedliche Speichermedien



1 extern gespeicherte Kopie

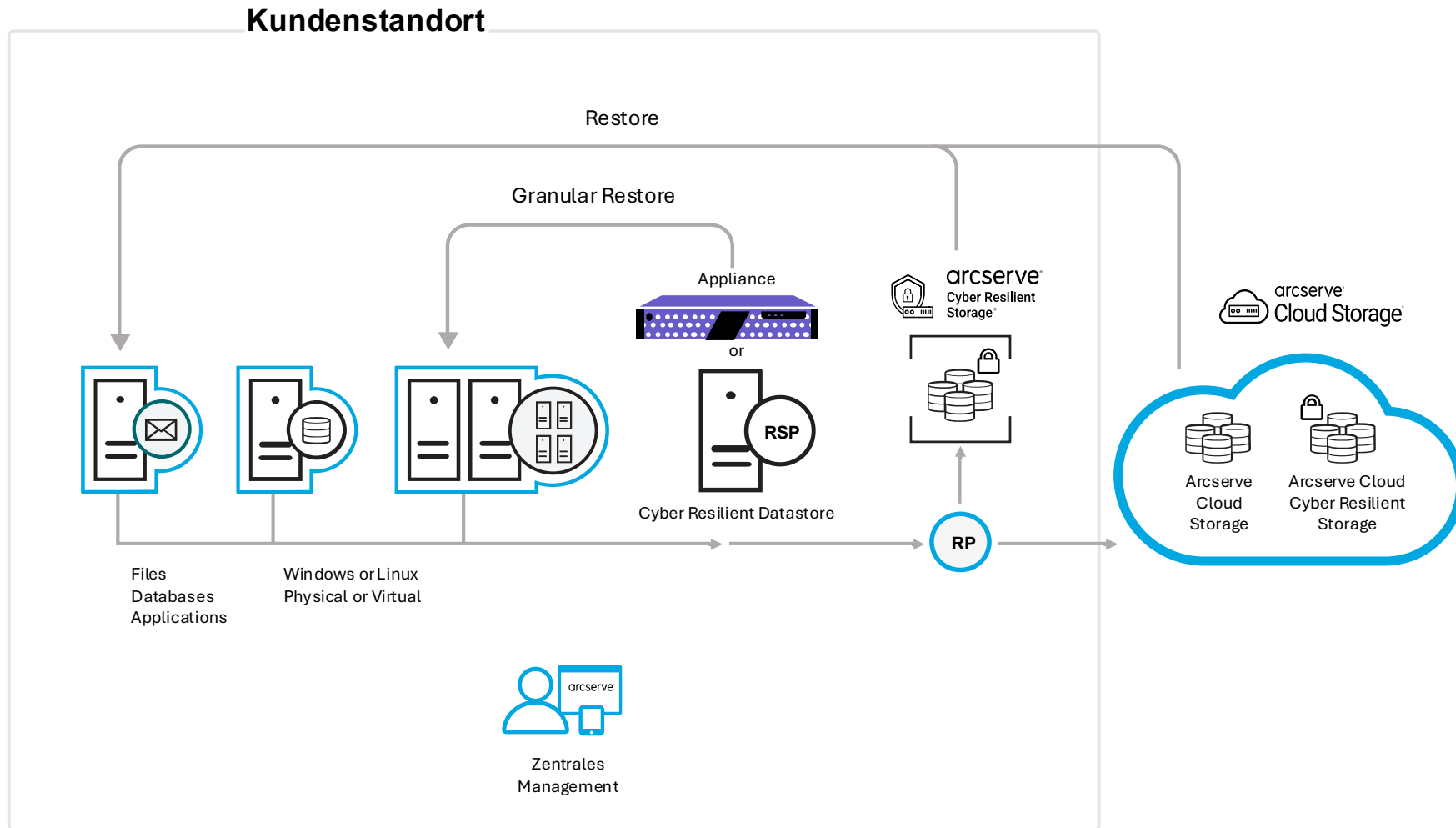


1 Kopie auf immutable Speicher



0 Fehler bei der Wiederherstellungsprüfung

Immutable Backups schützen geschäftskritische Daten



84%

der Partner bestätigen, dass
Arcserve fortschrittliche
Ransomware-
Schutzlösungen bereitstellt,
die die Cyber-Resilienz ihrer
Kunden erhöhen.*

Arcserve: Globaler Marktführer für Data Resilience

Schutz von Daten vor Ransomware, Cyberangriffen und Ausfällen – durch intuitive, flexible und kosteneffiziente Datenschutzlösungen, die speziell für kleine und mittelständische Unternehmen entwickelt wurden.



9

Unterstützte Sprachen

150+

Länder

10,000+

VAR und MSP partners

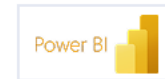
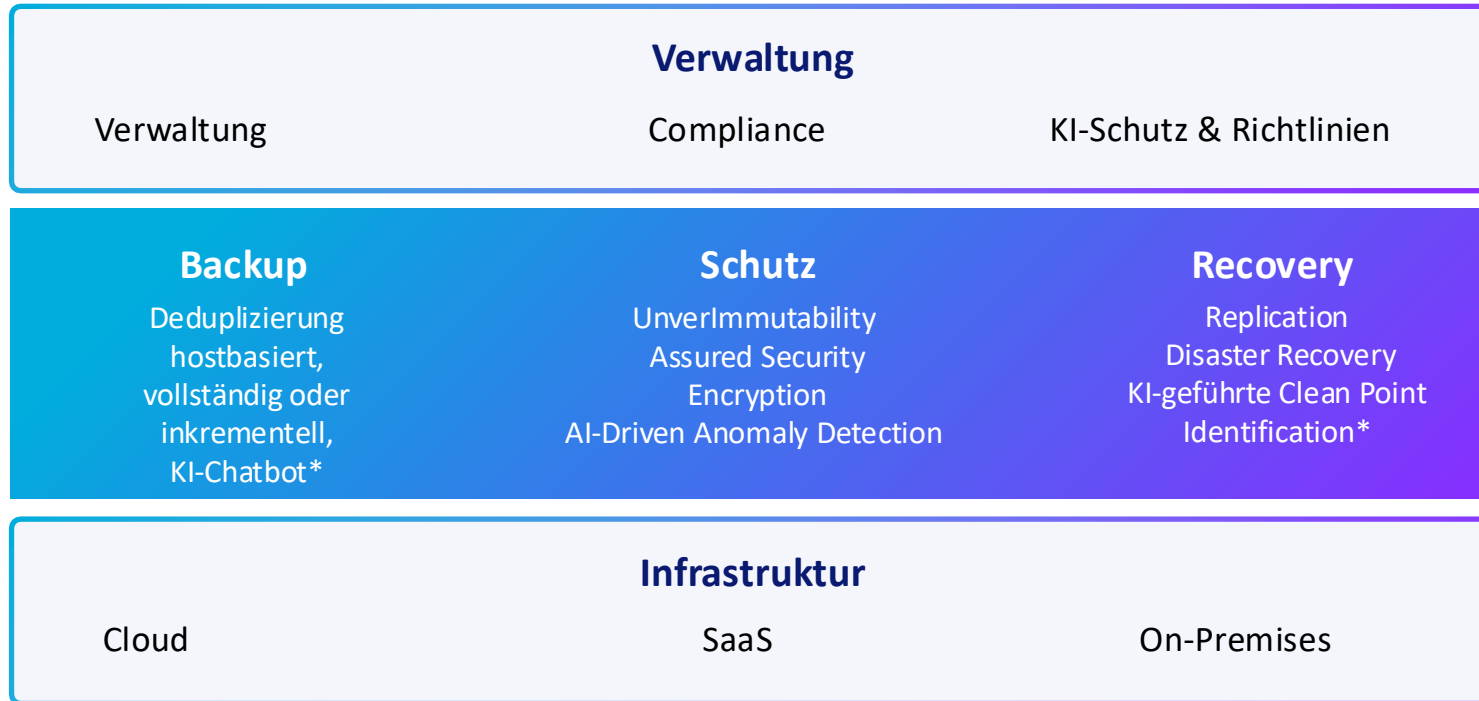
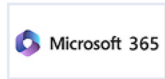
50,000+

Kunden



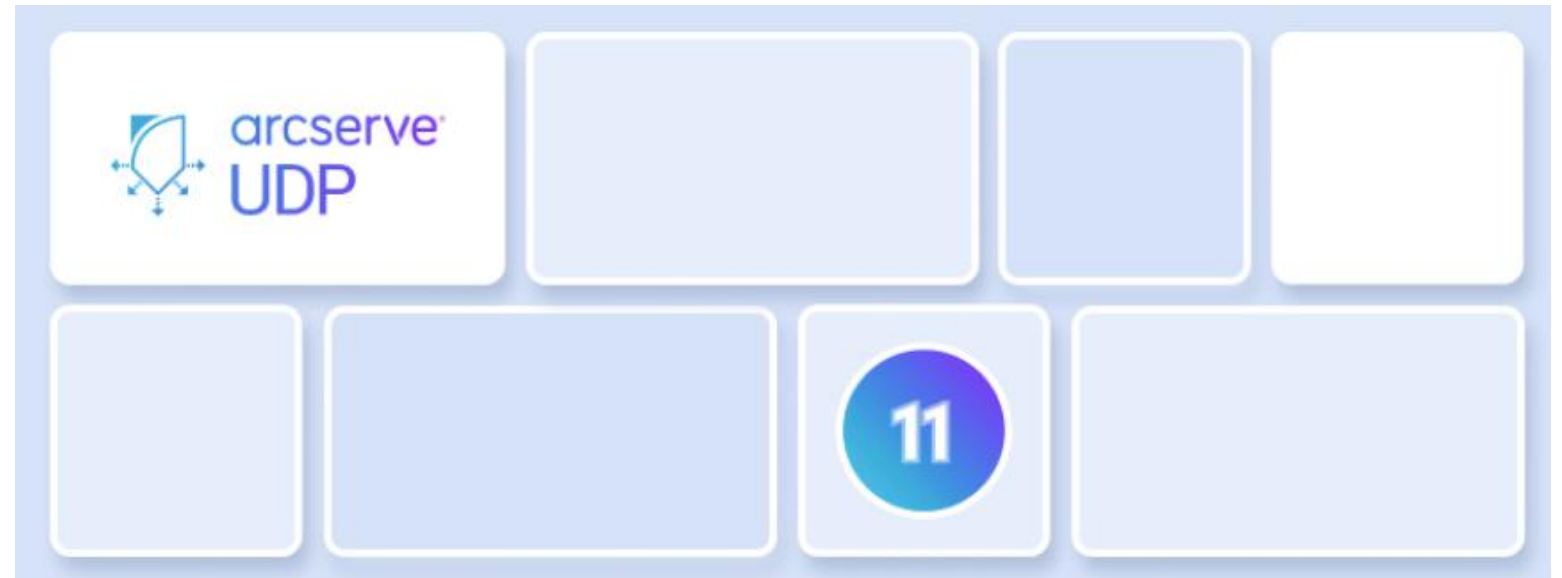
*ITR Market View

Arcserve: einfach, flexibel, erschwingliche Datenresilienz



*Erscheint 2026

UDP 11: Data Resilience für das KI-Zeitalter



Globales Online-Launch-Event 11. Juni | 17:00 Uhr CET

- **Wie KI und Ransomware die Anforderungen an moderne Data Resilience verändern**
- **Neue Funktionen für schnellere und sicherere Recovery-Prozesse**
- **Einblicke in aktuelle Trends aus dem „State of Data Resilience 2026“-Report**
- **Praxisbeispiele und Best Practices für Cyber-Resilienz**
- **Live-Demos und technische Sessions**

Seien Sie auf Ransomware vorbereitet: Setzen Sie schon heute auf Immutable Storage

**On-premises Immutable
Storage**



[30-day Free Trial](#)

Cloud Immutable Storage



[30-day Free Trial](#)

**Arcserve UDP – Data
Resilience Platform**



[30-day Free Trial](#)

**Arcserve UDP 11 Event
June 11**



[Jetzt anmelden \[ENG\]](#)