OBJECT FIRST

White Paper

Zero Trust und Datensicherung im Unternehmen

Zero Trust als Grundlage für Datenresilienz

Zero Trust: Datensicherung und Wiederherstellung

Das Zero-Trust-Modell hat sich als Best Practice für Unternehmen etabliert, die ihre Daten und ihr Business schützen möchten. Im Bereich Datensicherung und Wiederherstellung findet es jedoch bislang kaum Anwendung. Das auf Zero Trust spezialisierte Beratungsunternehmen Numberline Security und Veeam haben gemeinsam ein neues Modell entwickelt, das diese Lücke schließt und Risiken für Unternehmen mindert, in denen Perimetersicherheit nicht mehr ausreicht: das Modell der Zero-Trust-Datenresilienz (ZTDR).

Zero-Trust-Datenresilienz basiert auf dem Zero-Trust-Reifegradmodell (Zero Trust Maturity Model, ZTMM) der Cybersecurity and Infrastructure Security Agency (CISA) und weitet die ZTMM-Prinzipien auf die Datensicherung und Wiederherstellung aus.

Das Zero-Trust-Datenresilienz-Framework bietet praxisnahe Orientierungshilfe für IT- und Sicherheitsteams, die den Datenschutz optimieren, Sicherheitsrisiken minimieren und die Cyberresilienz des Unternehmens verbessern möchten.

Ziel von Cyberangriffen und Ransomware-Attacken sind in 93 % der Fälle Backup-Daten.

Backup-Daten sind häufig das primäre Ziel von Ransomware- und Datenexfiltrationsangriffen. Bestehende Zero-Trust-Frameworks sind jedoch nicht auf die Sicherheit von Systemen zur Datensicherung und Wiederherstellung ausgelegt.

Das Original-Whitepaper „Zero Trust Data Resilience – A Secure Data Backup and Recovery Model“ kann hier heruntergeladen werden:

https://go.veeam.com/zero-trust-data-resilience

Zero-Trust-Prinzipien

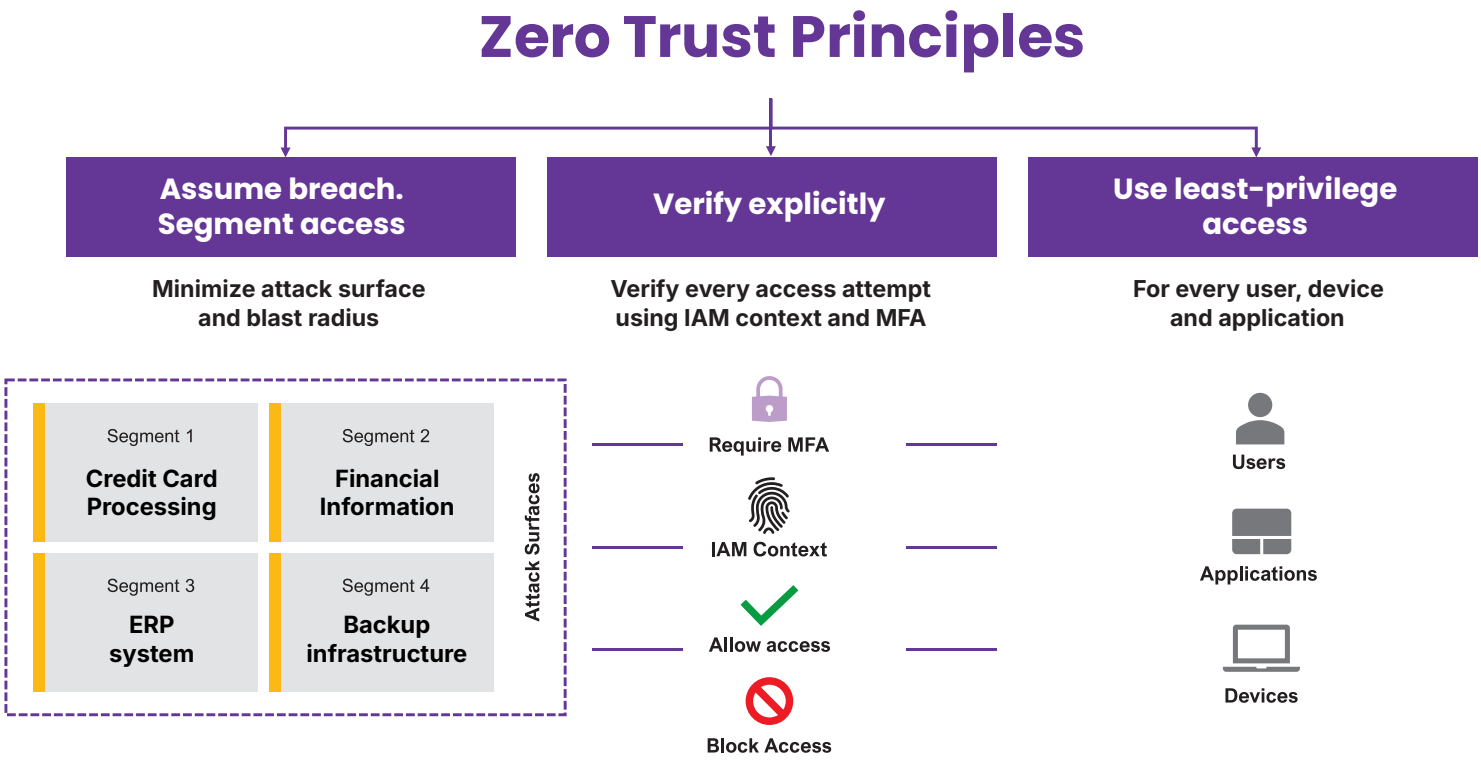
Zero Trust ist ein Sicherheitsparadigma, das den herkömmlichen Ansatz der Perimetersicherheit ablöst. Dieser wird modernen Sicherheitsanforderungen immer weniger gerecht. US-Behörden und Unternehmen weltweit implementieren Zero Trust, um ihre Systeme und Daten nach dem führenden IT-Sicherheitsstandard zu schützen.

Zero Trust kann von Unternehmen jeder Größe und aller Branchen sowohl in On-Premise- als auch in Cloud- und hybriden Umgebungen genutzt werden.

Zero Trust basiert auf diesen Grundprinzipien:

- **Erwarten eines Angriffs:** Segmentieren des Zugriffs auf besonders wichtige Daten, um die Angriffsfläche und den Angriffsradius für die einzelnen Segmente zu minimieren
- **Explizite Verifizierung:** Authentifizierung und Autorisierung mithilfe des Kontexts der Identitäts- und Zugriffsverwaltung (Standort, Uhrzeit usw.) und mit einem sicheren MFA-Verfahren
- **Zugriff nach dem Prinzip der geringsten Rechte** für alle Benutzer, Geräte und Anwendungen

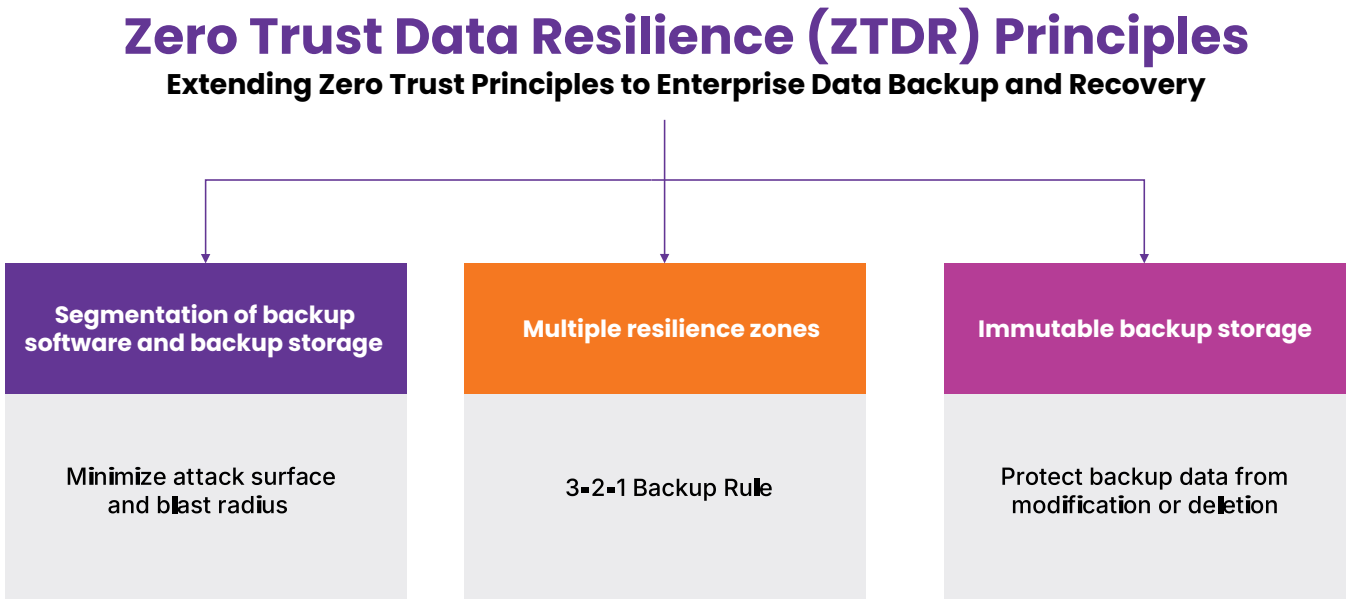
Das Zero-Trust-Modell setzt darüber hinaus eine kontinuierliche Sicherheitsüberwachung und -analyse, Automatisierung und Orchestrierung sowie Governance für das Lebenszyklusmanagement von Daten voraus.



Prinzipien der Zero-Trust-Datenresilienz (ZTDR)

Mit den folgenden Prinzipien der Zero-Trust-Datenresilienz lässt sich Zero Trust auf die Sicherung und Wiederherstellung von Unternehmensdaten ausweiten:

- **Segmentierung: Trennung zwischen der Backup-Software und dem Backup-Speicher** zur Durchsetzung des Prinzips der geringsten Rechte und zur Minimierung der Angriffsfläche und des Angriffsradius
- **Einrichtung mehrerer Datenresilienzzonen oder Sicherheitsdomänen** zur Einhaltung der **3-2-1-Regel für Backups** und zur Gewährleistung mehrstufiger Sicherheit
- **Immutable Backup-Speicher** zum Schutz von Backup-Daten vor Änderungen und Löschungen **Keine Administratorrechte und kein Zugriff auf das Betriebssystem** zum Schutz vor externen Angreifern und kompromittierten Administratorkonten und zur Gewährleistung **echter Immutability**



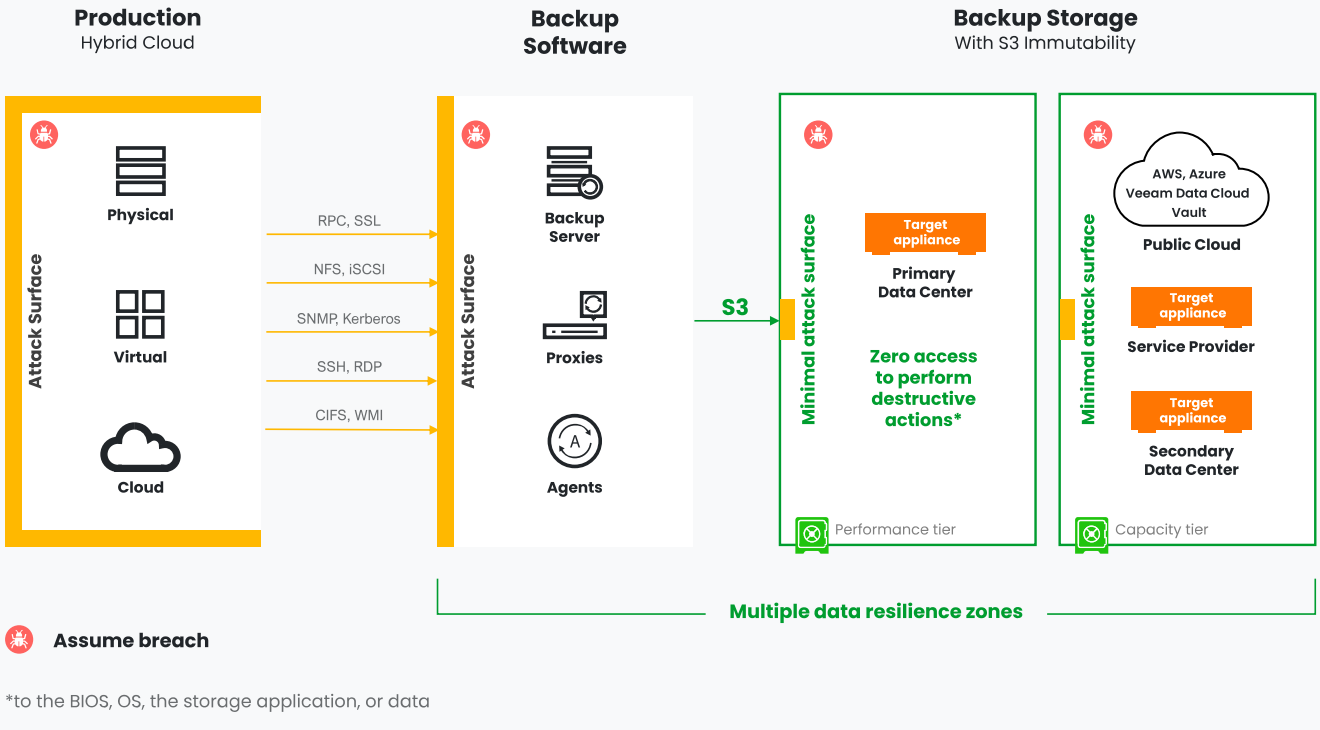
Trennung zwischen Backup-Software und Backup-Speicher

Die Backup-Infrastruktur weist naturgemäß eine große Angriffsfläche auf, da sie Lese- und Schreibzugriff auf die Produktivsysteme für alle Unternehmensanwendungen und Datenquellen sowohl in On-Premise- als auch in Hybrid-Cloud-Umgebungen benötigt. Um dieses Risiko zu mindern, erfordert Zero-Trust-Datenresilienz die Segmentierung der Backup-Infrastruktur in verschiedene Resilienzzonen (z. B. Backup-Software, primärer Backup-Speicher und sekundärer Backup-Speicher). Für diese Zonen gilt jeweils das Prinzip der geringsten Rechte, sodass sich die Angriffsfläche und der Angriffsradius verringern. Dabei kann die Backup-Software weiterhin eine exponierte Angriffsfläche aufweisen, während die des Backup-Speichers minimiert ist. Erreicht wird dies durch Zero-Trust-Zugriffssteuerung und ein sicheres Kommunikationsprotokoll wie S3 über HTTPS, um das Risiko einer Penetration des Backup-Speichers zu mindern (siehe **Abbildung 1**).

Abbildung 1

Architektur mit Zero-Trust-Datenresilienz (ZTDR)

Trennung zwischen Backup-Software und Backup-Speicher



*to the BIOS, OS, the storage application, or data

Mehrere Datenresilienzzonen

Ein Grundkonzept von Zero Trust für das Networking ist die Mikrosegmentierung, mit der Sicherheitsperimeter in kleinere Zonen aufgebrochen werden. Ziel ist es, einen Zugriff nach dem Prinzip der geringsten Rechte durchzusetzen sowie den Angriffsradius kompromittierter Zonen zu verringern und die laterale Ausbreitung von Angriffen zu verhindern.

Dieses Konzept kann durch die Einrichtung mehrerer Datenresilienzzonen umgesetzt werden. Resilienzzonen trennen den Backup-Speicher von der Backup-Software und isolieren die Steuerungsebene des Speichers von der Backup-Software und deren Steuerungsebene.

Dadurch entsteht eine wichtige Demarkationslinie, die dafür sorgt, dass die Back-Daten intakt bleiben und wiederhergestellt werden können – selbst wenn die Backup-Software kompromittiert wird. Eine solche Kompromittierung kann viele Ursachen haben, beispielsweise auch interne Angreifer. Ein Backup-System muss sicherstellen, dass sich die Backup-Daten über eine saubere Installation der Backup-Software schnell und einfach wiederherstellen lassen. Durch Einrichtung verschiedener Datenresilienzzonen können Unternehmen eine wirksame mehrstufige Sicherheitsstrategie umsetzen und die 3-2-1-Regel für Backups befolgen.

3-2-1 Regel für Backups

Immutable Backup-Speicher

Gemäß dem ZTDR-Modell müssen gesicherte Daten auch immutable – also unveränderlich – sein, damit sie im Falle eines Ransomware-Angriffs nicht geändert oder gelöscht werden können. Von maximaler Datenresilienz profitieren Kunden mit einem gehärteten Immutable-Storage-Ziel mit Compliance-Modus und ohne Administratorrechte oder Zugriff auf das Betriebssystem. Ein solches Storage-System kann anbieterspezifische Lösungen und Protokolle oder Standardprotokolle wie S3 beinhalten.

S3-native Immutability und Sicherheit

S3 bietet hochgradig zuverlässige Immutability nach Branchenstandard, Sicherheit, Identitäts- und Zugriffsverwaltung sowie ein sicheres Kommunikationsprotokoll.

Offenes Design und offene Architektur

Ein offenes Design und eine offene Architektur sind allgemeine Grundprinzipien der IT-Sicherheit. Der Einsatz des Standardprotokolls S3 anstelle eines proprietären Protokolls wird diesen Prinzipien am besten gerecht.

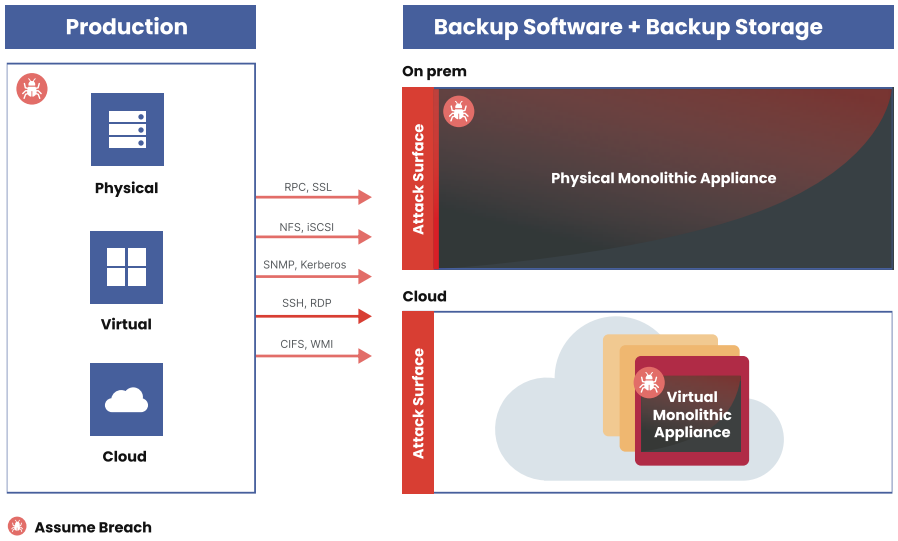
Ein Datensicherungs- und Wiederherstellungssystem mit solider Architektur zeichnet sich durch eine Segmentierung zwischen den Ebenen Backup-Management-Software und Backup-Speicher aus. Diese Segmentierung ist entscheidende Voraussetzung für die Resilienz, Immutability und Flexibilität, die Unternehmen benötigen. Sie verringert die Angriffsfläche und sorgt für mehrstufige Sicherheit, wodurch das Risiko einer Datenschutzverletzung deutlich gemindert wird.

Monolithische Appliance: kein Zero Trust

Alternative Architekturen wie monolithische Appliances erfüllen die Anforderungen von Zero-Trust-Datenresilienz nicht, da Backup-Software und Backup-Speicher nicht voneinander getrennt sind. Eine solche Architektur bietet keine echte Immutability, da Angreifer bei einer Kompromittierung vollständigen Zugriff auf die Backup-Software und den Backup-Speicher haben. Sie wären damit in der Lage, Backup-Daten zu ändern, zu löschen oder unzugänglich zu machen. Mit anderen Worten: Der Radius eines Angriffs würde auch das gesamte Datensicherungs- und Wiederherstellungssystem beinhalten (siehe **Abbildung 2**). Dieser Ansatz setzt außerdem großes Vertrauen in die Immutability des Dateisystem des Anbieters voraus.

Abbildung 2

Monolithische Appliance in On-Premise und Cloud-Umgebungen – kein Zero Trust



- **Erwarten eines Angriffs** auf die physische Appliance oder Cloud-Instanz
- **Keine echte Immutability** bei einem Angriff
- **Keine Trennung** zwischen Backup-Software und Backup-Speicher
- **Angriffsradius umfasst die gesamte Appliance**

Wichtig ist in diesem Zusammenhang auch, dass die Bereitstellung einer monolithische virtuellen Appliance in einer Cloud-Instanz keine echte Immutability in einem Hybrid-Cloud-Szenario gewährleisten kann. Werden bei einem Angriff Anmeldeinformationen für das Betriebssystem, die Instanz oder ein Konto kompromittiert, ist die gesamte virtuelle Appliance Risiken ausgesetzt. Dadurch vergrößert sich der Angriffsradius. Das Sicherheitsrisiko entsteht dadurch, dass Daten auf dem proprietären Speichersystem der cloudbasierten virtuellen Appliance gesichert werden. Diese Schwachstelle – die durch eine Architektur verursacht wird, die nicht den Prinzipien der ZTDR entspricht – könnte durch die Sicherung der Daten direkt auf Immutable Cloud-Objektspeicher außerhalb der Instanz behoben werden.

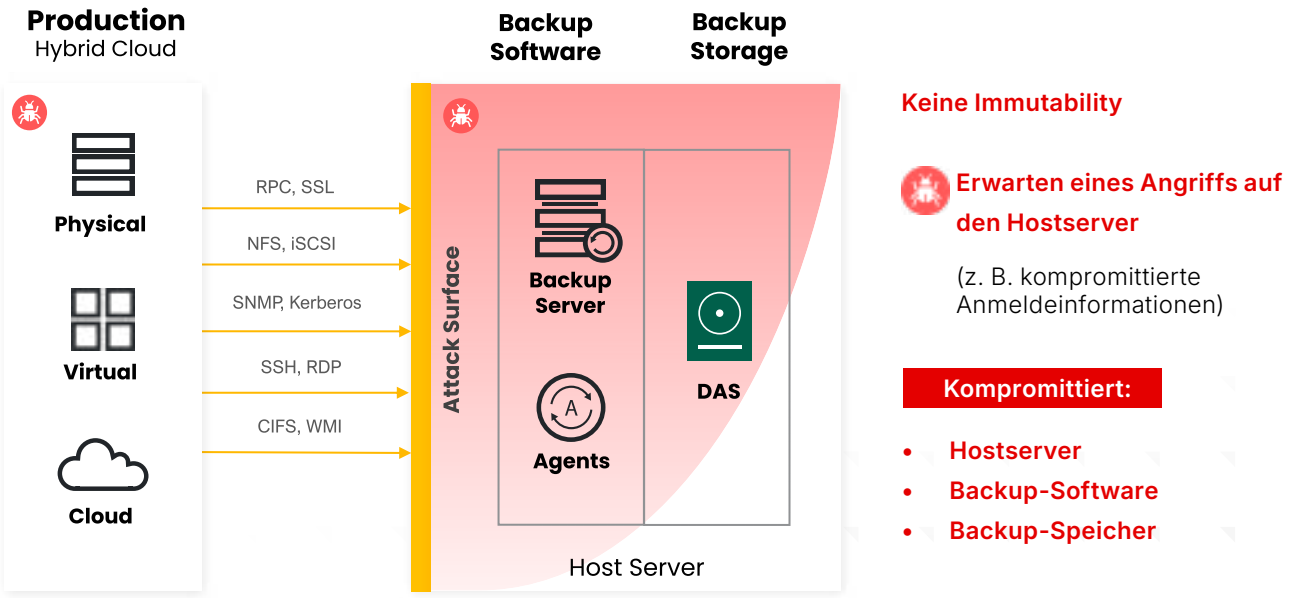
Direct Attached Storage (DAS): kein Zero Trust

Direct Attached Storage (DAS) bietet keine Immutability und ist direkt mit dem Veeam Backup & Replication-Server verbunden. Backup-Software und Backup-Speicher sind nicht voneinander getrennt. Verschafft sich ein Angreifer Zugriff auf den Host, indem er eine Schwachstelle im Betriebssystem oder in einer Anwendung ausnutzt, kann er auf alle Daten auf diesem System zugreifen (siehe **Abbildung 3**).

Abbildung 3

DAS – Direct Attached Storage

KEIN Zero Trust und keine Trennung zwischen Backup-Software und Backup-Speicher



Fazit

Angesichts der wachsenden Zahl von Cyberbedrohungen liegt es auf der Hand, dass herkömmliche Sicherheitsmaßnahmen nicht mehr ausreichen. Eine wichtige Voraussetzung für mehr Cyberresilienz ist die Umsetzung eines Zero-Trust-Ansatzes. Zwar wenden immer mehr Unternehmen die Prinzipien von Zero Trust an, um ihre Daten besser zu schützen und Ausfallzeiten zu verringern, doch deckt das bislang vorherrschende Zero-Trust-Reifegradmodell (ZTMM) die Sicherung und Wiederherstellung von Unternehmensdaten nicht ab.

Zero-Trust-Datenresilienz (ZTDR) ist ein neues Modell, dass die Prinzipien von Zero Trust auf das Anwendungsszenario der Datensicherung und Wiederherstellung überträgt. Die Grundprinzipien von ZTDR umfassen die Trennung zwischen Backup-Software und Backup-Speicher, die Einrichtung mehrerer Resilienzzonen zur Einhaltung der 3-2-1-Regel für Backups und Immutable Backup-Speicher zum Schutz von Daten vor Änderungen und Löschungen. Object First setzt diese Best Practices um und stellt leistungsfähige Speicherlösungen bereit, mit denen sich echte Zero-Trust-Datenresilienz erreichen lässt.

Durch Implementierung eines ZTDR-Modells können Unternehmen klar definierte und konkrete Maßnahmen zur Verbesserung der Sicherheit ergreifen. Sie profitieren dadurch von effizienteren Abläufen und einer besseren Abstimmung ihrer IT- und Sicherheitsteams, sodass sie im Falle eines Angriffs ihre Daten schnell und sicher wiederherstellen können.

1.0_20251118

OBJECT FIRST