OBJECT FIRST

Whitepaper

Absolute Immutability

Der ultimative Ransomware-Schutz

Immutable Backup-Storage Ihre einzige Garantie für die Wiederherstellung nach einem Ransomware-Angriff

Ransomware hat sich zur größten Bedrohung für die Cybersicherheit entwickelt: 66 % der Unternehmen sind in den vergangenen zwei Jahren mindestens einmal Opfer eines Ransomware-Angriffs geworden. Diese Angriffe können verheerende Folgen haben und sind somit nicht mehr nur ein „IT-Problem“, sondern müssen zur Chefsache von CIOs, CEOs und Vorstandsmitgliedern werden. Denn sie tragen die unternehmerische und zunehmend auch die rechtliche Verantwortung für die Aufrechterhaltung des Geschäftsbetriebs.

Um sich vor Ransomware zu schützen, müssen Unternehmen eine moderne, mehrstufige Cybersicherheitsstrategie entwickeln, die auf Zero-Trust-Prinzipien basiert. Hierzu gehört auch die Implementierung umfangreicher Tools und Lösungen für Firewalls, Malware-Erkennung, Bedrohungserkennung, Zugriffssteuerung, die erweiterte Erkennung und Abwehr auf Endgeräten und vieles mehr.

Die ungeschminkte Wahrheit lautet jedoch: Kein System ist eine uneinnehmbare Festung, ganz gleich, welches Bollwerk Sie errichtet haben. Deshalb sind zwei Dinge wichtig: dass Sie Angriffe erwarten und sich für eine Wiederherstellung rüsten.

Die einzige Garantie für die Wiederherstellung nach einem Ransomware-Angriff besteht darin, rundum zuverlässige Backups vorzuhalten. In diesem Whitepaper stellen wir ein neues Konzept vor: „Absolute Immutability“. Nach diesem Konzept können Daten unter keinen Umständen geändert oder gelöscht werden. Dadurch wird sichergestellt, dass Ihre Daten selbst bei einer Kompromittierung der Produktiv- und Datensicherungssysteme geschützt bleiben.

Ohne absolute Immutability sind viele Unternehmen Angriffen schutzlos ausgesetzt. Obwohl inzwischen 96 % der Ransomware-Angriffe nicht nur auf Primärsysteme, sondern auch auf Backups abzielen, nutzen 41 % der Unternehmen keinen Immutable Storage für ihre Backup-Daten.

Dieses Whitepaper zeigt auf, wie Unternehmen mit absoluter Immutability von ultimativem Ransomware-Schutz profitieren Business- und IT-Verantwortliche finden darin außerdem praktische Ratschläge, wie sie durch Einführung dieses Konzepts ihr Unternehmen resilienter machen können.

50%

der Unternehmen benötigten für die Wiederherstellung nach einem Ransomware Angriff mehr als sechs Tage*

96%

der Ransomware-Angriffe zielen nicht nur auf Primärsysteme, sondern auch auf Backups ab*

41%

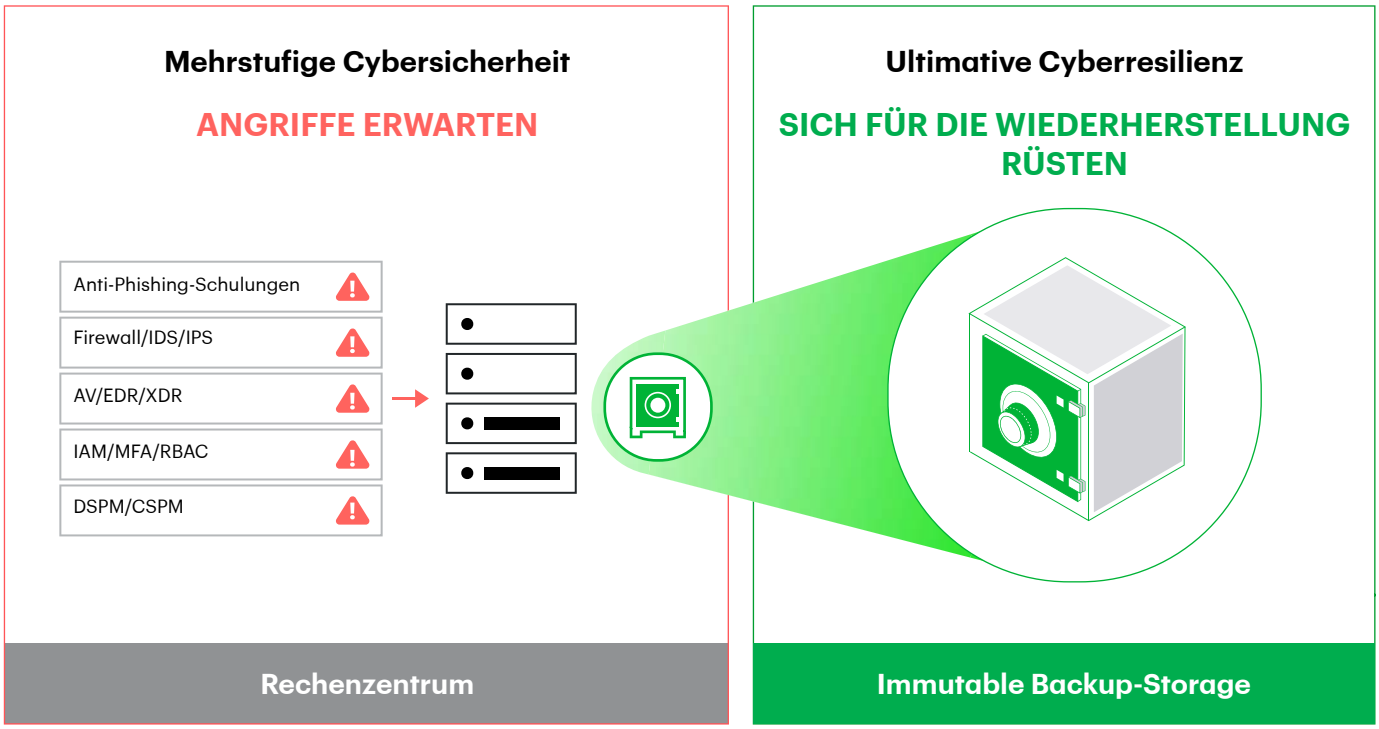
der Unternehmen nutzen derzeit keinen Immutable Storage*

*Studie von ESG, 2025

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Absolute Immutability

Immutable Backup-Storage – der ultimative Ransomware-Schutz



Bei einem Angriff – und ein solcher wird über kurz oder lang unvermeidbar sein – stehen Ihr Unternehmen, Ihr Ruf und Ihre Karriere auf dem Spiel. Deshalb ist Immutable Backup-Storage Ihr ultimativer Ransomware-Schutz.

Wichtige Konzepte

Was ist Immutability?

Einfach definiert bedeutet Immutability, dass Daten nach der Speicherung nicht mehr geändert oder gelöscht werden können. So lassen sich kritische Daten zuverlässig schützen. Diese Definition berücksichtigt jedoch nicht, wie komplex die Implementierung von Immutability ist und welche nicht unmittelbar erkennbaren Ausnahmen und Hintertüren es gibt. Deshalb müssen Unternehmen ABSOLUTE Immutability sicherstellen.

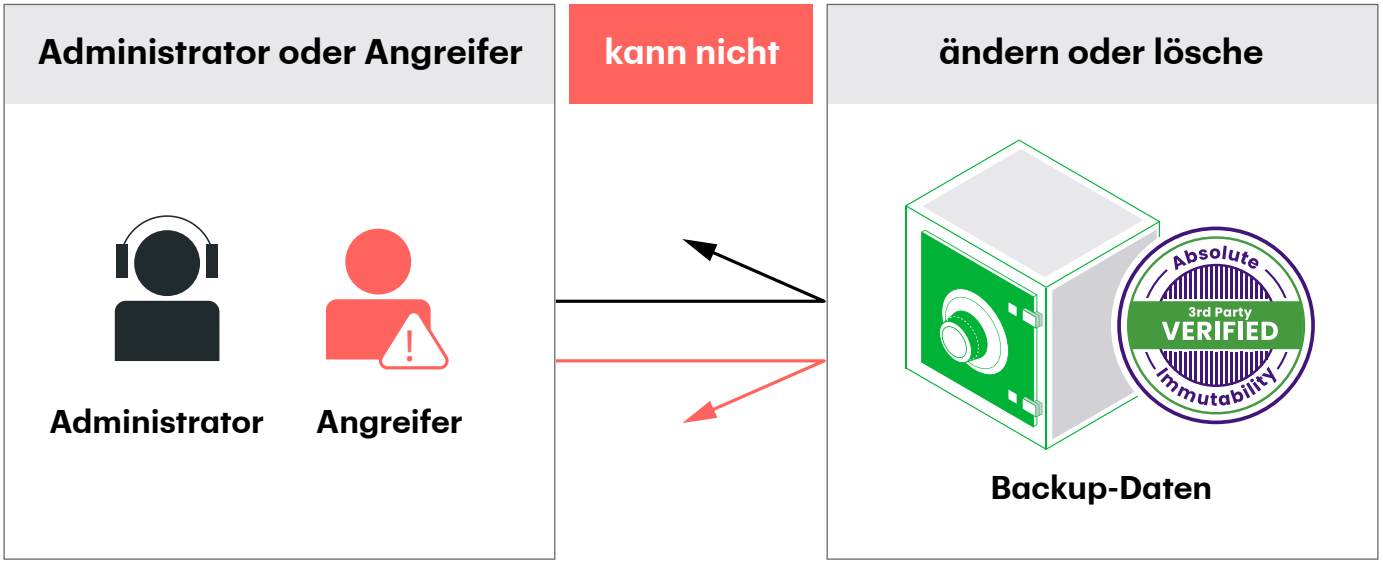
Was ist ABSOLUTE Immutability?

Absolute Immutability bedeutet, dass selbst Administratoren mit weit gefassten Rechten oder Angreifer mit Zugriff auf den Backup-Storage Ihre Daten nicht ändern oder löschen können. Dies kann nur mit einem Backup-Storage-System erreicht werden, das das Prinzip „Security by Design“ unterstützt und keinerlei Zugriff gewährt, über den schädliche Aktionen möglich sind (Zero Access). Dabei muss im Rahmen von Tests durch Dritte überprüft werden können, dass tatsächlich kein Zugriff möglich ist.

Warum ist das so wichtig? Weil nicht alle Lösungen, die Immutability versprechen, diese auch tatsächlich gewährleisten. Das werden wir noch unter Beweis stellen

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Absolute Immutability:
Keinerlei Zugriff auf schädliche Aktionen
Tests und Überprüfung durch Dritte



Von Zero Trust zu Zero Access

Bei einem Angriff werden die Anmeldeinformationen oder Berechtigungen vom Angreifer kompromittiert, z. B. durch Phishing, Social Engineering oder Ausnutzung von Zero-Day-Sicherheitslücken.

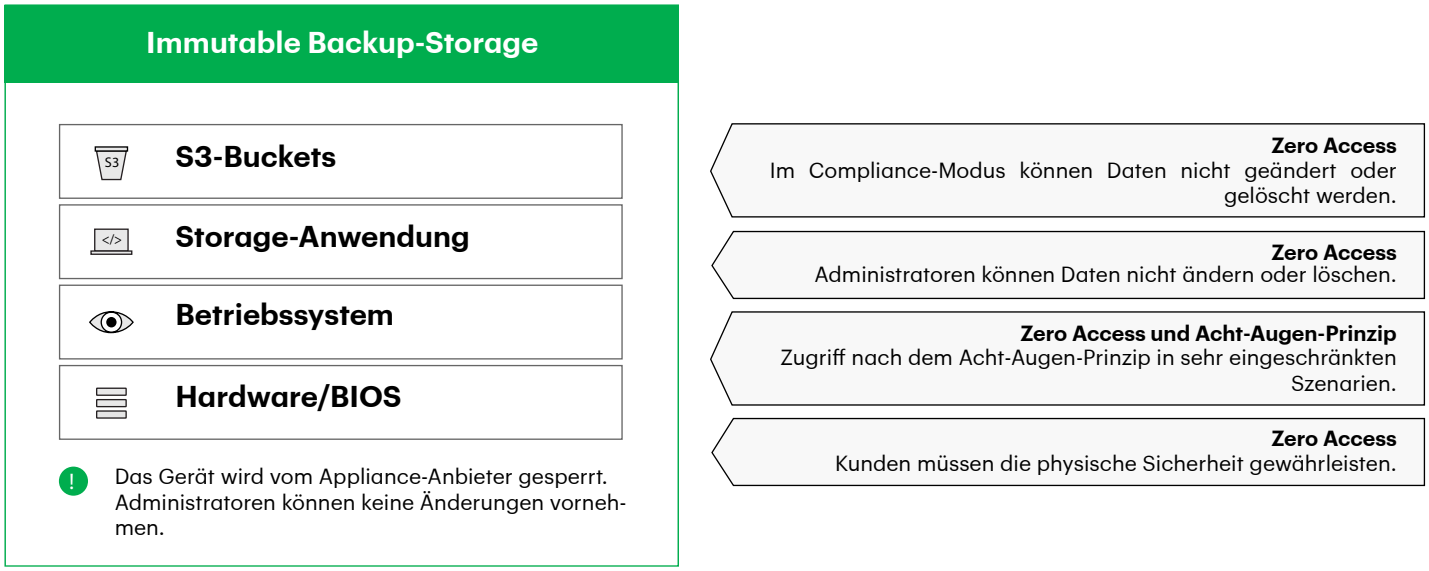
Der Zugriff nach dem Prinzip der geringsten Rechte, einer der Grundpfeiler von Zero Trust, schränkt die Administratorrechte ein. Zero Access (keinerlei Zugriff) geht noch einen Schritt weiter und sorgt dafür, dass Administratoren keine schädlichen Aktionen durchführen können. Dadurch werden Daten vor Angreifern mit Administratorrechten oder Insidern mit unlauterer Absicht geschützt.

Im Fall von Backup-Appliances mit S3-Objektspeicher wird dieser Schutz durch Zero Access wie folgt gewährleistet:

- Im Compliance-Modus können keine Buckets oder Objekte gelöscht werden.
- Der Zugriff auf das Betriebssystem und Backup-Storage-Anwendungen auf der Root-Ebene wird blockiert, sodass Immutability-Einstellungen nicht außer Kraft gesetzt werden können.
- Weder Kunden noch Anbieter haben die Möglichkeit, einseitig eine Zurücksetzung auf die Werkseinstellungen vorzunehmen. Dadurch wird eine vollständige Datenlöschung auf dem System vermieden.
- Der BIOS-Zugriff wird auf Änderungen des physischen Systems beschränkt, sodass keine Manipulation von Boot-Prozessen oder Sicherheitseinstellungen möglich ist.
- Es können ausschließlich Serviceverfahren und Firmware- und Software-Updates ausgeführt werden, die vom Anbieter bereitgestellt werden. Auch dabei werden durch Zero Access schädliche Aktionen verhindert

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Zero Access für den gesamten Backup-Storage



Acht-Augen-Prinzip

Anbieter, die das Zero-Access-Prinzip umsetzen, implementieren auch Genehmigungsprozesse mit mehreren Personen, um einseitige schädliche Aktionen wie das Zurücksetzen von Geräten, das Ändern von Sicherheits- oder Aufbewahrungseinstellungen oder ungewöhnliche Servicevorgänge zu verhindern. Viele befolgen bereits das Vier-Augen-Prinzip, das vorsieht, dass zwei Personen – ein Mitarbeiter des Kunden und ein Mitarbeiter des Anbieters – wichtige Vorgänge wie die oben genannten genehmigen. Die Überprüfung bleibt jedoch in der Regel Mitarbeitern auf Kundenseite überlassen. Dies birgt das Risiko, dass kompromittierte Anmeldedaten von Administratoren zur Umgehung des Prozesses verwendet werden könnten.

Bei Immutable Backup-Storage empfiehlt sich eine Erweiterung auf das Acht-Augen-Prinzip. Dabei sind beim Kunden und beim Anbieter jeweils zwei Mitarbeiter erforderlich, um die Rechtmäßigkeit einer potenziell schädlichen Aktion vor deren Ausführung sicherzustellen. Die Identitätsüberprüfung muss außerdem durchgesetzt werden, bevor endgültige Entscheidungen mit Auswirkungen auf die Sicherheit getroffen werden.

Praktische Umsetzung

Um durch Zero Access absolute Immutability zu gewährleisten, müssen drei Grundprinzipien befolgt werden:

Absolute Immutability	Ungeprüfte Immutability
1. S3-Objektspeicher	Proprietärer Storage
2. Sofortige Immutability	Zeitlich verzögerte Immutability Snapshot-basierte Immutability
3. Zielspeicher-Appliance	Integrierte Appliance Deduplizierungs-Appliance Selbst verwaltetes System Selbst entworfenes Speichersystem

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

1. S3-Objektspeicher

Nur S3-Objektspeicher bietet integrierte Sicherheit mit nativer Immutability, die direkt in das Protokoll und die APIs eingebettet ist.

Mit diesem Design wird sichergestellt, dass Daten nach dem Speichern nicht mehr geändert oder gelöscht werden können. Herkömmliche Block- und Dateispeichersysteme bieten hingegen keine native Immutability und greifen stattdessen auf proprietäre, nachträglich hinzugefügte Lösungen zurück.

S3-Objektspeicher basiert auf einer offenen Architektur nach Branchenstandard, die sich an Best Practices für die IT-Sicherheit orientiert. Im Gegensatz zu proprietären Systemen, die mit Verschleierung arbeiten und nicht unabhängig überprüft werden können, sorgt S3 durch offene Standards für Transparenz. Dieser Ansatz erhöht die Sicherheit, verbessert die Kompatibilität und langfristige Zuverlässigkeit und ermöglicht eine nahtlose Integration in moderne Datensicherungslösungen wie Veeam.

S3-Objektspeicher wird in einer Vielzahl von Branchen erfolgreich eingesetzt. Seine Funktionalität wird in Implementierungen bei Kunden und Tests durch Dritte laufend überprüft, sodass Unternehmen von einem Höchstmaß an Sicherheit und Zuverlässigkeit profitieren.

Mit seinen nativen Funktionen, dem offenen Design und Immutability auf Protokollebene ist S3-Objektspeicher die einzige Lösung, die absolute Immutability gewährleisten kann und damit die Grundlage für eine resiliente, überprüfbare Backup-Speicherstrategie bildet

Object Lock und Versionsverwaltung

Object Lock sorgt dafür, dass gespeicherte Objekte für die Dauer eines definierten Aufbewahrungszeitraums nicht geändert oder gelöscht werden können. Selbst wenn die Anmeldedaten für einen Bucket kompromittiert werden, lassen sich Daten nicht ändern oder löschen.

Zugleich werden durch die Versionsverwaltung mehrere Iterationen der unveränderlichen Daten aufbewahrt. Dadurch stehen mehrere Wiederherstellungspunkte zur Verfügung und frühere Versionen lassen sich nach einem Cyberangriff sicher überprüfen, um zu ermitteln, wann und wo der Angriff erfolgte.

Compliance-Modus

S3-Objektspeicher unterstützt zwei Immutability-Mechanismen: den Compliance-Modus und den Governance-Modus. Im Compliance-Modus werden die Aufbewahrungszeiträume strikt durchgesetzt, sodass selbst Administratoren Daten erst nach Ablauf dieses Zeitraums ändern oder löschen können.

Dies gewährleistet absolute Immutability. Der Governance-Modus hingegen bringt schwerwiegende Sicherheitsrisiken mit sich und sollte deshalb vermieden werden. Zwar ermöglicht er eine flexible Verwaltung, doch können privilegierte Benutzer in diesem Modus die Object-Lock-Einstellungen außer Kraft setzen. Dadurch kann der Immutability-Schutz verkürzt oder ausgesetzt werden. Wenn sich ein Angreifer Administratorzugriff verschafft – beispielsweise über kompromittierte Anmeldedaten oder Insider-Aktionen – kann er im Governance-Modus die Immutability deaktivieren und Backup-Daten unbrauchbar machen.

Auch wenn manche Anbieter den Governance-Modus aufgrund seines Bedienkomforts empfehlen, raten wir dringend davon ab. Die Flexibilität geht zulasten der Sicherheit und läuft damit dem eigentlichen Zweck der Immutability zuwider.

Für Unternehmen, für die Datenintegrität, die Einhaltung gesetzlicher Vorschriften und der zuverlässige Schutz vor Ransomware Vorrang haben, ist der Compliance-Modus die einzig akzeptable Option. Der Modus sorgt dafür, dass die Immutability weder von Administratoren noch von Angreifern noch versehentlich umgangen werden kann. Damit schafft er die Voraussetzungen für eine wirklich sichere und überprüfbare Backup-Strategie.

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

End-to-End-Verschlüsselung

Trotz der Immutability von Backup-Daten auf Objektspeicher können Daten nach wie vor von Angreifern exfiltriert und gelesen werden, die sich während einer Kompromittierung Zugriff auf die Anmeldedaten für S3-Buckets verschafft haben. Um dieses Risiko zu beseitigen, müssen alle Backup-Daten bereits bei der Erstellung und noch vor der Übertragung an das Speichersystem verschlüsselt werden. Der Datenschutz muss an dem Punkt ansetzen, an dem Daten aus dem Produktivsystem ausgelesen werden.

Veeam unterstützt und empfiehlt die End-to-End-Verschlüsselung mit rotierenden Schlüsseln als Best Practice. Bei dieser Art der Verschlüsselung ändern sich die Schlüssel bei jeder Backup-Session. Dadurch lässt sich selbst bei Sicherheitsverletzungen, bei denen ein Zugriff auf Buckets erfolgt, eine Exfiltration von Daten verhindern.

Deduplizierungs-Appliances bieten KEINEN Schutz vor Exfiltrationsangriffen!
Beim Einsatz von Deduplizierungsspeicher muss die End-to-End-Verschlüsselung deaktiviert werden, da mit rotierenden Schlüsseln verschlüsselte Daten nicht effektiv dedupliziert oder komprimiert werden können.

Der Verzicht auf Datensicherheit zugunsten möglicher Speicheroptimierungen ist kein akzeptabler Kompromiss. Der Schutz von Backup-Daten vor unbefugten Zugriffen sollte stets Vorrang haben.

Sicherheitstests durch Dritte

Absolute Immutability darf kein leeres Versprechen bleiben, sondern muss durch unabhängige Dritte überprüft werden. Solche Tests durch Dritte sind jedoch nur möglich, wenn die Bewertung auf Basis offener Protokolle nach Branchenstandard erfolgt.

Proprietäre Systeme können nicht durch unabhängige Dritte getestet und verifiziert werden. Sie sind eine Art „Black Box" und setzen voraus, dass Kunden den Sicherheitsversprechen des Anbieters vertrauen.

Mit seinem offenen Design, seiner offenen Architektur und seiner vollständig dokumentierten API ermöglicht es S3-Objektspeicher unabhängigen Sicherheitsexperten, Prüfern und Sicherheitsteams, die Immutability, Zugriffskontrollen und Resilienz unter praxisnahen Angriffsbedingungen auf Herz und Nieren zu prüfen.

Berichte zu unabhängigen Tests zeigen, dass Sicherheit eine Grundvoraussetzung für alle Unternehmen sein sollte, die absolute Immutability realisieren möchten. Dennoch haben bislang nur wenige Anbieter solche Tests durchgeführt – und die Lizenzvereinbarungen einiger Anbieter untersagen Tests durch unabhängige Dritte sogar ausdrücklich.

Ohne S3-Objektspeicher und seine einzigartigen Funktionen zur Unterstützung und Durchsetzung von Datensicherheit ist absolute Immutability nicht möglich.

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

2. Sofortige Immutability

Die Gewährleistung der Immutability von Backup-Daten bereits bei der Erstellung ist entscheidend, um unbefugte Änderungen zu verhindern, die Datenintegrität aufrechtzuerhalten und Daten vor Ransomware zu schützen. Die bewährte und sicherste Methode dafür ist die S3-Versionsverwaltung in Kombination mit Object Lock. Sie gewährleistet Immutability bereits bei der Erstellung eines Objekts im Speichersystem. Dadurch wird das Risiko einer Manipulation, Einschleusung von Malware oder Löschung beseitigt – selbst bei Insider-Bedrohungen oder einer Kompromittierung von Anmeldedaten.

Die Architektur von älteren Speicherlösungen, die vor dem Ransomware-Zeitalter entwickelt wurden, unterstützt hingegen keine native Immutability. Um dies zu kompensieren, haben viele Anbieter versucht, ihre Lösungen nachträglich mithilfe verschiedener Workarounds um Immutability zu ergänzen. Sie bieten jedoch nicht dasselbe Maß an Schutz wie native Immutability.

Keine Immutability: **zeitlich verzögerte „Immutability“**

Manche Speicherlösungen wie Deduplizierungs-Appliances oder Eigenentwicklungen für die Datensicherung (Administratoren implementieren, konfigurieren und warten ein eigenes Backup Repository) schreiben Backup-Daten zunächst in eine veränderbare Landing Zone oder ein temporäres Dateisystem. Die Anwendung von Immutability erfolgt erst nach Abschluss des Backup-Jobs. Innerhalb dieses Zeitfensters können Daten geändert werden und sind Risiken ausgesetzt. Angreifer könnten diese Lücke ausnutzen, um Malware einzuschleusen oder die Daten vor der Durchsetzung von Immutability zu manipulieren. Dadurch wird die Integrität der Backup-Daten kompromittiert.

Keine Immutability: **Snapshot-basierte „Immutability“**

Herkömmliche Speichertypen wie DAS (Direct Attached Storage), JBOD (Just a Bunch of Disks), NAS (Network Attached Storage) und SAN (Storage Area Network) unterstützen keine native Immutability. Stattdessen versuchen die Anbieter solcher Lösungen, Immutability mithilfe von Snapshots zu simulieren. Damit ist bei Bedarf ein Rollback auf diese Point-in-Time-Kopien möglich. Snapshots bieten jedoch keineabsolute Immutability. Sie werden nach dem Schreiben der Daten erstellt und werden im selben Speichersystem vorgehalten wie die primären Daten. Dadurch können bei einem erfolgreichen Angriff auf das Produktivspeichersystem sowohl die Live-Daten als auch die zugehörigen Snapshots gelöscht oder beschädigt werden.

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

3. Zielspeicher-Appliance

Spezielle Backup-Storage-Appliances bestehen aus eigenständigen Storage-Geräten, die für die Speicherung von Backup-Daten konfiguriert und optimiert sind. Es gibt zwei Arten dieser Appliances: integrierte Appliances, die Backup-Software und Storage in einem System vereinen, und ZielspeicherAppliances, mit denen ein schlüsselfertiges Storage-Gerät für externe Backup-Software wie Veeam zur Verfügung steht.

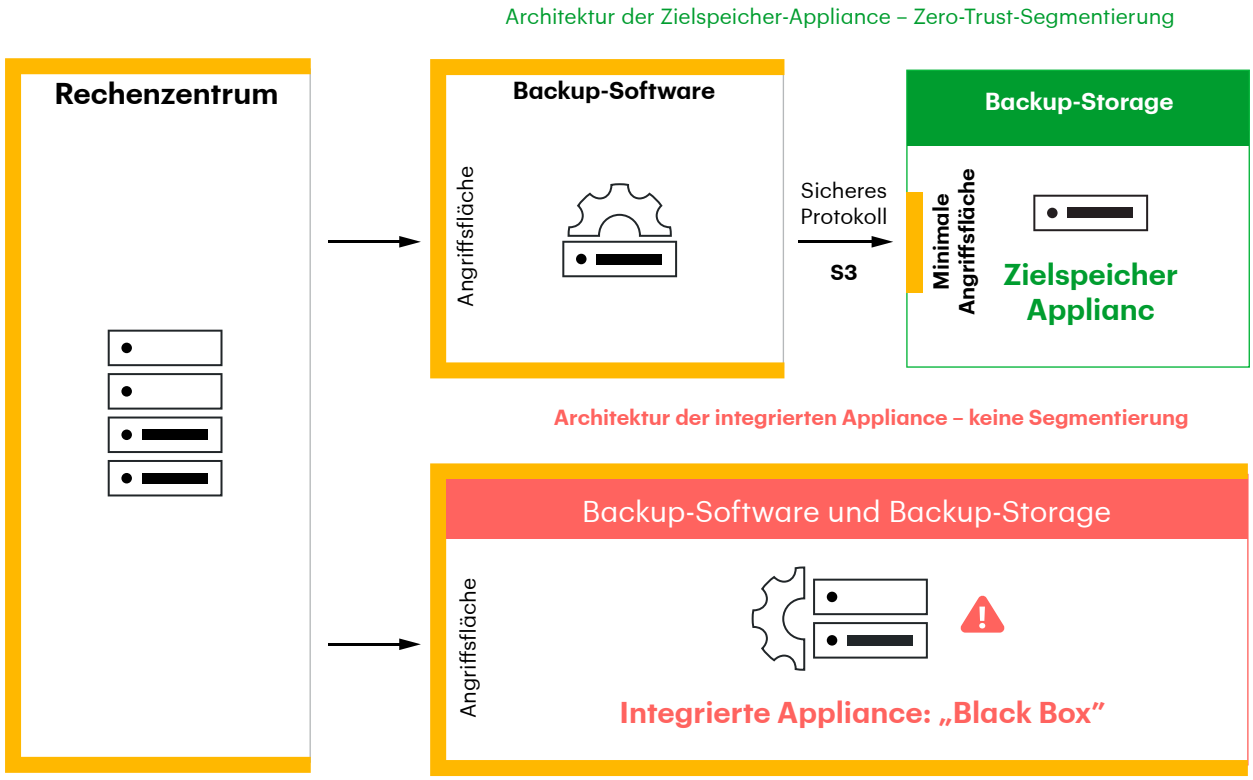
Trennung zwischen Backup-Software und Backup-Storage

Eine wesentliche Voraussetzung für absolute Immutability ist die strikte Trennung zwischen BackupSoftware und Backup-Storage. Diese Trennung ist eine Anforderung der von Veeam und Numberline Security entwickelten Architektur für Zero-Trust-Datenresilienz. Bei einer Zielspeicher-Appliance mit ordnungsgemäßer Segmentierung verringert sich die Angriffsfläche, indem sichergestellt wird, dass Backup-Daten physisch von der Backup-Software getrennt sind, mit der sie nach einem klar definierten, dokumentierten Protokoll verwaltet werden. Werden mehrere Kopien derselben Backup-Daten vorgehalten, sorgt die Segmentierung außerdem dafür, dass diese separat in unterschiedlichen Resilienzzonen gespeichert werden.

Dadurch wird gewährleistet, dass Angreifer auch mit gestohlenen Anmeldedaten Backup-Daten nicht ändern oder löschen können und Schutzmaßnahmen gegen Systemausfälle oder andere Katastrophen implementiert sind.

Nur Zielspeicher-Appliances, die auf S3 mit Zero-Access-Prinzipien basieren, können diese Trennung ordnungsgemäß vornehmen.

Zielspeicher-Appliance und integrierte Appliance im Vergleich



© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Keine überprüfbare Sicherheit: **Integrierte Backup-Appliance**

Integrierte Backup-Appliances bieten keine absolute Immutability, da Angreifer bei einer Kompromittierung vollständigen Zugriff auf die Backup-Software und den Backup-Storage 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.

Dieser Ansatz setzt großes Vertrauen in die Immutability des Dateisystems des Anbieters voraus. Es ist unmöglich zu wissen oder zu testen, was innerhalb dieser „Black Box" passiert. Nur Zielspeicher-Appliances, die auf dem offenen S3-Protokoll basieren, können unabhängig getestet werden und damit überprüfbare Sicherheit bieten

---

Unzureichende Sicherheit: **Selbst entworfenes Backup-Storage-System**

Bei einem selbst entworfenen System wird der Backup-Storage entweder manuell eingerichtet, indem Storage-Software auf selbst bereitgestellter Hardware installiert wird, oder vorkonfiguriert auf einem Allzweck-Server bereitgestellt. Während sich der erste Ansatz durch Flexibilität und der zweite durch eine einfache Bereitstellung auszeichnet, liegen bei beiden wichtige Aufgaben wie die tägliche Überwachung, das Einspielen von Patches, Service und Lebenszyklusmanagement in der Verantwortung des Kunden.

Dadurch wird jede Implementierung zu einer singulären, in vielen Fällen undokumentierten Umgebung, für die es keinen standardisierten Support gibt und keine ordnungsgemäße Netzwerksegmentierung, konsistente Konfiguration oder Best Practices für den Betrieb sichergestellt werden können. Diese mangelnde Konsistenz hat wesentliche Sicherheitslücken zur Folge. Zugleich sind umfassende Fachkenntnisse sowohl im Bereich Linux als auch im Bereich Cybersicherheit erforderlich. Damit kann dieser ressourcenintensive Ansatz auch dazu führen, dass Unternehmen auf ganz bestimmte Mitarbeiter mit diesem Fachwissen angewiesen sind.

Unzureichende Sicherheit: **Selbst entworfenes, als VM bereitgestelltes Backup-Storage-System**

Die Bereitstellung eines selbst entworfenen Backup-Storage-Systems auf einer virtuellen Maschine bringt weitere Risiken mit sich. Bei einer solchen Konfiguration wird Immutability ausschließlich über Softwarekontrollen innerhalb der VM durchgesetzt und nicht auf Ebene der Hardware oder Speicherinfrastruktur. Dadurch wird das System insgesamt anfälliger. Wenn sich ein Angreifer Zugriff auf die Virtualisierungsebene oder den zugrunde liegenden physischen Storage verschafft, kann er die gesamte Backup-VM und ihre virtuellen Datenträger mit nur wenigen Klicks ganz einfach löschen, neu zuweisen oder manipulieren.

SNur spezielle, schlüsselfertige S3-Zielspeicher-Appliances können nachweislich absolute Immutability gewährleisten – mit ordnungsgemäßer Segmentierung und der Durchsetzung von Sicherheit und Lebensyzklusmanagement auf Systemebene. Dadurch lassen sich die typischen Risiken und Inkonsistenzen von Eigenentwicklungen sowie der Vertrauensvorschuss in integrierte „Black Box"-Appliances vermeiden.

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Fazit

Absolute Immutability ist eine entscheidende Voraussetzung für den Schutz von Backup-Daten vor Ransomware-Bedrohungen. Sie sorgt für den Schutz sensibler Informationen, stellt die Einhaltung von Vorschriften sicher und gewährleistet die Datenintegrität bei Rechtsverfahren. Vor allem aber garantiert sie die Wiederherstellbarkeit und Resilienz von Daten.

Wenn eine Storage-Lösung zwar Immutability verspricht, Daten aber von Backup- oder StorageAdministratoren, Anbietern oder Angreifern überschrieben werden können, handelt es sich nicht um absolute Immutability.

Wenn Sie das Grundkonzept von absoluter Immutability verstehen, sind Sie besser in der Lage, zwischen wirklich sicheren Backup-Systemen und leeren Versprechungen der Anbieter zu unterscheiden.

Dieses Grundkonzept – und die Definition von absoluter Immutability – zeichnet sich dadurch aus, dass keinerlei Zugriff (Zero Access) auf schädliche Aktionen gewährt wird. So kann niemand – auch kein Administrator mit weit gefassten Rechten oder ein Angreifer mit Zugriff auf den Backup-Storage – Ihre Daten ändern oder löschen.

- **S3-Objektspeicher:** Ein umfassend dokumentierter, offener Standard mit nativer integrierter Immutability, der Penetrationstests und die Überprüfung durch unabhängige Dritte ermöglicht.
- **Sofortige Immutability:** Die Immutability von Backup-Daten muss ab dem Zeitpunkt ihrer Erstellung gewährleistet sein.
- **Zielspeicher-Appliance:** Bei einer dedizierten Zielspeicher-Appliance sind Storage und Backup-Software voneinander getrennt. Die Risiken, die beim Betrieb und insbesondere bei der Einrichtung, Aktualisierung und Wartung von selbst entworfenem und verwaltetem Backup-Storage entstehen, werden erfolgreich beseitigt. Kunden benötigen wenige bis gar keine Sicherheitskenntnisse und der Anbieter trägt die alleinige Verantwortung.

Durch Befolgung dieser drei Grundprinzipien können Unternehmen absolute Immutability gewährleisten und auf diese Weise sicherstellen, dass ihre Backup-Daten in jedem Fall – auch bei RansomwareAngriffen, Insider-Bedrohungen oder der Kompromittierung von Anmeldedaten – rundum geschützt und wiederherstellbar sind.

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

Über Object First

Object First bietet Ransomware-Schutz und integrierte Immutability. Damit profitieren Unternehmen von einem sicheren, unkomplizierten und leistungsfähigen Backup-Storage, der speziell für VeeamUmgebungen entwickelt wurde. Die Appliance ist in nur 15 Minuten einsatzbereit. Object First unterstützt die Prinzipien Security by Design und Security by Default. So können Veeam-Administratoren eine Architektur für Zero-Trust-Datenresilienz implementieren, die eine zuverlässige Sicherung und Wiederherstellung ermöglicht.

Simply Resilient for Veeam

© 2026 Object First. Alle Rechte vorbehalten. Alle Marken sind Eigentum der jeweiligen Inhaber.

1.0_20251118

OBJECT FIRST