Eine Ransomware-resistente Strategie mit Zadara und Veeam

In der heutigen datengesteuerten Welt sind Cyberangriffe wie Ransomware immer häufiger und ausgefeilter als je zuvor. Dies macht den Schutz von Daten nicht nur zu einer IT-Verantwortung, sondern zu einer geschäftskritischen Anforderung. Die Fähigkeit, sich schnell von einem solchen Angriff zu erholen, ist entscheidend, um Ausfallzeiten zu minimieren und potenziell katastrophale Auswirkungen zu begrenzen.

In diesem Blog werden wir untersuchen, wie **Zadara Object Storage** mit **Object-Lock-Unveränderlichkeit** und **Zadara VPSA (Virtual Private Storage Array)** als bedarfsgesteuerte Wiederherstellungsziele eine robuste Verteidigung gegen Ransomware bieten können. Darüber hinaus zeigen wir, wie **Datenschutzlösungen wie Veeam Data Platform 12.2** nahtlos mit den Lösungen von Zadara integriert werden können, um erweiterten Datenschutz und Wiederherstellungsmöglichkeiten zu bieten.

Zadara Object Storage als Backup-Ziel mit Object-Lock-Unveränderlichkeit

Zadara Object Storage ist eine skalierbare, unternehmenstaugliche Speicherlösung, die als direktes Backup-Ziel für geschäftskritische Workloads dient. Besonders für den Schutz vor Ransomware hebt sich diese Lösung durch ihre **Object-Lock-Unveränderlichkeitsfunktion** hervor, die sicherstellt, dass einmal gespeicherte Daten nicht verändert, gelöscht oder manipuliert werden können – und das für eine vorab festgelegte Aufbewahrungsdauer.

Diese Funktion macht **Zadara Object Storage** ideal für den Schutz von Backups vor Ransomware, da Cyberkriminelle Ihre Backups nicht verschlüsseln oder löschen können, selbst wenn sie in Ihre primären Systeme eindringen.

Wichtige Funktionen:

- **Write-Once-Read-Many (WORM):** Mit Object-Lock gespeicherte Daten sind unveränderlich, sodass selbst Administratoren sie nicht versehentlich oder absichtlich löschen können, bevor die vordefinierte Frist abläuft.
- **Regelbasierte Aufbewahrung:** Unternehmen können Richtlinien zur Datenaufbewahrung festlegen, um sicherzustellen, dass Backups für die erforderliche Dauer unverändert bleiben.
- **Compliance:** Object-Lock hilft bei der Einhaltung regulatorischer Vorgaben – in vielen Fällen ist es ohne diese Funktion schwierig oder gar unmöglich, eine Cyber-Versicherung abzuschließen.

Durch die Nutzung von **Zadara Object Storage** als direktes Backup-Ziel mit **Object-Lock** stellen Unternehmen sicher, dass ihre Backup-Daten unberührt und vollständig wiederherstellbar bleiben – selbst im Falle eines Ransomware-Angriffs.

Zadara VPSA als bedarfsgesteuerte Wiederherstellungsziele

Im Falle eines **Ransomware-Angriffs** oder einer **Katastrophe** benötigen Unternehmen eine zuverlässige und flexible Möglichkeit zur Wiederherstellung kritischer Daten. **Zadara VPSA** bietet die ideale Lösung als **On-Demand-Wiederherstellungsziel** für solche Szenarien.

Vorteile der Nutzung von Zadara VPSA:

- **Bedarfsgesteuerte Bereitstellung:** VPSAs können bei Bedarf gestartet werden, sodass Speicher- und Rechenressourcen ohne Vorabinvestition verfügbar sind.
- **Sofortige Wiederherstellungstests:** Backups können einfach in VPSA-Umgebungen wiederhergestellt und getestet werden, um sicherzustellen, dass sie im Ernstfall abrufbar sind.
- **Disaster Recovery:** Falls die primäre Infrastruktur kompromittiert ist, können VPSAs als **sekundäre Umgebung**dienen, in der Anwendungen wiederhergestellt werden, während die primäre Infrastruktur repariert wird.

Durch die Kombination von **Zadara Object Storage** mit **Object-Lock** und **Zadara VPSAs** erhalten Unternehmen eine schnelle Wiederherstellungslösung – sowohl für **Wiederherstellungstests** als auch für **echte Notfallszenarien**. Dank der integrierten Multi-Tenancy-Funktionalität ist dabei keine komplexe Multi-Vendor-Lösung erforderlich.

Defense-in-Depth-Strategie: Die Auswirkungen von Ransomware begrenzen

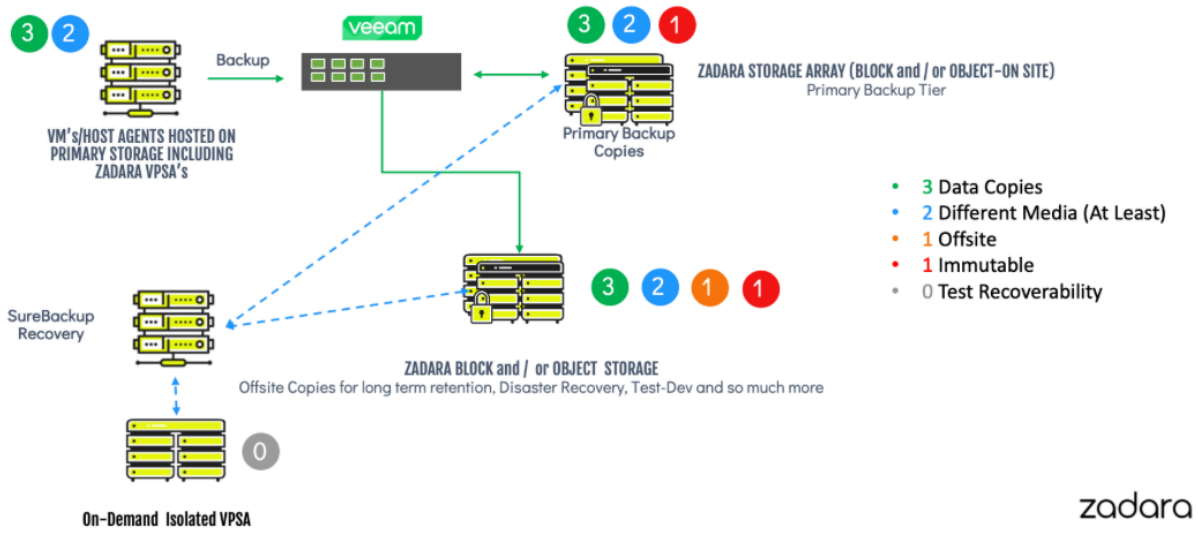
Eine **Defense-in-Depth-Strategie** ist entscheidend, um das Risiko einer erneuten Infektion oder zusätzlichen Schäden durch einen Ransomware-Angriff zu minimieren. Durch das Zusammenspiel mehrerer Sicherheitsmaßnahmen entsteht ein umfassender Schutz, der die Wahrscheinlichkeit eines **totale Datenverlustes** drastisch reduziert.

Wie Zadara eine Defense-in-Depth-Strategie unterstützt:

- **Isolation von Ressourcen:** Durch Netzwerksegmentierung und isolierte Speicherumgebungen wird verhindert, dass sich Ransomware von einem System auf ein anderes ausbreitet. Kritische Backup-Ressourcen wie **Zadara Object Storage** und **VPSA** bleiben isoliert, wodurch das Infektionsrisiko erheblich reduziert wird.
- **Unveränderliche Backups:** Selbst wenn Ransomware das Produktionsnetzwerk infiziert, bleiben mit Object-Lock gesicherte Backups unberührt und wiederherstellbar.
- **Granulare Wiederherstellungsoptionen:** On-Demand-VPSAs können als isolierte Wiederherstellungsumgebungen genutzt werden, in denen Backups getestet werden, bevor sie zurück ins Produktionssystem gelangen. Dies reduziert das Risiko einer erneuten Infektion.

Integration mit Veeam Data Platform 12.2

Mit Zadara können Veeam-Benutzer mehrere Backups erstellen und verwalten und Backup-Repositories zwischen Tenants auf Festplattenebene isolieren.



Die **Veeam Data Platform 12.2** erweitert die Schutz- und Wiederherstellungsfunktionen, wenn sie mit der **Zadara-Infrastruktur** kombiniert wird.

Schlüsselfunktionen von Veeam Data Platform 12.2:

- **Direkte Backups in Object Storage:** Veeam unterstützt die direkte Integration mit **Zadara Object Storage**, sodass keine Zwischenrepositorien erforderlich sind.
- **Backup-Unveränderlichkeit:** Veeam nutzt die **Object-Lock-Funktion** von Zadara, um Backups selbst auf Objektspeicher-Ebene zu schützen.
- **Sofortige Wiederherstellung:** Veeams „**Instant Recovery**"-Funktion ermöglicht es, Backups direkt von **Zadara Object Storage** auf **VPSA-Umgebungen** zu mounten, um Ausfallzeiten zu minimieren.
- **Automatisierte Wiederherstellungstests:** Mit der **SureBackup-Technologie** von Veeam können Wiederherstellungstests innerhalb der **Zadara VPSA-Umgebungen** automatisiert werden, um die Integrität und Wiederherstellbarkeit von Daten zu gewährleisten.

Durch die Kombination von **Veeam Data Platform 12.2** mit **Zadara Object Storage** und **VPSA** erhalten Unternehmen eine einheitliche Lösung für **Datensicherheit, Unveränderlichkeit, automatisierte Tests** und **flexible Wiederherstellung**.

Fazit: Eine Ransomware-resistente Strategie mit Zadara und Veeam

Die Bedrohung durch **Ransomware** wird nicht verschwinden – doch mit den richtigen Tools und Strategien können Unternehmen ihr Risiko drastisch reduzieren und ihre **Wiederherstellungsfähigkeiten verbessern**.

Zadara Object Storage mit Object-Lock-Unveränderlichkeit und **On-Demand-VPSAs** bieten eine **unsichtbare Kombination** zum Schutz Ihrer Daten und deren Wiederherstellbarkeit – selbst im schlimmsten Fall. Durch die Integration mit **Veeam Data Platform 12.2** können Unternehmen eine **ransomware-resistente Architektur** aufbauen.

Eine Defense-in-Depth-Strategie mit **isolierten Backup-Umgebungen** und **unveränderlichen Backups** reduziert den **Schaden** und das **Risiko einer erneuten Infektion**.

Nutzen Sie diese modernen Technologien, um der Cyberbedrohung einen Schritt voraus zu bleiben und Ihre Daten sowie Ihren Betrieb sicherzustellen – selbst in schwierigen Zeiten.

- ➔ **Schützen Sie Ihre Daten.**
- ➔ **Testen Sie Ihre Wiederherstellung.**
- ➔ **Planen Sie für den schlimmsten Fall – mit Zadara und Veeam sind Sie darauf vorbereitet.**

Wichtige Erkenntnisse:

- **Zadara Object Storage mit Object-Lock** schützt Backups vor Manipulation und Löschung.
- **Zadara VPSA** ermöglicht flexible, bedarfsgesteuerte Wiederherstellungsumgebungen.
- **Veeam Data Platform 12.2** integriert sich nahtlos für optimierte Backups und schnelle Wiederherstellung.
- **Eine Defense-in-Depth-Strategie** minimiert die Auswirkungen von Ransomware und das Infektionsrisiko.

Autor: Steve Costigan, Field CTO EMEA bei Zadara