Optimierung Ihres Data-Protection-Plans mit einer schnell reagierenden und robusteren Cyber-Recovery-Lösung

Basierend auf unserer Studie kann Dell Technologies PowerProtect Cyber Recovery eine physische Isolierung für Backup-Vaults und tiefergehende Scans nach Ransomware bereitstellen.

Physische Air-Gap-Isolierung für Backup-Vaults

Erstellen Sie eine physische Barriere, die Daten nicht überwinden können.

Tiefergehende Scans auf Ransomware

CyberSense analysiert Dateiinhalte und Datenbanken, nicht nur Metadaten.

Scannen von 2-mal mehr Anomalie-Workloads

Suchen Sie mit einem einzigen Tool an mehr Orten nach Malware.

Die durchschnittlichen Kosten eines Ransomwareangriffs sind in zwei Jahren um fast 20 % auf 5,23 Mio. USD gestiegen.[1] Effiziente Cyber-Recovery-Lösungen können dazu beitragen, diese potenziellen Kosten zu reduzieren oder sogar zu vermeiden, indem sie Unternehmen eine schnelle Wiederherstellung nach Incidents ermöglichen. Unternehmen können außerdem Datenverluste reduzieren, Ausfallzeiten minimieren und gleichzeitig ihre Markenintegrität wahren. Lösungen müssen bekannt fehlerfreie Daten nach dem Angriff lokalisieren und wiederherstellen können, um sicherzustellen, dass das Unternehmen kritische Daten und Systeme retten und gleichzeitig Geschäftsrisiken und Ausfallzeiten minimieren kann.

Dell PowerProtect Cyber Recovery (Cyber Recovery) ist eine solche Lösung. Sie hilft Unternehmen, ihre Daten und Anwendungen vor Ransomware, destruktiven Cyberangriffen und unerwarteten Ereignissen zu schützen. In diesem Bericht werden öffentlich verfügbare Daten verwendet, um grundlegende Data-Protection-Funktionen von Cyber Recovery und einer Konkurrenzlösung, Rubrik Security Cloud (RSC), zu vergleichen. Wir haben uns insbesondere die Funktionen und Merkmale angesehen, die Kunden bei Cyber-Recovery-Lösungen für wichtig halten, darunter Recovery Vault, Unveränderlichkeit, Workload-Unterstützung, Scantechnologie, Wiederherstellbarkeit und Isolierung.

Im Gegensatz zu RSC basiert Cyber Recovery auf einem Multi-Copy-Ansatz, was bedeutet, dass Backups (oder normalerweise eine ausgewählte Teilmenge von Backups) nach der Erstellung zur Sicherung und Analyse in einen isolierten Storage kopiert werden. Cyber Recovery umfasst mehrere Komponenten, darunter einen oder mehrere Storage Vaults, die sich entweder in einer PowerProtect Data Domain-On-Premise-Appliance oder über den softwarebasierten Dell APEX Protection Storage for Public Cloud in der Cloud befinden können. Im Vergleich dazu bietet RSC keine lokalen Vault-Optionen. Cyber Recovery umfasst außerdem CyberSense, eine vollständig automatisierte und integrierte intelligente Sicherheitsanalysen-Engine, die Daten, Dateien, Datenbanken und Images im Vault auf Anzeichen von Beschädigung durch einen Ransomwareangriff scannt. Die CyberSense-Lösung kann doppelt so viele Anomalie-Workloads scannen wie die Rubrik-Lösung. Dadurch kann das CyberSense-Scan-ML-System (maschinelles Lernen) die Auswirkungen von Malware oder anderen Aktivitäten von BedrohungsakteurInnen in mehr Daten erkennen. Wir analysieren, inwiefern PowerProtect Cyber Recovery anders funktioniert und für Ihr Unternehmen vorteilhafter sein könnte.

Produktübersicht

Übersicht über Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery besteht aus einer Storage Appliance, die Produktionsdaten enthält, und einer Ziel-Storage-Appliance im Vault für die Replikation. Die Lösung umfasst außerdem die Cyber Recovery-Software, mit der Sie die Synchronisation koordinieren, mehrere Datenkopien auf dem PPDD-System (PowerProtect Data Domain)-System im Cyber Recovery Vault managen, den Recovery-Prozess überwachen und den Analyseprozess mit CyberSense beaufsichtigen können.

Sie überträgt eindeutige Daten aus dem Produktions-PPDD-MTree über die MTree-Replikation an das Vault-Gegenstück und ermöglicht die Unveränderlichkeit von Daten* für eine festgelegte Dauer. Der Vault verfügt über einen Server, der die Cyber Recovery-Software und eine Komponente enthält, in der die Lösung Backupanwendungen und -daten wiederherstellt. Jeder Cyber Recovery Vault enthält in der Regel viele solcher Komponenten. Der Vault beinhaltet außerdem einen Analyse-/Indexierungshost, der mit Datenanalysesoftware ausgestattet ist und eine direkte Integration zwischen der Cyber Recovery-Software und CyberSense ermöglicht.

* Ziel der Produkte von Dell ist, Kunden bei ihren Bemühungen zum Schutz ihrer kritischen Daten zu unterstützen. Wie bei jedem elektronischen Produkt können auch bei Data-Protection-, Storage- und anderen Infrastrukturprodukten Sicherheitslücken auftreten. Es ist wichtig, dass Kunden Sicherheitsupdates installieren, sobald sie von Dell zur Verfügung gestellt werden.

Abbildung 1 bietet eine Übersicht über die Dell Cyber Recovery-Lösung.

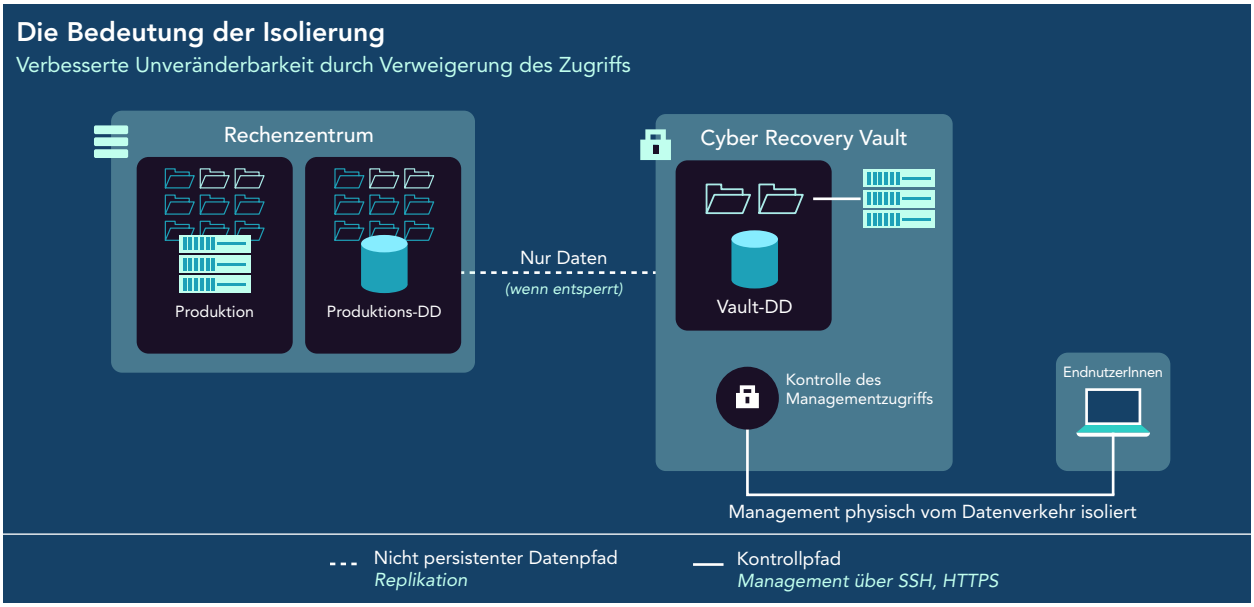

Abbildung 1: Allgemeine Daten- und Kontrollpfadarchitektur des Cyber Recovery Vault. Quelle: Principled Technologies.

Weitere Informationen zu den Kernkomponenten der Dell PowerProtect Cyber Recovery-Lösung finden Sie im Dell PowerProtect Cyber Recovery – Lösungshandbuch.

Übersicht über Rubrik Security Cloud

Rubrik beschreibt Rubrik Security Cloud als SaaS-Plattform (Software as a Service), mit der Kunden „ihre [Daten] sichern, Datenrisiken überwachen und [ihre] Daten schnell wiederherstellen, unabhängig davon, wo sie sich befinden – im gesamten Unternehmen, in der Cloud und in SaaS-Anwendungen“.[4] Rubrik gibt an, dass die Lösung auf einer „sicheren Microservices-Architektur basiert, die Hochverfügbarkeitsservices und eine in Google Cloud Platform (GCP) ausgeführte Infrastruktur nutzt“.[5] In Abbildung 2 ist die allgemeine Struktur von Rubrik Security Cloud dargestellt.

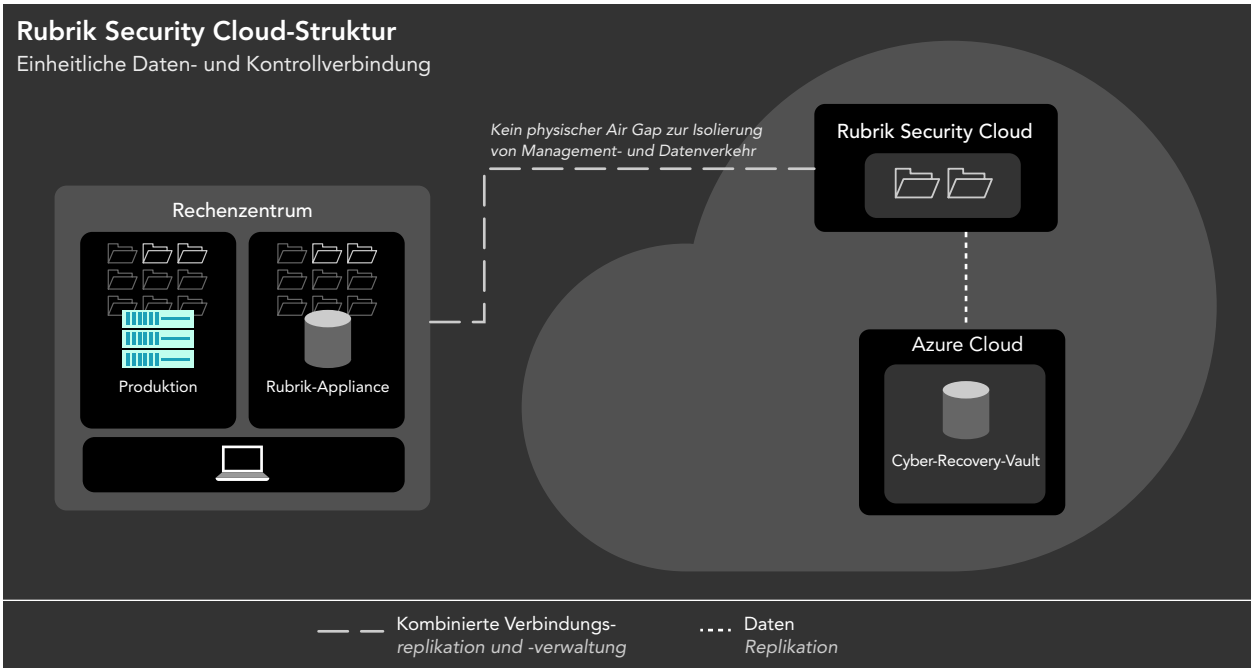

Abbildung 2: Die allgemeine Struktur von Rubrik Security Cloud. Quelle: Principled Technologies.

Unterstützte Funktionen

Recovery Vault

Vaults sind der dedizierte Storage, der verschlüsselte Kopien von Backups enthält, die mit der Lösung in Ihrer Produktionsumgebung erstellt werden. Die Vaults sind nicht Teil der Produktionsbackuplösungen. Stattdessen dienen sie jeweils als isolierter Speicherort für das Backup vom Backup, über den Kunden validierte Backups wiederherstellen können.

Dell bietet mehrere Vault-Optionen an, darunter an einem On-Premise-Standort, an einem Remote-Colocation-Standort oder in einer Public Cloud. Der On-Premise Vault nutzt eine PPDD mit Air-Gap-Betrieb, die sich in Ihrem Rechenzentrum befindet, potenziell sogar im selben Rack wie Ihre Backuplösung. Eine Air-Gap-Lösung ist normalerweise physisch von der Produktionsumgebung isoliert. Für einen Vault an einem externen Colocation-Standort sind dedizierte Netzwerkverbindungen zu einem physischen Vault wie bei einer On-Premise-Version erforderlich, aber der Vault ist in einem Remoterechenzentrum geografisch getrennt. Dell stellt außerdem Vaults in der Public Cloud bereit und arbeitet dafür mit den Cloud-Serviceanbietern Amazon Web Services (AWS), Microsoft Azure und Google Cloud zusammen. Public-Cloud-Vaults können Konfigurationsflexibilität bieten, um Kundenanforderungen zu erfüllen.[6, 7, 8]

Rubrik Cyber Recovery ist eine Komponente von Rubrik Security Cloud. Der Recovery Vault wird über ein Software as a Service-Modell bereitgestellt und nutzt nur Storage in Microsoft Azure. In vielen der öffentlich verfügbaren Dokumente, die wir während unserer Studie gefunden haben, ist der Rubrik Cyber Recovery Vault mit dem Rubrik Cloud Vault, dem Backup-Tier, verbunden, der Unveränderlichkeit bietet.[9, 10] Dieser Vault erfordert keine zusätzliche Hardware und kann von jeder Version der Rubrik Cloud Data Management-Plattform (CDM) ab Version 6.02 verwendet werden.

Unveränderbarkeit

Unveränderlichkeit bezieht sich auf die Bedingung, dass etwas unveränderlich oder dauerhaft ist. Mit unveränderlichen Backups und Sicherungskopien können AdministratorInnen Permanenz für Dateien schaffen. NutzerInnen oder Systeme können diese erst ändern oder löschen, wenn ein zugewiesener Zeitrahmen überschritten wurde. Dann werden die Dateien „entsorgt" – sie werden von der Lösung automatisch entfernt. Lösungen führen diesen Prozess in der Regel über Richtlinien oder Definitionen durch, die steuern, wie das System Dateien behandelt.[11]

Die Unveränderlichkeit von Dell PowerProtect Cyber Recovery beruht auf Aufbewahrungssperren über die „Retention Lock"-Funktion, um das Löschen oder Ändern (für einen bestimmten Zeitraum) oder den erzwungenen frühzeitigen Ablauf von Sicherungskopien zu verhindern. (PPDD ist ein Dateisystem, das nur angehängt werden kann, unabhängig davon, ob das Unternehmen Retention Lock aktiviert hat oder nicht.[12]) Dell Kunden managen Backups mithilfe von PPDD-MTrees, bei denen es sich um nutzerdefinierte logische Partitionen mit unabhängigen Aufbewahrungseinstellungen handelt, die sie als Ziele für Backupanwendungen zuweisen.[13] Kunden können zwischen zwei Arten von Aufbewahrungssperren wählen: Governance und Compliance. Compliance-Sperren sind die strengere und sicherere Option. Kunden aktivieren Aufbewahrungssperren pro MTree, d. h. dass alle Dateien innerhalb eines bestimmten MTree der Aufbewahrungssperrdefinition für diesen MTree entsprechen. Die Dauer für die Aufbewahrung wird auf Dateiebene festgelegt. Sobald Kunden eine Compliance-Aufbewahrungssperre definiert haben, kann sie weder von NutzerInnen noch vom System entfernt werden. Eine Governance-Aufbewahrungssperre – die weniger strenge Option – kann von AdministratorInnen rückgängig gemacht werden.[14]

Die Unveränderlichkeit der Lösung von Rubrik basiert ebenfalls auf Aufbewahrungssperren, um das Löschen oder frühzeitige Ablaufen von Sicherungskopien zu verhindern. Wie PowerProtect Cyber Recovery hängt die Rubrik-Lösung neue Daten an das Dateisystem an, statt vorhandene Daten zu überschreiben. Die Lösung versieht eingehende Daten mit einem Fingerabdruck und speichert diesen mit den Daten. **Die Rubrik-Lösung bietet keine standardmäßige Aktivierung von Aufbewahrungssperren.** Kunden müssen entweder ein Ticket beim Rubrik-Support öffnen oder eine Zwei-Personen-Regel aktivieren, um Aufbewahrungssperren zu ermöglichen. (Vor Rubrik Cloud Data Management Version 7.0.1 mussten sich Kunden an den Rubrik-Support wenden, um Aufbewahrungssperren zu aktivieren. Die Rubrik-Dokumentation enthält keine klaren Angaben dazu, ob Kunden den Support immer noch kontaktieren müssen, damit dies funktioniert.) Nach der Aktivierung durch Kunden verhindern Aufbewahrungssperren, dass NutzerInnen oder Systeme Daten außerhalb der definierten Parameter löschen können. Rubrik-Aufbewahrungssperren erfordern einen externen NTP-Server (Network Time Protocol) für die Zeitsynchronisation, was böswilligen AkteurInnen die Möglichkeit geben kann, die Referenz-NTP-Quelle zu manipulieren und dadurch Aufbewahrungssperren vorzeitig ablaufen zu lassen.[15]

> *„Die Rubrik-Lösung bietet keine standardmäßige Aktivierung von Aufbewahrungssperren. Kunden müssen entweder ein Ticket beim Rubrik-Support öffnen oder eine Zwei-Personen-Regel aktivieren, um Aufbewahrungssperren zu ermöglichen."*

Lizenzierung und Abonnements

Dell PowerProtect Cyber Recovery ist eine lizenzierte Lösung. Während der Installation installiert Dell standardmäßig eine 90-tägige Evaluierungslizenz. Nach 90 Tagen müssen Kunden eine neue Lizenz erwerben, um das Produkt weiterhin verwenden zu können. Dell bietet sowohl eine Standardlizenzierung (permanent) als auch eine abonnementbasierte Lizenzierung.

Rubrik integriert Rubrik Cyber Recovery in Rubrik Security Cloud (RSC). Kunden müssen über ein Rubrik Enterprise Edition-Abonnement verfügen, um Rubrik Cyber Recovery verwenden zu können. Die Abonnements haben eine Laufzeit von drei Jahren.[16, 17] Bei einem RSC-Ausfall benötigen SAP HANA- und Db2-Workloads Drittanbietertools für die Wiederherstellung von Daten, was zusätzliche Abonnementkosten verursachen kann.[18]

Verwaltungszugriff

Das Management des Dell PowerProtect Cyber Recovery-Systems erfolgt lokal für jede Topologie, die Kunden für die Bereitstellung auswählen. Da die Lösung die Recovery aus dem Vault initiiert, melden sich AdministratorInnen bei der Managementbenutzeroberfläche an, wo immer sich ihr Vault befindet. On-Premise Vaults bieten AdministratorInnen lokalen Zugriff ohne Internetzugang, was Cyberangriffe erheblich beeinträchtigen können – sei es aufgrund von Denial-of-Service-Angriffen oder der Sicherung der Daten durch Trennen der Internetverbindung, wie vom National Institute of Standards and Technology (NIST) empfohlen. Vaults an Colocation-Standorten ermöglichen den physischen Zugriff auf die Appliance von einem Remotestandort und nutzen Verbindungen außerhalb des öffentlichen Internets. Cloudbasierte Vaults benötigen für die Recovery einen Internetzugang, was die Recovery vor Ort verzögern könnte, bis der Cyberangriff beendet und die normale Netzwerkverbindung wieder hergestellt wurde.

Für das Management von Rubrik Cyber Recovery ist der Zugriff auf Rubrik Security Cloud erforderlich, was einen Internetzugang voraussetzt. Wie bereits erwähnt, könnte diese Art von Konnektivität die Recovery vor Ort verzögern, bis die Netzwerkfunktion nach einem Cyberangriff wieder normal hergestellt ist.

Da Kunden Zugriff auf RSC haben müssen, um Rubrik Cyber Recovery-Funktionen nutzen zu können, wird RSC zu einem Single-Point-of-Failure. Wenn dieser Service nicht mehr verfügbar ist, wird die Recovery aus dem Vault für den betroffenen Kunden behindert. Rubrik kann 10 Workloads während einer RSC-Serviceunterbrechung wiederherstellen, aber zwei Datenbank-Workloads benötigen für die Wiederherstellung Drittanbietertools und Unterstützung des Rubrik-Supports.[19, 20] Außerdem erhalten kompromittierte Administratorkonten oder bösartige AkteurInnen mit Zugriff auf die RSC-Plattform Zugriff auf den gesamten Datenbestand statt auf einen einzigen Vault.

Zusätzliche Hilfe mit Managed Detection and Response von Dell

Einige Unternehmen fühlen sich bei Cybersicherheit möglicherweise nicht wohl mit einem Ansatz, bei dem sie auf sich allein gestellt sind. Dell bietet diesen Kunden Managed Detection and Response (MDR), einen vollständig gemanagten Service, der Bedrohungen und Risiken überwacht und erkennt und mit Kunden zusammenarbeitet, um diese Risiken zu mindern. Laut Dell bietet der Service folgende Vorteile:[21]

- Vertrauenswürdiger Support, einschließlich fachkundiger Beratung bei der Bereitstellung und Konfiguration der XDR-Sicherheitsanalyseplattformen (Extended Detection and Response), die Dell unterstützt
- Bedrohungsabwehr- und Sicherheitskonfiguration, einschließlich bis zu 40 Stunden servicebezogener Sicherheitskonfiguration pro Quartal
- 24/7-Erkennung und -Untersuchung mit proaktiver Bedrohungssuche, die speziell auf die Umgebung jedes Kunden abgestimmt ist, um neue Bedrohungen oder Varianten bekannter Bedrohungen zu erkennen, die den Sicherheitssystemen entgehen
- Einleiten von Maßnahmen gegen Cyber-Incidents, einschließlich 40 Stunden jährlicher Remoteunterstützung bei der Reaktion auf Incidents, sodass Ermittlungsaktivitäten schnell beginnen können

In Kombination mit Dell APEX Cyber Recovery Services ermöglicht MDR Kunden die Auswahl aus zahlreichen Optionen für die Überwachung, Erkennung und Minderung von Bedrohungen und Risiken. Die Verfügbarkeit von Optionen kann eine erweiterte Abdeckung oder einen hybriden Ansatz bedeuten, der den Anforderungen Ihres Unternehmens entspricht.

Weitere Informationen zu MDR finden Sie unter **https://www.dell.com/en-us/dt/services/managed-services/managed-workplace-services/managed-detection-response.htm**.

Nahtlosigkeit

Setup

Die Einrichtung von Dell PowerProtect Cyber Recovery umfasst die Softwareinstallation auf einem Linux-System oder die Erstellung einer VMware® vSphere® Appliance über eine OVF-Vorlage (Open Virtualization Format). Für die Softwareinstallation sind 14 Schritte erforderlich[22], während die alternative vSphere Appliance nur 8 Schritte und 5 Minuten in Anspruch nimmt.[23] Nach der Installation können AdministratorInnen über Webbrowser in der isolierten Umgebung auf die Lösung zugreifen.

Kunden müssen CyberSense separat bereitstellen, eine vollständig automatisierte und integrierte intelligente Sicherheitsanalysen-Engine.[24] Die Anweisungen für die Installation von CyberSense in Dell PowerProtect Cyber Recovery sind nicht öffentlich verfügbar.[25]

Dell verfügt über mehrere Kennzahlen, die NutzerInnen optimieren können, darunter das Ziel für die Erkennung einer Vernichtung (Destruction Detection Objective, DDO), das Ziel für die Bewertung einer Vernichtung (Destruction Assessment Objective, DAO), den Cyber-Recovery-Punkt (Cyber Recovery Point, CRP), die Cyber-Recovery-Zeit (Cyber Recovery Time, CRT), das Cyber-Recovery-Synchronisierungsintervall (Cyber Recovery Synchronization Interval) und die Anzahl der Cyber-Recovery-Datenkopien (Cyber Recovery Data Copy Count). Dell empfiehlt außerdem, Daten zu charakterisieren, die geschützt werden müssen. Diese Daten können erfolgskritisch, geschäftskritisch, abhängig von Kerninfrastrukturservices oder anderen Anwendungen oder allgemein sein, z. B. Anwendungsbinärdateien, Start-Images und Backupkataloge. Das Angebot an Optionen gibt Kunden die volle Kontrolle über ihre Backupumgebung und die Möglichkeit, die Klassifizierung ihrer Daten anzupassen. Dell Consulting Services kann außerdem weitere Unterstützung und Vorschläge bereitstellen.[26]

Für die Einrichtung bei Rubrik sind ebenfalls mehrere Schritte erforderlich. Vor der Erstellung eines Clusters müssen Rubrik-Supportservices und Rubrik CDM installiert und konfiguriert werden. Anschließend müssen AdministratorInnen die neueste oder gewünschte Version von CDM herunterladen und installieren (15 Schritte).[27] Danach können AdministratorInnen einen Rubrik-Cluster über die Benutzeroberfläche oder die CLI einrichten. Sie können den Cluster mit der Benutzeroberfläche (UI) oder der Befehlszeile (CLI) einrichten, wobei beide Ansätze 24 Schritte benötigen.[28, 29] Dann können AdministratorInnen die Rubrik-Cluster mithilfe einer Onlinemethode (12 Schritte)[30] oder einer Offlinemethode (18 Schritte) registrieren.[31] Als Nächstes aktivieren die AdministratorInnen die Multi-Faktor-Authentifizierung (MFA), was 13 Schritte umfasst.[32] Schließlich fügen die AdministratorInnen das erste Konto (6 Schritte) und alle anderen Konten hinzu.[33] In Abbildung 3 ist die maximale Anzahl der möglichen Schritte zum Einrichten der einzelnen Cyber-Recovery-Lösungen dargestellt.

Rubrik-Kunden können andere Kennzahlen nicht optimieren, was möglicherweise weniger Flexibilität bietet, ihre Anforderungen zu erfüllen. Ein Prüfer gab an: „Die Benutzeroberfläche ist größtenteils relativ unkompliziert und einfach, aber in einigen Bereichen ist keine Beschreibung zur Verwendung vorhanden oder die Option fehlt. Zwar wird dadurch das Nutzererlebnis vereinfacht, aber viele optimierbare Optionen sind nicht vorhanden und erfordern, dass ein Support-Tunnel geöffnet wird, damit ein/e SupportmitarbeiterIn Änderungen in der Kundenumgebung vornehmen kann.“[34]

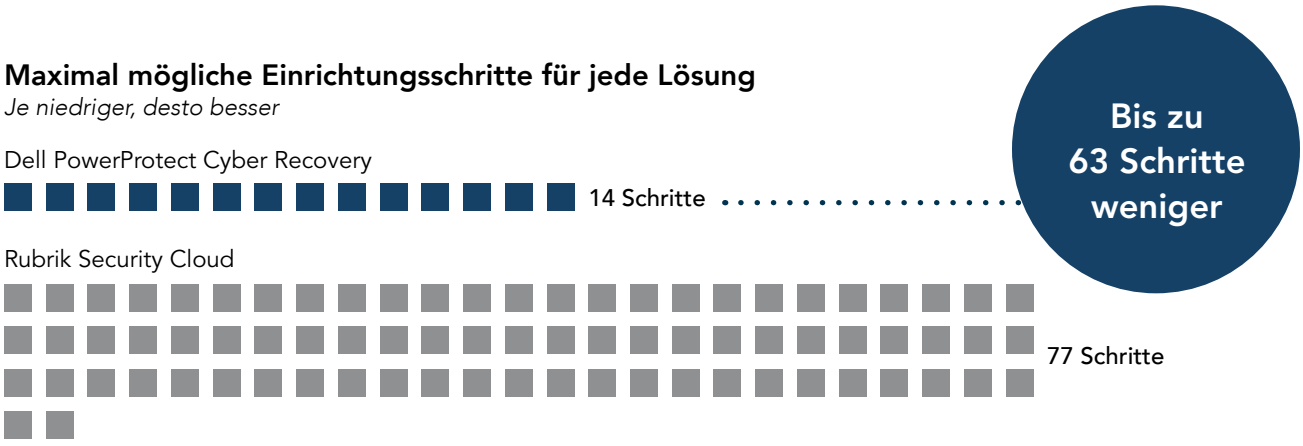

Abbildung 3: Maximale Anzahl der möglichen Schritte für die Einrichtung von Dell PowerProtect Cyber Recovery und Rubrik Security Cloud. Je niedriger, desto besser. Quelle: Principled Technologies.

Wartung

Wir haben beobachtet, dass die Benutzeroberflächen von Dell und Rubrik für die Durchführung alltäglicher Wartungsvorgänge nach der Einrichtung ähnlich sind. Nach der Konfiguration können Kunden Dell PowerProtect Cyber Recovery so konfigurieren, dass Folgendes ausgeführt wird:[35, 36]

- Automatische Generierung von Cyber Recovery-Jobberichten gemäß einem Zeitplan und als Reaktion auf eine manuelle Nutzeranfrage
    - Jobs werden durch NutzerInnen oder Zeitpläne erstellt, wenn sie eine Richtlinie, einen Recovery-Vorgang, ein Systembackup oder einen Bereinigungsvorgang initiieren
- Automatisches Monitoring von Vault-Status, Storage-Kapazität, Cyber Recovery-Vorgängen, Warnmeldungen, wenn die Kopie/Synchronisierung fehlschlägt oder der Cyber Recovery Vault ausgefallen ist, und Cyber Recovery-Jobs
- Automatische und kontinuierliche Scans auf Angriffe und Anzeige von nach Schweregrad angeordneten CyberSense-Warnmeldungen mit der Anzahl der betroffenen Dateien, Hosts und Richtlinien, der spezifischen erkannten Bedrohung, dem Zeitpunkt des Angriffs, damit Sie ein fehlerfreies Backup finden können, und einer Liste der beschädigten Dateien für die Angriffsanalyse

Auf ähnliche Weise können Kunden Rubrik für folgende Aufgaben konfigurieren:[37]

- Automatische Nutzung von Rubrik Security Cloud, um alle Ereignisse aller verbundenen Rubrik-Cluster zu verfolgen, zu überwachen und anzuzeigen; 3 Ereignistypen sind verfügbar:[38]
    - Kritisch: Ereignisse, die Aufmerksamkeit erfordern, z. B. fehlgeschlagene Backups, Archivierung oder Replikation
    - Warnung: Backup, Archivierung oder Wiederherstellung wurde abgeschlossen
    - Information: rein informativ
- Automatische und kontinuierliche Scans von Snapshots auf neue und vorhandene Bedrohungsanzeigen mit Threat Monitor; bereitgestellt werden der Zeitpunkt, an die Lösung zuletzt einen Snapshot erstellt hat, die Ereigniszeitachse, die Erkennungszeit, die Anzahl der geänderten Dateien, die Anzahl der verdächtigen Dateien, der Clustername sowie der Objekttyp und -name

Anomalie-Workload-Unterstützung

Sowohl Rubrik Security Cloud Data Threat Analytics als auch CyberSense scannen mehrere Workload-Typen. Laut den von uns gefundenen Quellen unterstützt CyberSense jedoch doppelt so viele Workloads zur Erkennung von Anomalien. Dazu gehört das Scannen der folgenden Arten von Workloads:

- VMs
- Kerninfrastruktur
- Nutzerdateien, die Dokumente, Verträge und geistiges Eigentum enthalten können
- Datenbanken
- Von anderen Clients erstellte Backups

"Bei der Anzahl der unterstützten Workloads haben wir in öffentlich verfügbaren Daten herausgefunden, dass CyberSense 21 Workloads zur Erkennung von Anomalien unterstützt, Rubrik dagegen 7."

Bei der Anzahl der unterstützten Workloads haben wir in öffentlich verfügbaren Daten herausgefunden, dass CyberSense 21 Workloads zur Erkennung von Anomalien unterstützt, Rubrik dagegen 7. Das bedeutet, dass CyberSense gemäß der von beiden Unternehmen bereitgestellten öffentlich verfügbaren Daten doppelt so viele Workloads wie Rubrik Security Cloud Data Threat Analytics unterstützt. Je mehr Daten eine Cyber-Recovery-Lösung scannen kann, desto höher ist die Wahrscheinlichkeit, dass sie heimtückische Malware oder andere Beschädigungen findet.

VM-Workload-Unterstützung

VM-Workloads beziehen sich auf die Anwendungen, Services oder Aufgaben, die VMs auf einem physischen Hostserver oder in einer Cloud-Umgebung ausführen. Da sich diese Workloads in ihren Funktionen und vielen anderen Aspekten unterscheiden, die ihre Gefährdung durch Malware wahrscheinlicher machen könnten, ist das Scannen von VMs unerlässlich. Rubrik Security Cloud Data Threat Analytics umfasst „Anomalieerkennung, Bedrohungsmonitoring, Bedrohungssuche und Daten-Recovery-Services auf geschützten Ressourcen“ und[39] unterstützt das Scannen der folgenden VM-Workloads:[40]

- VMware
- Nutanix® AHV
- Microsoft Hyper-V
- Microsoft Azure

CyberSense unterstützt das Scannen der folgenden VM-Workloads:[41, 42, 43]

- VMware
- Amazon Web Services (AWS)
- Hyper-V mit Dell Avamar- oder Dell NetWorker-Backups

VMware behauptet, dass „bis zu 80 % der virtualisierten Workloads auf VMware-Technologie ausgeführt werden“.[44] Im ersten Quartal 2024 kontrollierte der beliebteste Anbieter auf dem Markt für Cloud-Infrastrukturservices, Amazon Web Services (AWS), 31 % des gesamten Markts. Microsoft Azure belegt mit einem Marktanteil von 25 % den zweiten Platz.[45]

Kerninfrastruktur

Die Kerninfrastruktur beinhaltet die grundlegenden Komponenten und Services, die den Betrieb einer Technologieumgebung ermöglichen. Die Erkennung von Malware auf dieser Ebene kann dazu beitragen, den Schweregrad eines Angriffs zu reduzieren, da sich die Kerninfrastrukturfunktionen auf viele Systeme und NutzerInnen auswirken können. In der Rubrik Security Cloud-Dokumentation wird keine Unterstützung für das Scannen der Kerninfrastruktur erwähnt.[46]

Im Gegensatz dazu unterstützt CyberSense das Scannen der folgenden Kerninfrastruktur:[47]

- Active Directory
- DNS
- LDAP

Nutzerdateien, die Dokumente, Verträge und geistiges Eigentum enthalten können

Rubrik Security Cloud Data Threat Analytics unterstützt das Scannen der folgenden Nutzerdateien:[48]

- NAS-Datei- und -Datensätze
- Windows-Volume-Gruppen
- Linux und Windows

CyberSense kann Linux- und Windows-Nutzerdateien scannen.[49]

Scannen von Datenbanken

CyberSense 7 im Vergleich zu 0 bei RSC Data Threat Analytics

Datenbanken

Anwendungen können aus vielen Gründen unterschiedliche Arten von Datenbanken verwenden. Daher kann die Erkennung von Malware in verschiedenen Datenbanken entscheidend für eine schnelle Reaktion sein. Rubrik Security Cloud Data Threat Analytics kann Datenbanken sichern, aber wir haben keine öffentliche Dokumentation gefunden, gemäß der diese Datenbankbackups gescannt werden können.

CyberSense unterstützt das Scannen der folgenden Datenbanken mit Scans auf Seitenebene:[50]

- SQL
- Oracle®
- SAP HANA
- Db2
- PostgreSQL
- Epic® Caché
- MariaDB/MySQL

Von anderen Clients erstellte Backups

Einige Unternehmen verfügen möglicherweise über Datenbackups von mehreren Anbietern, um Redundanz zu bieten, Bestimmungen einzuhalten oder aus anderen wichtigen Gründen. In der Rubrik Security Cloud-Dokumentation wird die Unterstützung für das Scannen von Backups, die von anderen Backup-Clients erstellt wurden, nicht erwähnt.[51]

Mit einem klaren Vorteil in dieser Kategorie unterstützt CyberSense das Scannen von Backups, die von den folgenden Backup-Clients erstellt wurden:[52, 53, 54]

- DNAS
- SQL
- NetWorker
- Veritas NetBackup
- Umtausch
- Avamar
- CommVault

Scantechnologie

Rubrik Security Cloud bietet viele Tools für das Scannen und die Unterstützung beim Scannen in Data Threat Analytics:

- Rubrik Anomaly Detection zeigt verdächtige Dateien, Snapshot-Änderungen und Anomaliedetails als Anomalie-Incidents an[55], die Kunden untersuchen und bei der Snapshot-Untersuchung verwenden können.[56] Die Software bietet auch Recovery-Optionen.[57]
- Rubrik VM Encryption Detection erkennt Angriffe auf virtuelle VMware vSphere-Festplattendateien.[58]
- Rubrik Threat Monitoring zeigt Informationen zu erkannten Bedrohungen und Übereinstimmungen an.[59]
- Rubrik Threat Hunt ist ein von NutzerInnen initiierter Scan nach Anzeichen für eine Gefährdung.[60]
- Rubrik Quarantine isoliert Objekte, die bei einer Bedrohungssuche angezeigt werden.[61]

Rubrik RSC verfügt außerdem über Rubrik Backup Service Connectors für jeden Rubrik-Cluster.

Rubrik-Kunden müssen das richtige Tool für ihre Aufgabe auswählen, Scans möglicherweise manuell initiieren oder mehrere Tools verwenden, um ihre Aufgabe zu erledigen. Im Gegensatz dazu bietet Dell eine einzige CyberSense-Scanoption, die Kunden möglicherweise einfacher zu managen und zu verwalten finden.

CyberSense-Scans gehen tiefer als die „reinen Oberflächen"-Scans von Rubrik RSC Data Threat Analytics. CyberSense führt vollständige Inhaltsscans von Dateien und Scans von Datenbanken auf Seitenebene durch und kann eine partielle Verschlüsselung von Dateien erkennen.[62] Das Tool verwendet eine ML-Datenbank (maschinelles Lernen), die von Index Engines für Tausende von Datenbedrohungen trainiert wurde, und mehr als 200 Analysepunkte enthält, um Datenbeschädigungen zu erkennen.[63] Im Gegensatz zu Rubrik Threat Monitoring und Threat Hunt verlässt sich CyberSense nicht auf externe Threat-Intelligence-Agenturen, um Malwaresignaturen bereitzustellen. Stattdessen werden neue Bedrohungen erkannt.[64] **CyberSense stützt sich weder auf willkürliche Schwellenwerte für akzeptable Dateiänderungen oder Entropielevel zwischen Snapshots, die zu falsch negativen Ergebnissen führen können,** noch wird das ML-System auf eine Baseline des vorherigen Kundenverhaltens trainiert.[65, 66, 67]

Die Rubrik-Anomalieerkennungssoftware basiert ausschließlich auf Metadaten, um festzustellen, ob ein Snapshot beschädigt ist, bevor eine Inhaltsanalyse durchgeführt wird. Im Vergleich zum fortlaufenden CyberSense-ML-System erkennt die Rubrik-Software Beschädigungen nach Erhalt von Signaturen. Die Erkennung von Anomalien in Rubrik muss ein Verhaltensmodell erstellen, um die normale Baseline eines Kunden zu definieren. Dies kann mehrere Backups erfordern. Das Rubrik-Verhaltensmodell erfordert mindestens zwei Backups, um eine Baseline mit typischen Änderungen an einem Dateisystem zu erstellen, wenn keine Angriffe vorhanden sind. Ein einziger Satz von Änderungsstatistiken reicht jedoch möglicherweise nicht aus, um festzulegen, was typisch

„CyberSense stützt sich weder auf willkürliche Schwellenwerte für akzeptable Dateiänderungen noch auf Entropielevel zwischen Snapshots, die zu falsch negativen Ergebnissen führen können, …."

ist. Geschäftsereignisse können mehr oder weniger Aktivitäten oder verdächtigere Arten von Aktivitäten auslösen, die zwischen dem ersten und zweiten Rubrik-Snapshot nicht aufgetreten sind. Je mehr Backups die Rubrik-Lösung analysiert, desto genauer kann sie ihr Verhaltensmodell auf eine Baseline trainieren.[68, 69]

CyberSense enthält alle Analysen im Vault. In der Pipeline zur Analyse des Dateisystemverhaltens sendet Rubrik Metadaten zu Änderungen des Dateisystems des Kunden an die cloudbasierte Polaris-Plattform, um die Verhaltensanalyse durchzuführen, wodurch eine Angriffsfläche geöffnet wird.[70]

Kunden können Rubrik Threat Monitoring und Threat Hunt nur als Teil der Rubrik Enterprise Edition verwenden.[71] Sie müssen Threat Hunt-Scans mit RBAC-Berechtigungen (rollenbasierte Zugriffskontrolle) durchführen. NutzerInnen müssen zudem angeben, nach welchen spezifischen Anzeigen einer Kompromittierung (Indicators of Compromise, IOC) sie suchen möchten.[72] Das ist keine Best Practice der Branche.[73] Wie CyberSense unterstützt Threat Hunt VMware-, AHV-, Hyper-V- und NAS-Dateisätze sowie Linux- und Windows-Server.[74]

In den folgenden Abschnitten wird ausführlicher erläutert, wie die Bedrohungserkennung der Rubrik-Lösung funktioniert.

Metadaten- und Dateisystemstatistiken

Das Rubrik Anomaly Detection-ML-Verhaltensmodell protokolliert die Änderungen am Dateisystem seit dem letzten Snapshot, z. B. die Anzahl der hinzugefügten, gelöschten oder verschobenen Dateien, als Metadaten.[75] Dann wird ein ML-Modell mit diesen Änderungen trainiert, um eine Verhaltensmodell-„Baseline" für das Dateisystem zu erstellen. Rubrik markiert einen Snapshot als anomal, wenn zu viele Änderungen erkannt werden. Nachdem die Verhaltensanalyse einen Snapshot markiert hat, beginnt die Lösung mit einer Dateiinhaltsanalyse.[76] Das Monitoring von Metadaten kann eine Sicherheitsebene hinzufügen, bietet aber möglicherweise nicht den erforderlichen Schutz, der Ausfallzeiten durch ein Ereignis verhindert oder verringert.

> *CyberSense benötigt keine Baseline. Die Lösung überwacht und analysiert Änderungen an Datei- und Datenbankinhalten ab den ersten Sicherungskopien.*

Im Gegensatz dazu **benötigt CyberSense keine Baseline. Die Lösung überwacht und analysiert Änderungen an Datei- und Datenbankinhalten ab den ersten Sicherungskopien.** Der CyberSense-Ansatz bietet mehr Granularität, da die Software selbst Teile einer Datei oder einzelne Seiten einer Datenbank analysiert. Ähnlich wie bei der Rubrik-Lösung enthalten CyberSense-Scans Metadateneigenschaften und geben die Ergebnisse in die ML-Engine ein. Im Gegensatz zur Rubrik-Lösung beschränkt sich CyberSense nicht auf das Scannen von Metadaten und Index Engines hat seine ML-Engine mit von Index Engines dokumentierten Angriffen und nicht mit Signaturen oder vorherigem Kundenverhalten trainiert.[77, 78]

Schwellenwerte

Während der Verhaltensanalyse bestimmt Rubrik ML, wie wahrscheinlich es ist, dass eine Anomalie auf einem Dateisystem aufgetreten ist. Wenn die Rubrik-Lösung dies wahrscheinlich findet, führt sie eine Inhaltsanalyse durch. Dies könnte ein vom Verhaltensmodell bestimmter Schwellenwert für „anomales Verhalten" sein. Zum Beispiel könnte die Rubrik-Lösung auffälliges Verhalten kennzeichnen, wenn sie viele neue oder geänderte Dateien sieht oder eine erhöhte Zufälligkeit oder Verschlüsselungsindikatoren feststellt.[79] Während der Inhaltsanalyse zeigt Rubrik Anomaly Detection Änderungen am Dateiinhalt an und berechnet die Wahrscheinlichkeit der Verschlüsselung durch eine Berechnung der Entropie des Dateisystems. Die Entropie eines Dateisystems zeigt die Wahrscheinlichkeit an, dass ein Ransomwareangriff verschlüsselte Dateien enthält. Wenn die Entropie einen Anomalieschwellenwert überschreitet, warnt die Lösung den/die NutzerIn.[80, 81] Die Wirksamkeit bei der Erkennung von Datenbeschädigungen hängt von der Stringenz des Schwellenwerts ab. Zu wenig Stringenz kann zu falsch negativen Ergebnissen und somit zu einem falschen Sicherheitsgefühl führen.[82] Kunden müssen Schwellenwerte entsprechend festlegen.

Im Gegensatz dazu sucht CyberSense nach einer partiellen Verschlüsselung einer Datei, indem die Dateiinhalte mit einer Zuverlässigkeit von 99,99 % (laut Dell und Index Engines) bei der Erkennung von Datenbeschädigungen gescannt werden.[83]

Signaturen und Dateierweiterungen

Rubrik Threat Monitoring and Threat Hunts scannen Snapshots auf IOCs. Wenn eine der mehreren Threat-Intelligence-Quellen, die Rubrik überwacht, einen neuen IOC erkennt, sendet Threat Monitoring den Bedrohungs-Feed mit weiteren YARA-Regeln (Yet Another Ridiculous Acronym) zur Identifizierung der neuen Malware, auch als Malwaresignatur bezeichnet, an alle Rubrik-Cluster. Die Cluster beginnen dann mit dem Scannen.[84] Ein aktueller WatchGuard-Bericht legt nahe, dass 57,8 % der Malware die Signaturerkennung vermeiden. Fortschrittliche Malware wie BianLian kann Methoden nutzen, um die Signaturerkennung zu umgehen, und neue Malwarevarianten können geringfügig andere Signaturen als das Original haben. Daher könnte es für die Threat Intelligence schwieriger sein, auf dem neuesten Stand zu bleiben.[85]

Im Vergleich dazu verwendet CyberSense mehr als 200 Analysen und bietet ein ML-Modell, das mit Tausenden von Ransomwarevarianten trainiert wurde. Index Engines hat bewiesen, dass die CyberSense-Methode zuvor unbemerkte, ausgefeilte Varianten erkennen kann, ohne Signaturen herunterzuladen,[86] was ein weiterer Vorteil ist, wenn Sie sich während eines Ereignisses nicht auf das Internet verlassen müssen.

Massenverschlüsselungsereignisse

Die Rubrik-Lösung überwacht Massenverschlüsselungsereignisse, indem die Entropie des gesamten Dateisystems berechnet wird.[87] CyberSense bietet einen wesentlich feiner abgestimmten Ansatz. Die Lösung scannt nicht nur das Dateisystem im Allgemeinen oder sogar jede einzelne Datei, sondern stattdessen Teile des internen Inhalts von Dateien. Laut Index Engines werden bei der Berechnung der Entropie für nur eine ganze Datei statt für Teile davon „nur eine extreme Verschlüsselung der gesamten Datei“ oder Massenverschlüsselungsereignisse erkannt.[88]

Wiederherstellbarkeit

Basierend auf der Dokumentation betrachten wir die Recovery mit Dell PowerProtect Cyber Recovery als einen einfacheren und besser optimierten Prozess als die Recovery mit Rubrik. In diesem Abschnitt des Berichts, einschließlich seiner Unterabschnitte, werden die Recovery-Funktionen der beiden Lösungen und die Implementierung dieser Funktionen in den Lösungen verglichen.

In der Rubrik-Dokumentation wird angegeben, welche Recovery-Funktionen für welche VM-Typen geeignet sind. Dies scheint ein nützliches Maß an Granularität zu bieten, aber die vielen Bedingungen und Variationen machen die Recovery komplex. Rubrik-Kunden müssen beispielsweise bei der Wiederherstellung von Daten, Dateien und Systemen auswählen, welche Snapshot-Objekte sie in ihren Recovery-Plan aufnehmen möchten. Nach der Erstellung eines oder mehrerer Recovery-Pläne bietet Rubrik viele Wiederherstellbarkeitsoptionen an, darunter die folgenden:[89, 90, 91, 92, 93]

- Wiederherstellung von Dateien, indem sie heruntergeladen oder überschrieben und in einem separaten Ordner wiederhergestellt bzw. auf einen anderen Host oder in einen Clusterservice exportiert werden
- Wiederherstellung von Dateien für VMs, indem sie heruntergeladen oder überschrieben und in einem separaten Ordner wiederhergestellt oder in eine andere virtuelle Maschine exportiert werden
- Vollständige Snapshot Recovery einer VM oder eines Festplatten-Snapshots über die folgenden Methoden:
  - Live Mount, wodurch eine neue VM aus dem Snapshot erstellt wird
  - Mounten von virtuellen Laufwerken, wodurch neue virtuelle Laufwerke aus dem Snapshot erstellt werden
  - Instant Recovery, wobei die aktuelle VM durch eine neue VM ersetzt wird, die vom Snapshot erstellt wurde
  - Export, wodurch eine neue VM aus dem Snapshot in einem ausgewählten Datenspeicher erstellt wird
  - Batch-Recovery von VMs
- Massen-Cyber-Recovery für Recovery-Pläne über Live Mount and Export
- Rubrik Security Cloud Orchestrated Application-Recovery für die VM-Disaster-Recovery in einer isolierten Sandbox, an einem Remotestandort oder vor Ort

Die Batch-Recovery von Rubrik ist außerdem mit weiterer Komplexität verbunden. In Tabelle 1 sind die Batch-Recovery-Funktionen, die die Rubrik je nach Hypervisor dargestellt.[94]

Tabelle 1: Rubrik bietet Batch Recovery-Funktionen für verschiedene Hypervisors. Quelle: Rubrik.

Optionen für die VM-Erstellung				
	Live Mount	**Live Mount mit optionaler Migration**	**Exportieren**	**Instant Recovery**
vSphere-VMs	Verfügbar, nutzt den Rubrik-Cluster als Datenspeicher	Nicht verfügbar	Verfügbar, nutzt den Datenspeicher des wiederhergestellten Hypervisors	Verfügbar, nutzt den Rubrik-Cluster als Datenspeicher
AHV-VMs	Verfügbar, nutzt den Rubrik-Cluster als Datenspeicher	Verfügbar, nutzt den Rubrik-Cluster als Datenspeicher und den Nutanix-Container für alle nachfolgenden Schreibvorgänge	Verfügbar, nutzt den Nutanix-Container als Datenspeicher	Nicht verfügbar
Virtuelle Hyper-V-Maschinen	Verfügbar, nutzt den Rubrik-Cluster als Datenspeicher	Nicht verfügbar	Verfügbar, nutzt den Datenspeicher des wiederhergestellten Hypervisors	Verfügbar, ersetzt die aktuelle VM durch eine neue aus dem Snapshot; nutzt den Rubrik-Cluster als Datenspeicher

Bei der Rubrik-Lösung befindet sich der wiederhergestellte Datenspeicher in der Regel auf dem Rubrik-Cluster und nicht in der Produktionsumgebung, was zu Problemen führen kann. Wir stellen diese Probleme im nächsten Abschnitt vor: "Rubrik limitations". Im Gegensatz dazu kann PowerProtect wiederhergestellte Daten in Recovery- oder Produktionsumgebungen platzieren, um eine schnellere und reibungslosere Recovery zu ermöglichen, die Ausfallzeiten minimieren könnte.

In Tabelle 2 sind zusätzliche Informationen von Rubrik zur Recovery von vSphere-VMs dargestellt.[95] Wie die Tabelle zeigt, befinden sich die meisten vSphere-Recovery-Datenspeicher auf dem Rubrik-Cluster.

Tabelle 2: Recovery-Funktionen, die Rubrik für vSphere-VMs bereitstellt. Quelle: Rubrik.

Recovery-Funktionen, die Rubrik für vSphere bereitstellt				
Aktion	**Datenspeicher**	**Stromzustand**	**Netzwerk**	**Source VM**
Wiederherstellen von Dateien	Unzutreffend	Nicht zutreffend	Nicht zutreffend	Keine Auswirkung
Live Mount	Lokaler Rubrik-Cluster	Aktiviert oder deaktiviert	Nicht verbunden	Keine Auswirkung
Mounten virtueller Laufwerke	Lokaler Rubrik-Cluster	Ein	Nicht verbunden	Keine Auswirkung
Instant Recovery	Lokaler Rubrik-Cluster	Ein	Verbunden (optional)	Ausgeschaltet und umbenannt
Exportieren	Datenspeicher des Hypervisors	Aus	Nicht verbunden	Keine Auswirkung
In-Place-Recovery	Datenspeicher des Hypervisors	Ein	Identisch mit der Quell-VM	Bei der In-Place-Recovery werden die Dateien des virtuellen Laufwerks der Quell-VM mit den Daten des virtuellen Laufwerks aus dem Snapshot überschrieben, ohne die Eigenschaften der VM zu ändern

Die Rubrik-Lösung bietet keine umfassende Implementierung für die Massen-Recovery und die Optionen für die Massen-Recovery sind begrenzt und komplex. Wie im "Dell PowerProtect Data Manager offers the equivalent of Rubrik "mass restore"" Abschnitt dieses Berichts näher erläutert, ist Dell PowerProtect optimiert und einfacher.

Der Mythos der Massenwiederherstellung

Rubrik wirbt für die Massen-Recovery, die als schnelle Wiederherstellung des Geschäftsbetriebs durch die Recovery von Anwendungen, Dateien oder NutzerInnen in großem Umfang definiert wird.[96] Das Unternehmen bietet viele Optionen für die Massen-Recovery. Die Rubrik-Lösung speichert die wiederhergestellten Daten jedoch in der Regel auf dem Rubrik-Cluster und nicht in der Produktionsumgebung.[97] Workloads hängen von der Verfügbarkeit des Rubrik-Systems ab, bis die Lösung ihre Migration abgeschlossen hat. Der lokale Rubrik-Cluster ist Tier-3-Storage, sodass Kunden eine zusätzliche Migration in ihre Produktionsumgebung durchführen müssen, um zu den geplanten Performanceleveln zurückzukehren. Mit diesem Single-Point-of-Failure und der reduzierten Performance während der Migration des Systems kann die Recovery erst als abgeschlossen betrachtet werden, wenn die Rubrik-Lösung die Workloads in der Produktionsumgebung wiederherstellt.

Dell PowerProtect bietet ebenfalls eine Massen-Recovery, da NutzerInnen mehrere VMs für die Recovery in der Recovery-Benutzeroberfläche auswählen können.

Dell PowerProtect Data Manager bietet eine äquivalente Funktion zur „Massenwiederherstellung" von Rubrik.

Im Vergleich zur Rubrik-Lösung bietet die Dell Lösung auch mehrere gleichwertige Recovery-Optionen für vSphere-VMs. Dell PowerProtect kann VM-Daten in Recovery- oder Produktionsumgebungen platzieren. Bei den meisten Rubrik-Optionen werden Daten nur im Rubrik-Cluster platziert. In Tabelle 3 sind die Recovery-Optionen von Dell gezeigt.[98, 99, 100, 101]

Tabelle 3: Recovery-Optionen von Dell. Quelle: Principled Technologies.

Recovery-Optionen von Dell	
Typ	**Beschreibung der Funktion**
Wiederherstellung auf Dateilevel	Stellt nur infizierte Dateien vor Ort oder durch Rollback wieder her
Live VM	Stellt eine VM auf dem Cluster mit einer späteren Migration in die Produktion wieder her
Restore to new	Stellt die ursprüngliche Umgebung oder neue Umgebung (z. B. einen Reinraum oder eine Recovery-Infrastruktur) wieder her, währenddessen NutzerInnen mehrere VMs gleichzeitig für eine Massenwiederherstellung oder eine Wiederherstellung nach Maß auswählen können
Zugriff/Live VM	Erstellt eine isolierte Kopie der Produktionsdaten
Recovery-Orchestrierung	Ermöglicht es AdministratorInnen, die Wiederherstellung zu planen oder sie bei Bedarf verfügbar zu machen; priorisiert die automatische Recovery von VMs in der Produktion oder einer Recovery-Umgebung

Einschränkungen bei Rubrik

Die Rubrik-Lösung versetzt Snapshots, die mit Malware infiziert sind, für eine spätere Analyse in Quarantäne. Die Rubrik-Lösung stellt jedoch standardmäßig keine Quarantäne für Snapshots bereit. Kunden können dann die in Quarantäne versetzten Dateien herunterladen und sie selbst entweder manuell oder mit Hilfe von Drittanbietertools forensisch analysieren,was sie potenziell für Malware anfällig macht.[102, 103]

> *CyberSense führt die Analyse ohne eigene forensische Untersuchungen durch NutzerInnen durch. Außerdem automatisiert die Software die Erstellung von Wiederherstellungspunkten.*

CyberSense analysiert standardmäßig Dateien und Datenbanken. NutzerInnen müssen Snapshots nicht manuell unter Quarantäne stellen. **CyberSense führt die Analyse ohne eigene forensische Untersuchungen durch NutzerInnen durch. Außerdem automatisiert die Software die Erstellung von Wiederherstellungspunkten.**[104]

Rubrik RSC im reinen RSC-Managementmodus ist ein Single-Point-of-Failure für viele Funktionen. Am besorgniserregendsten ist, dass ein Angriff zu einer RSC-Serviceunterbrechung führen kann, die sich auf die Internetverbindung oder die Konnektivität zwischen dem Nutzerstandort und RSC auswirkt. Nach solchen Angriffen bietet die Lösung NutzerInnen eine begrenzte Anzahl von Funktionen, die über die Rubrik CDM-Benutzeroberfläche oder API-basierte Automatisierung verfügbar sind, aber nur, wenn NutzerInnen vor dem Angriff ein RSC-Servicekonto erstellt haben.[105, 106]Ein Unternehmen kann die folgenden Workloads und Daten ohne RSC wiederherstellen: MongoDB, Microsoft Exchange, Dateien, Hyper-V-Snapshots, Live Mount von gemanagten Volumes, NAS-Hostdateien, Oracle, SQL Server, VCD und VMware.[107] Für die Wiederherstellung von SAP HANA ohne RSC sind Tools von Drittanbietern wie Studio und Cockpit Cross sowie Rubrik-Support über den Support-Tunnel erforderlich. Die Wiederherstellung von IBM DB2 ohne RSC erfordert zudem IBM-Tools von Drittanbietern und Rubrik-Support über den Support-Tunnel.[108]

Air Gap/Isolierung

NIST definiert einen Air Gap als „eine Schnittstelle zwischen zwei Systemen, an der (a) sie nicht physisch verbunden sind und (b) jede logische Verbindung nicht automatisiert ist (d. h., dass Daten nur manuell über die Schnittstelle und unter menschlicher Kontrolle übertragen werden)".[109]

Air Gaps können dazu beitragen, den Datenfluss von einer Quelle zu einem Ziel zu kontrollieren. Sie können außerdem eine wichtige Komponente jeder Strategie für den Schutz vor Ransomware und die Cyber-Recovery sein. Wenn ein Angriff oder Ereignis Ihre Produktionsbackupsysteme gefährdet, kann die Möglichkeit, Datenverkehr von Ihren Produktionssystemen zu geschützten Backups in Ihren Cyber Recovery Vaults zu verhindern, Ausfallsicherheit bieten.

Physische Isolierung

Vielleicht haben Sie ein Beispiel für eine physisch isolierte Lösung im Film „Mission Impossible" gesehen, in dem der Hauptcharakter alle anderen Sicherheitsfunktionen der Einrichtung umgehen musste, um auf sensible Daten auf einem Computersystem zuzugreifen, das nicht mit einem externen Netzwerk verbunden war. Die physische Isolierung kann auch normalerweise getrennte Segmente dedizierter physischer Netzwerke verwenden, um Sicherungskopien von Ihren Produktionssystemen in den Vault zu übertragen. Wenn keine Verbindung besteht, erstellen diese betrieblichen Air Gaps eine physische Hürde, die Daten nicht automatisch überschreiten können, sodass der Zugriff für bösartige AkteurInnen erschwert wird.

Unternehmen können Dell PowerProtect Cyber Recovery physisch isolieren, um eine betriebliche Air-Gap-Strategie zu ermöglichen. Die Lösung nutzt eine dedizierte physische Verbindung und führt die Datenreplikation als Pull-Vorgang aus dem Vault statt als Push-Vorgang aus der Backuplösung durch. Während des Kopierens/Replizierens aktiviert die Lösung die Verbindung, verschlüsselt Daten und migriert sie über die dedizierte Zeile.[110] Nach Abschluss der Replikation deaktiviert die Lösung die Verbindung von der Vault-Seite erneut. Die Lösung macht Vault-Kopien mit gesperrten Richtlinien für eine Aufbewahrungssperre unveränderlich, sodass selbst wenn NutzerInnen oder Systeme Zugriff erhalten, die Vault-Kopien nicht geändert oder gelöscht werden können. Kein Managementdatenverkehr durchläuft den Replikationspfad. **Selbst wenn böswillige AkteurInnen die Kontrolle über Ihre On-Premise-**

Backuplösung erlangen, initiiert und trennt der Vault den Replikationspfad und verwendet unidirektionale, reine Datenabrufe von der Datenquelle, wodurch der direkte Zugriff auf den Vault eingeschränkt wird.[111]

Logische Isolierung

Die logische Isolierung hingegen verwendet Systeme, die sich möglicherweise im selben physischen Netzwerk befinden, aber eine logische Netzwerktrennung und -kontrolle erstellen, um sicherzustellen, dass Systeme keine Daten untereinander senden können. Die Lösung nutzt zusätzliche Sicherheitsimplementierungen wie Verschlüsselung und Hashing zusammen mit RBAC und Multi-Faktor-Authentifizierung, um sicherzustellen, dass ein nicht autorisiertes System oder unbefugte NutzerInnen die Daten, die sich in einem anderen System befinden, nicht lesen können.

Rubrik beschreibt seine Cyber-Recovery-Funktion als die Nutzung einer logischen Air-Gap-Strategie.[112, 113] Viele der verfügbaren öffentlichen Aussagen von Rubrik werfen jedoch Zweifel an der Notwendigkeit von Air Gaps auf. In einer Rubrik-Präsentation mit dem Titel „Rubrik Security – Air Gap and Immutability" wird behauptet, dass die native Lösung des Unternehmen einen Air Gap nutzt, da es keine Möglichkeit gibt, auf die Backups zuzugreifen oder sie zu bearbeiten, sobald die Lösung sie erstellt hat, obwohl die Rubrik-Appliance im physischen Netzwerk verbleibt.[114] Authentifizierte böswillige AkteurInnen können jedoch weiterhin Zugriff auf die Appliance-GUI erhalten, was Auswirkungen auf die Recovery haben kann. Um dies zu mindern, verfügt Rubrik über Aufbewahrungssperren, die den Ablauf von Backups verhindern, wodurch sie unveränderlich werden. Nach der Aktivierung verhindern Aufbewahrungssperren außerdem, dass ein Rubrik-Cluster auf die Werkseinstellungen zurückgesetzt und gelöscht wird. Gemäß dem Rubrik CDM-Sicherheitshandbuch deaktiviert die Lösung standardmäßig Aufbewahrungssperren auf dem Cluster global und erfordert, dass Kunden sich an den Rubrik-Support wenden, um diese zu aktivieren.[115] In öffentlich verfügbaren Quellen wird nicht geklärt, ob der Rubrik-Support auch Aufbewahrungssperren deaktivieren kann, was die Wahrscheinlichkeit erweckt, dass autorisierte böswillige AkteurInnen die Sicherheitsebenen weiterhin umgehen können.

„Kein Managementdatenverkehr durchläuft den Replikationspfad. Selbst wenn böswillige AkteurInnen die Kontrolle über Ihre On-Premise-Backuplösung erlangen, initiiert und trennt der Vault den Replikationspfad und verwendet unidirektionale, reine Datenabrufe von der Datenquelle, wodurch der direkte Zugriff auf den Vault eingeschränkt wird."

Entscheidung

Unternehmen müssen aktiv zahlreiche Angriffsvektoren in ihren Rechenzentren in Betracht ziehen. Ein guter Data-Protection-Plan zielt darauf ab, alle Daten zu schützen, insbesondere die kritischen Daten, die für den Betrieb unerlässlich sind. Wir haben uns öffentlich verfügbare Informationen zu Dell PowerProtect Cyber Recovery und Rubrik Secure Cloud angesehen, um zu ermitteln, wie beide Lösungen Datenmanagement, Schutz und Recovery angehen.

Bei PowerProtect Cyber Recovery werden Sicherungskopien kritischer Daten in einem Vault physisch isoliert und deren Wiederherstellbarkeit im Falle eines Cyberangriffs sichergestellt. Die Lösung nutzt eine auf einen Air-Gap-Betrieb basierende Strategie mit physischer Isolierung, was Rubrik Secure Cloud nicht für sich beanspruchen kann – die Lösung basiert auf logischer Isolierung.

Cyber Recovery nutzt ML-basierte Analysen in CyberSense, um die Integrität der Daten im Vault zu bewerten und saubere Backupdaten für die Recovery zu identifizieren. Rubrik Secure Cloud bietet dagegen ein ML-trainiertes Analysetool, das nach Anomalien sucht, statt tiefgehende Scans für Dateien durchzuführen.

Darüber hinaus bietet die Cyber Recovery-Lösung mehrere Recovery-Optionen, die nicht kompromittierte Daten aus dem Vault nutzen, um eine effiziente und nahtlose Rückkehr zum Betrieb zu ermöglichen. In vielen Fällen kann PowerProtect Cyber Recovery Funktionen und Vorteile bieten, die Rubrik Secure Cloud fehlen. Das bedeutet, dass die Lösung potenziell sicherer ist und tiefergehende Analysen ermöglicht, um Ausfallzeiten zu minimieren und die Recovery zu beschleunigen.

---

1. Anastasia Dergacheva und Jesse R. Taylor, „Study Finds Average Cost of Data Breaches Continued to Rise in 2023“, abgerufen am 25. Juli 2024, https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023.
2. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“, abgerufen am 18. April 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
3. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.
4. Rubrik, „Rubrik Security Cloud Architecture and Security Implementation“, abgerufen am 18. April 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
5. Rubrik, „Rubrik Security Cloud Architecture and Security Implementation“, abgerufen am 18. April 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/wp-rubrik-security-cloud-architecture-and-security-implementation.pdf.
6. Rob Emsley, „Public Cloud Vault to Secure, Isolate and Recover Data“, abgerufen am 20. März 2024, https://www.dell.com/en-us/blog/public-cloud-vault-to-secure-isolate-and-recover-data/.

7. Brian White, „Dell's PowerProtect Cyber Recovery Expands to Microsoft Azure", abgerufen am 20. März 2024, https://www.dell.com/en-us/blog/dells-powerprotect-cyber-recovery-expands-to-microsoft-azure/.
8. Dell, „Cyber Recovery on Google Cloud Platform", abgerufen am 20. März 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-cyber-recovery-reference-architecture/cyber-recovery-on-google-cloud-platform/.
9. Chris Mellor, „Up to $5m compensation if Rubrik Cloud Vault recovery busted", abgerufen am 20. März 2024, https://blocksandfiles.com/2022/02/24/up-to-5m-compensation-if-rubrik-cloud-vault-recovery-busted/.
10. Kristina Avrionova, „Frequently Asked Questions about Rubrik Cloud Vault", abgerufen am 20. März 2024, https://www.rubrik.com/blog/company/22/3/faq-about-rubrik-cloud-vault.
11. Chris Wahl, „Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture", abgerufen am 22. März 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.
12. Dell, „Data Domain Invulnerability Architecture: Enhancing Data Integrity and Recoverability", abgerufen am 7. Juni 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h7219-data-domain-data-invul-arch-wp.pdf.
13. Dell, „Consolidate Governance and Compliance Archive Data", abgerufen am 4. April 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-domain-retention-lock/consolidate-governance-and-compliance-archive-data/.
14. Dell, „Dell PowerProtect Cyber Recovery Solution Guide", abgerufen am 24. März 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.
15. Rubrik, „Retention-locked SLA Domain attributes", abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/8.0/ug/cdm/attributes_of_retention_locked_sla_domains.html.
16. Rubrik, „Rubrik Cyber Recovery", abgerufen am 20. März 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/brf-rubrik-cyber-recovery.pdf.
17. Rubrik, „Rubrik Licensing: Subscribe to Simplicity", abgerufen am 20. März 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/data-sheet/rubrik-licensing-data-sheet.pdf.
18. Rubrik, „Workloads require third-party tools for recovery", abgerufen am 6. Mai 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.
19. Rubrik, „Recoverable workloads during RSC service disruption", abgerufen am 6. Mai 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
20. Rubrik, „Workloads require third-party tools for recovery".
21. Dell, „Strengthen your security posture with Managed Detection and Response", abgerufen am 2. April 2024, https://www.delltechnologies.com/asset/pl-pl/services/managed-services/technical-support/managed-detection-and-response-datasheet.pdf.
22. Dell, „Dell PowerProtect Cyber Recovery 19.13 Installation Guide", abgerufen am 20. März 2024, https://www.dell.com/support/manuals/en-us/cyber-recovery/irs_p_19.13_installation/installing-the-cyber-recovery-software?guid=guid-8718978d-ddd0-4dc0-bca7-fb04a2f3d1fb&lang=en-us.
23. Dell, „Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
24. Dell, „Dell PowerProtect Cyber Recovery 19.13 Installation Guide".
25. Dell, „Installing CyberSense in Dell PowerProtect Cyber Recovery", abgerufen am 20. März 2024, https://infohub.delltechnologies.com/en-US/l/ransomware-protection-secure-your-data-on-dell-powerflex-with-powerprotect-cyber-recovery-1/installing-cybersense-in-dell-powerprotect-cyber-recovery-1/.
26. Dell, „Dell PowerProtect Cyber Recovery Solution Guide".
27. Rubrik, „Downloading and installing Rubrik CDM", abgerufen am 20. März 2024, https://docs.rubrik.com/en-us/saas/install/download_install_cdm_on_appliance_nodes.html.
28. Rubrik, „Setting up a Rubrik Cluster using the UI", abgerufen am 20. März 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_ui.html.
29. Rubrik, „Setting up a Rubrik Cluster using the CLI", abgerufen am 20. März 2024, https://docs.rubrik.com/en-us/saas/install/setting_up_cli.html.
30. Rubrik, „Registering Rubrik clusters using the online method", abgerufen am 20. März 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_online.html.
31. Rubrik, „Registering Rubrik clusters using the offline method", abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/install/registering_clusters_offline.html.
32. Rubrik, „Enabling MFA", abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/install/rsc_enabling_mfa.html.
33. Rubrik, „Adding the initial account", 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/adding_the_initial_account.html.
34. TrustRadius, „Learning Rubrik by putting the pieces together Brik by Brik", abgerufen am 21. März 2024, https://www.trustradius.com/reviews/rubrik-2023-09-20-21-03-04.
35. Dell, „Dell PowerProtect Cyber Recovery Solution Guide".

36. Index Engines, „CyberSense®: How it Works“, abgerufen am 21. März 2024, https://www.indexengines.com/how-it-works.
37. Rubrik, „Anomaly event details“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_event_details.html.
38. Rubrik, „Events page“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/common/events_page.html.
39. Rubrik, „RSC Data Threat Analytics“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_ransomware_monitoring.html.
40. Rubrik „RSC Data Threat Analytics“.
41. Dell Technologies, „Dell PowerProtect Cyber Recovery: Reference Architecture“, abgerufen am 6. Mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/h18661-dell-powerprotect-cyber-recovery-reference-architecture-wp.pdf.
42. Dell Technologies, „Dell EMC Avamar for Hyper-V“, abgerufen am 16. Mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu89876.pdf.
43. Dell Technologies, „Dell EMC NetWorker Module for Microsoft for Hyper-V“, abgerufen am 16. Mai 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu92011.pdf.
44. VMware, „Accelerate IT. Innovate with your cloud.“, 9. Mai 2024, https://www.vmware.com/files/pdf/VMware-Corporate-Brochure-BR-EN.pdf.
45. Statista, „Cloud infrastructure services vendor market share worldwide from fourth quarter 2017 to first quarter 2024“, 17. Juli 2024, https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/.
46. Rubrik „RSC Data Threat Analytics“.
47. Dell Technologies, „CyberSense® für PowerProtect Cyber Recovery“, abgerufen am 27. Juni 2024, https://www.delltechnologies.com/asset/en-gb/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.
48. Rubrik „RSC Data Threat Analytics“.
49. Index Engines, „CyberSense® Support Matrix“, abgerufen am 21. März 2024, https://www.indexengines.com/csmatrix.
50. Dell Technologies, „CyberSense® für PowerProtect Cyber Recovery“.
51. Rubrik: „Keep Your Databases Running in the Face of Any Threat“.
52. Index Engines, „CyberSense® Support Matrix“.
53. Dell Technologies, „Dell EMC Avamar for Hyper-V“.
54. Dell Technologies, „Dell EMC NetWorker Module for Microsoft for Hyper-V“.
55. Rubrik, „Anomaly incidents“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_incident.html.
56. Rubrik, „Data Threat Analytics events“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/ri_events.html.
57. Rubrik, „Viewing Anomaly Detection“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_ri_investigations.html.
58. Rubrik, „VM Encryption Detection“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/vm_encryption_detection.html.
59. Rubrik, „Viewing the Threat Monitoring page“, 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/viewing_the_threat_monitoring_page.html.
60. Rubrik, „Initiating a threat hunt“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
61. Rubrik „Quarantining matched files or objects“, abgerufen am 2. April 2024, https://docs.rubrik.com/en-us/saas/saas/quarantining_matched_objects_or_files.html.
62. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
63. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
64. Index Engines, „The Power of CyberSense's Machine Learning“, abgerufen am 2. April 2024, https://go.indexengines.com/csmachinelearning.
65. Index Engines, „The Power of CyberSense's Machine Learning“.
66. Index Engines, „The Power of CyberSense's Machine Learning“.
67. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
68. Rubrik, „Anomaly Detection behavioral model“, abgerufen am 20. Mai 2024, https://docs.rubrik.com/en-us/saas/saas/anomaly_detection_behavioral_model.html.
69. Amazon, „Training ML Models“, abgerufen am 2. April 2024, https://docs.aws.amazon.com/machine-learning/latest/dg/training-ml-models.html.
70. Rubrik, "Defense in Depth with Polaris Radar," abgerufen am 21. März 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/Defense-In-Depth-Polaris-Radar-Technical-White-Paper.pdf.
71. Rubrik, „Data Threat Analytics dashboard“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_dashboard.html.
72. Rubrik, „Initiating a threat hunt“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/initiating_a_threat_hunt.html.
73. SentinelOne, „What Is A Malware File Signature (And How Does It Work)?“, abgerufen am 4. April 2024, https://www.sentinelone.com/blog/what-is-a-malware-file-signature-and-how-does-it-work/.

74. Rubrik, „Threat hunts“, abgerufen am 21. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_threat_hunts.html.
75. Rubrik, „Anomaly Detection features“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
76. Rubrik, „Behavioral model“.
77. Index Engines, „The Power of CyberSense's Machine Learning“.
78. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
79. Rubrik, „Behavioral model“.
80. Rubrik „Anomaly Detection features“.
81. Rubrik, „Behavioral model“.
82. Dell, „CyberSense® für PowerProtect Cyber Recovery“.
83. Morningstar, „Index Engines' CyberSense Announces 99,99% SLA in Detecting Ransomware Corruption, Empowering Smarter Recovery“, abgerufen am 17. Juli 2024, https://www.morningstar.com/news/pr-newswire/20240618ny41171/index-engines-cybersense-announces-9999-sla-in-detecting-ransomware-corruption-empowering-smarter-recovery.
84. Rubrik, „Threat Monitoring“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/threat_monitoring.html.
85. Index Engines, „The Power of CyberSense's Machine Learning“.
86. Index Engines, „The Power of CyberSense's Machine Learning“.
87. Rubrik, „Anomaly Detection features“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_features.html.
88. Index Engines, „The Power of CyberSense's Machine Learning“.
89. Rubrik, „Investigating and recovering anomalous files for filesets“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files.html.
90. Rubrik, „Investigating and recovering anomalous files for virtual machines“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/investigating_and_recovering_anomalous_files_for_virtual_machines.html.
91. Rubrik, „Full snapshot recovery of a virtual machine“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/full_snapshot_recovery_of_a_virtual_machine.html.
92. Rubrik, „Recovery of a batch of virtual machines“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
93. Rubrik, „Performing bulk recovery for Recovery Plans“, abgerufen am 22. März 2024, https://docs.rubrik.com/en-us/saas/saas/performing_bulk_recovery_for_recoveryplans.html.
94. Rubrik, „Recovery of a batch of virtual machines“, abgerufen am 4. April 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
95. Rubrik, „Recovery of virtual machines“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/vs_recovery_vm.html.
96. Der wiederhergestellte Datenspeicher befindet sich in der Regel auf dem Rubrik-Cluster und nicht in der Produktionsumgebung.
97. Rubrik, „Recovery of a batch of virtual machines“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/ri_batch_recovery_of_vm.html.
98. Dell, „Restore plan“, abgerufen am 16. April 2024, https://infohub.delltechnologies.com/en-US/l/powerprotect-data-manager-protection-for-vmware-cloud-foundation-on-dell-emc-vxrail-1/restore-plan/.
99. Dell, „PowerProtect Data Manager overview“, abgerufen am 16. April 2024, https://infohub.delltechnologies.com/en-US/l/dell-powerprotect-data-manager-deployment-best-practices-1/powerprotect-data-manager-overview-4/.
100. Dell, „PowerProtect Data Manager 19.9 Administration and User Guide“, abgerufen am 16. April 2024, https://www.dell.com/support/manuals/en-us/enterprise-copy-data-management/pp-dm_19.9_ag/file-level-restore-of-a-powerprotect-backup-in-the-vsphere-client.
101. Dell, „Recovery Orchestration with PowerProtect Data Manager Overview“, abgerufen am 16. April 2024, https://www.youtube.com/watch?v=po2oMnAg_x4.
102. Rubrik, „Quarantine files or objects“, 24. März 2024, https://docs.rubrik.com/en-us/saas/saas/quarantine.html.
103. Rubrik, „Downloading quarantined files for forensic analysis“, 24. März 2024, https://docs.rubrik.com/en-us/saas/saas/downloading_quarantined_files_for_forensic_analysis.html.
104. Forrester, „The Total Economic Impact™ Of Dell PowerProtect Cyber Recovery“, abgerufen am 16. April 2024, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/the-total-economic-impact-dell-powerprotect-cyber-recovery.pdf.
105. Rubrik, „Workload recovery during an RSC service disruption“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/workload_recovery_during_rsc_outage.html.
106. Rubrik, „Rubrik CDM APIs and service account workflows“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/rubrik_apis_sa_workflows.html.
107. Rubrik, „Recoverable workloads during RSC service disruption“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/recoverable_workloads_during_rsc_service_disruption.html.
108. Rubrik, „Workloads require third-party tools for recovery“, abgerufen am 16. April 2024, https://docs.rubrik.com/en-us/saas/saas/workloads_require_third_party_tools_for_recovery.html.

109. NIST, „Computer Security Resource Center Glossary: air gap“, abgerufen am 29. Juli 2024, https://csrc.nist.gov/glossary/term/air_gap.

110. Dell, „Dell PowerProtect Cyber Recovery Solution Guide“.

111. Dell, „Dell PowerProtect Cyber Recovery: Reference Architecture“.

112. Adam Eckerle, „Debunking the Myths about Air Gaps“, abgerufen am 14. März 2024, https://www.rubrik.com/blog/technology/2021/11/debunking-the-myths-about-air-gaps.

113. Rubrik, „Air-Gap, Isolated Recovery, and Ransomware - Cost vs. Value“, abgerufen am 14. März 2024, https://www.rubrik.com/content/dam/rubrik/en/resources/solutions-brief/Air-Gap-Isolated-Recovery-and-Ransomware-Cost-vs.-Value.pdf.

114. Brian Williams, „Rubrik Air Gap and Immutability“, abgerufen am 14. März 2024, https://vimeo.com/561870246.

115. Rubrik, „Retention locks in the Rubrik cluster“, abgerufen am 18. März 2024, https://docs.rubrik.com/en-us/9.0/sg/security_guide/retention_locks_in_the_rubrik_cluster.html.

▶ Lesen Sie die Originalversion dieses Berichts in englischer Sprache

Dieses Projekt wurde in Auftrag gegeben von Dell Technologies.

Principled Technologies®

Facts matter.®