# Beschleunigte Ransomware-Recovery mit Dell PowerProtect Backup Services

Recovery von Ransomware innerhalb von Stunden, nicht Tagen

### Wichtige Funktionen

Ransomwareangriffe treten immer häufiger auf und sind immer ausgefeilter und kostspieliger.

- Unfähigkeit, nicht infizierte Backups oder Dateien schnell zu identifizieren und wiederherzustellen
- Kontamination breitet sich aus und wird durch Recovery-Daten erneut infiziert.
- Datenverlust, Unfähigkeit, ein vollständiges Datenvolumen wiederherzustellen
- Schwierigkeiten bei der Koordination der Incident-Response-Orchestrierung
- Anforderungen an schnellere RPO-/RTO-Zeiten
- Kostspielige Geschäftsausfälle, die zu Umsatzeinbußen und Schäden am Markenimage führen
- Bußgelder und behördliche Auflagen aufgrund unzureichender Data Protection

## Die Herausforderung

Ransomware ist eine ernste Bedrohung für jedes Unternehmen. Cyberangriffe treten häufig auf und können katastrophale Schäden verursachen. 79 % der Unternehmen befürchten, dass in den nächsten 12 Monaten ein Störereignis eintreten wird. Unternehmen, die ihre Daten verlieren, laufen Gefahr, nach einer Katastrophe den Konkurs zu beantragen. Ransomwareangriffe finden nicht nur immer häufiger statt, sie werden technologisch immer ausgereifter und ziehen hohe Kosten nach sich.

## Die Lösung

Eine schnelle, zuverlässige Recovery beseitigt jeden Grund, eine Lösegeldzahlung überhaupt in Erwägung zu ziehen. Aber wenn ein Sicherheitsvorfall oder ein Cyberangriff auftritt, müssen Unternehmen verstehen, wie groß die Auswirkungen sind und was die Ursache ist, bevor sie eine Recovery durchführen. Mit makellosen Snapshots von Workloads und virtuellen Maschinen, die rund um die Uhr verfügbar sind, kontinuierlichem Monitoring für Nutzer- und Datenanomalien, der Integration in Sicherheitstools und der automatisierten Recovery sauberer Daten können Sie Ihren Sicherheitsstatus verbessern und einen verheerenden Vorfall in einen überlebensfähigen Incident verwandeln.

## Die Funktionen

**Für alle Workloads:**

• Sicherstellung, dass Sie über unveränderliche Air-Gap-Backups rund um die Uhr verfügen

• Wiederherstellen bereinigter Daten On-Premise oder in der Cloud mit RPO/RTO von Stunden, nicht Tagen oder Wochen

• Der Managed Data Detection and Response-(MDDR-)Service bietet 24x7x365-Echtzeitmonitoring von Backupumgebungen.

• Wenn Sie Workloads und VMs in einer beliebigen AWS-Region/einem beliebigen AWS-Account wiederherstellen und dabei Daten aus Ihrer Produktionsorganisation verwenden, viele Kopien davon erstellen und sie an mehreren Orten speichern, setzen Sie Ihr Unternehmen einem großen Risiko aus.

**Beschleunigte Ransomware-Recovery für wichtige Workloads:**

• Monitoring und proaktive Erkennung von Anomalien mit ML-basierten Algorithmen

• Orchestrierung von Response- und Recovery-Aktivitäten über SIEM- und SOAR-Integrationen

• Scannen von Snapshots vor der Recovery auf Malware und löschen infizierter Snapshots und Dateien aus Backups

• Automatisches Wiederherstellen der neuesten bereinigten Version jeder Datei in einem bestimmten Zeitrahmen aus einem goldenen Snapshot

## Schutz

Der erste Schritt zur Verhinderung von Schäden durch Ransomware besteht darin, sicherzustellen, dass Sie eine isolierte und unveränderliche Kopie Ihrer Daten haben. Dell PowerProtect Backup Services basiert auf einer hochgradig ausfallsicheren Cloud-Infrastruktur und macht es für Ransomware unmöglich, Backupdaten zu verschlüsseln. Die Zero Trust-Architektur, einschließlich Multi-Faktor-Authentifizierung, Envelope-Verschlüsselung und separatem Kontozugriff, stellt sicher, dass Ransomware keine kompromittierten Zugangsdaten der primären Umgebung verwenden kann, um die Backupumgebung oder -daten zu manipulieren. Und schließlich bieten Funktionen zur Vermeidung von übermäßigem Löschen und zur weichen Löschung (Papierkorb) eine weitere Sicherheitsebene, um Backups vor dem Löschen zu schützen.

## Erkennung

Die schnellstmögliche Erkennung eines Ransomwareangriffs kann Incident-Response-Teams helfen und die Ausbreitung von Kontaminationen verhindern. Das beschleunigte Ransomware-Recovery-Modul der Dell PowerProtect Backup Services bietet ein Security Command Center, um den Status Ihrer Backupumgebung zu überwachen. Mit Zugriffseinblicken und Anomalieerkennung können Sie ungewöhnliche Aktivitäten in Ihrer Umgebung und Ihren Daten schnell erkennen. Sehen Sie sich Standort-, Identitäts- und Aktivitätsinformationen für alle Zugriffsversuche von NutzerInnen und APIs an. Erkennen Sie Anomalien mit proprietären ML-Algorithmen, die Warnmeldungen für ungewöhnliche Datenaktivitäten (z. B. Löschen, Verschlüsselung usw.) bereitstellen. Der Algorithmus erlernt die Muster für Ihre spezifische Backupumgebung, sodass er keine Regeln einrichten oder abstimmen muss. Er verwendet auch entropiebasierte Einsichten, um falsche Positivfälle zu reduzieren.

## Antwort

Wenn Sicherheits- oder IT-AnalystInnen ein verdächtiges Ereignis erkennen oder, schlimmer noch, bestätigen, dass ein Ransomware-Incident aufgetreten ist, wird die Reaktionsgeschwindigkeit zu einem entscheidenden Faktor. Während es viele wertvolle Sicherheitstools für die primäre Umgebung gibt, die für die Erkennung und Reaktionsorchestrierung verwendet werden können, verbessern Analysen und Änderungsprotokolldaten aus sekundären Daten (Backupsysteme) die Untersuchung, Reaktion und forensische Aktivitäten. Das beschleunigte Ransomware-Recovery-Modul der Dell PowerProtect Backup Services bietet robuste API-Integrationen, die es einfach machen, die Lösung in Ihre allgemeine Sicherheitsumgebung zu integrieren. Die Orchestrierung von Reaktionsaktivitäten mit SIEM- und SOAR-Lösungen kann Ihre MTTR (Mean Time to Response, durchschnittliche Antwortzeit) drastisch reduzieren, indem Aktionen wie die Quarantäne infizierter Systeme oder Snapshots oder das Scannen von Backups auf IOCs basierend auf einem vorab festgelegten Ransomware-Playbook automatisch abgeschlossen werden.

## Recovery

Nach der ersten Antwortphase kommt die harte Recovery-Arbeit. Für viele Unternehmen ist dies ein manueller und zeitaufwändiger Prozess. Die Verweilzeit für böswillige Akteure und Ransomware kann von Wochen bis Monate reichen, was es schwierig macht, zu wissen, wie weit man zurückgehen muss, um saubere Daten zu finden. Selbst nachdem der beste Snapshot identifiziert wurde, kann versteckte Malware zu einer erneuten Infektion führen. Ein Recovery-Punkt vor 2 Wochen ist für die meisten Business-NutzerInnen jedoch nicht akzeptabel. Die Suche und Validierung neuerer Daten nach einem Ransomware-Incident ist jedoch manuell aufwändig, mühsam und oft unüberwindbar.

Dell PowerProtect Backup Services erleichtern diesen Aufwand mit einer effektiven Backuparchitektur und automatisierten Tools zur Beschleunigung der Recovery. Die Cloud-Plattform der Dell PowerProtect Backup Services sichert Workloads direkt in der Cloud und ist für eine sofortige Recovery im Falle eines Ransomwareangriffs bereit.

Das beschleunigte Ransomware-Recovery-Modul ermöglicht Ihnen eine zuverlässige Recovery, indem es die Hygiene von Recovery-Daten sicherstellt. Sie können Snapshots mithilfe der integrierten Virenschutzerkennung oder mithilfe von Threat Intelligence aus Ihren eigenen forensischen Ermittlungen oder Bedrohungsdaten-Feeds auf Malware und IOCs scannen. Durch das Scannen von Snapshots vor der Recovery wird eine erneute Infektion vermieden.