DELL Technologies

Lösungsübersicht

Dell PowerProtect Cyber Recovery

Moderner und ausfallsicherer Schutz kritischer Daten vor Ransomware und destruktiven Cyberangriffen

Gute Gründe für Cyber Recovery

Cyberangriffe sind auf die Kompromittierung Ihrer wertvollen Daten ausgelegt – das schließt auch Backups mit ein. Der Schutz Ihrer kritischen Daten und eine Wiederherstellung mit sichergestellter Integrität ist nach einem Angriff der Schlüssel zur Rückkehr zu einem normalen Geschäftsbetrieb.

Im Folgenden sind die Komponenten einer cybersicheren Lösung aufgeführt:

Unveränderlichkeit von Daten
Erstellen Sie unveränderliche Datenkopien, um Integrität und Vertraulichkeit der Daten mithilfe von Sicherheitsebenen und Kontrollen zu schützen.

Automatisierte Datenisolierung
Isolieren Sie unveränderbare Datenkopien automatisch aus der Produktionsbackup-Umgebung in einen sicheren digitalen Vault mit strengerem eingeschränkten Zugriff.

Intelligente Analysen
Automatisierte Integritätsprüfungen mit KI-basiertem maschinellem Lernen und eine vollständige Inhaltsindexierung mit leistungsstarken Analysen werden innerhalb des sicheren Vaults durchgeführt, um festzustellen, ob Daten durch Malware beeinträchtigt wurden.

Recovery und Korrektur
Nach einem Incident wird mittels Workflows und Tools und unter Verwendung dynamischer Wiederherstellungsprozesse sowie bestehender Disaster-Recovery-Verfahren eine Recovery durchgeführt.

Lösungsplanung und -design
ExpertInnen beraten Sie bei der Auswahl von kritischen Datensätzen, Anwendungen und anderen wichtigen Ressourcen zur Ermittlung von RTOs und RPOs und zur Optimierung der Recovery.

Die Herausforderung: Cyberangriffe sind der Feind datengestützter Unternehmen.

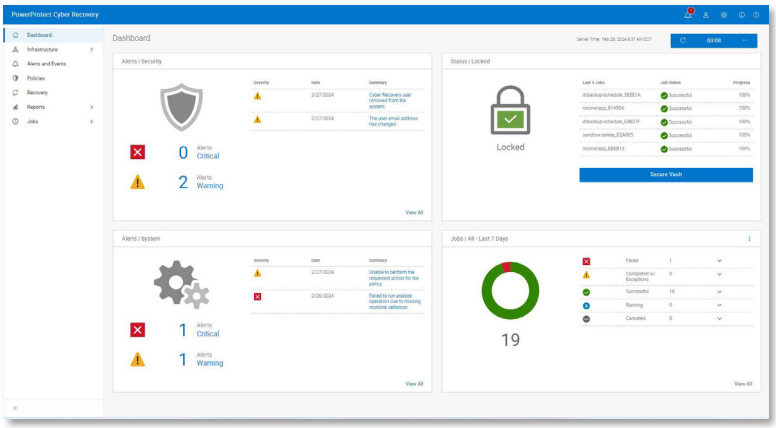
Daten sind die Währung der digitalen Wirtschaft und eine wichtige Ressource, die jederzeit geschützt und vertraulich bleiben und zugleich doch leicht zugänglich sein muss. Der moderne globale Markt ist auf einen kontinuierlichen Datenfluss in miteinander verbundenen Netzwerken angewiesen. Durch Initiativen zur digitalen Transformation und den zunehmenden Einsatz generativer KI steigt das Risiko, dass vertrauliche Informationen offengelegt werden.

Dadurch sind Unternehmensdaten für Cyberkriminelle ein attraktives und lukratives Angriffsziel. Unabhängig von der Branche oder der Unternehmensgröße sind Unternehmen und Behörden durch Cyberangriffe stets dem Risiko von infizierten Daten, Umsatzausfällen durch Ausfallzeiten, Rufschäden und teuren Ordnungsstrafen ausgesetzt.

Eine Strategie für die Ausfallsicherheit bei Cyberangriffen ist zu einem Muss für Führungskräfte in Unternehmen und Behörden geworden, doch vielen Unternehmen fehlt das Vertrauen in ihre Data-Protection-Lösungen. Laut dem Global Data Protection Index befürchten 79 % der IT-EntscheidungsträgerInnen, dass es in den nächsten 12 Monaten zu einer Unterbrechung Ihrer Geschäftstätigkeit kommen wird. 75 % befürchten, dass die vorhandenen Datenschutzmaßnahmen ihres Unternehmens nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen[1].

Die Lösung: Dell PowerProtect Cyber Recovery

Zur Verringerung der Geschäftsrisiken durch Cyberangriffe und für eine Data Protection mit verstärkter Ausfallsicherheit bei Cyberangriffen können Sie Ihre Recovery- und Business-Continuity-Strategien modernisieren und automatisieren. Gleichzeitig können Sie zur Entdeckung und Abwehr von Cyberbedrohungen die neuesten intelligenten Tools nutzen.



PowerProtect Cyber Recovery bietet einen bewährten, modernen, ausfallsicheren und intelligenten Schutz zur Isolierung kritischer Daten, der Erkennung verdächtiger Aktivitäten und einer beschleunigten Daten-Recovery, sodass Sie dank einer intelligenteren Wiederherstellung Ihrer kritischen Daten schnell wieder Ihren gewohnten Geschäftsbetrieb aufnehmen können. Laut Untersuchungen von Forrester Consulting trägt Dell PowerProtect Cyber Recovery dazu bei, die Ausfallzeit bei einem Cyberangriff um 75 % zu senken und den Stundenaufwand für die Recovery um 80 % zu reduzieren.[2]

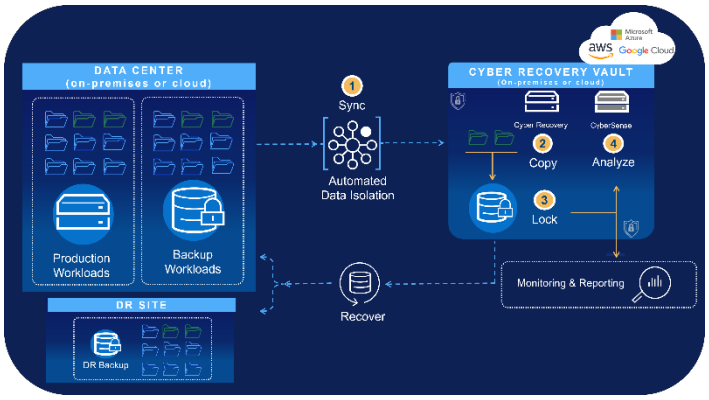
PowerProtect Cyber Recovery – Unveränderbarkeit, Isolierung und Intelligenz

Unveränderlichkeit – PowerProtect Data Domain

PowerProtect Data Domain ist die Grundlage von Dell PowerProtect Cyber Recovery. Mit mehreren Zero-Trust-Sicherheitsebenen werden unveränderliche Sicherungskopien erstellt, um die Integrität und die Vertraulichkeit der Daten zu gewährleisten. Funktionen wie Hardware Root of Trust, Secure Boot, Verschlüsselung, Aufbewahrungssperre, rollenbasierte Zugriffskontrolle und Multi-Faktor-Authentifizierung tragen zur Wiederherstellbarkeit Ihrer Daten bei.

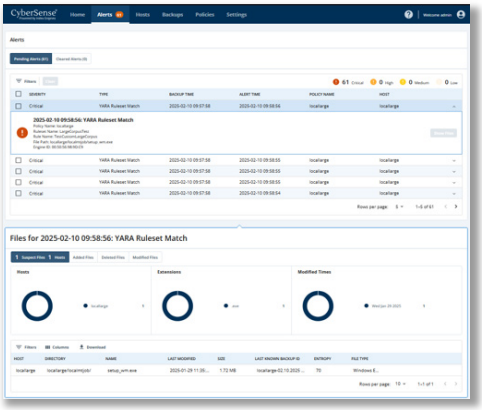
Isolierung – Cyber Recovery Vault

Der PowerProtect Cyber Recovery Vault ist eine isolierte Umgebung, die mehrere Sicherheitsebenen bietet. So sorgt er selbst bei Cyberangriffen durch Insider für Ausfallsicherheit. Die automatisierte Datenisolierung kopiert (synchronisiert) kritische Backupdaten (einschließlich Open Systems und Mainframe) sicher in einen physisch isolierten Vault, weg von der Angriffsfläche von Produktionsumgebungen, damit der Managementpfad zu keiner Zeit BedrohungsakteurInnen ausgesetzt ist. Im nächsten Schritt wird automatisch eine unveränderliche Kopie erstellt, um zu verhindern, dass die Daten abgeändert werden. Da Management, Netzwerk und Services dediziert angelegt sind und unabhängig von der Produktionsumgebung laufen, sind separate Sicherheitszugangsdaten und Multi-Faktor-Authentifizierung erforderlich, um für Recovery- und Testvorgänge auf die Daten zuzugreifen.



Intelligenz – CyberSense®

PowerProtect Cyber Recovery ist die erste Lösung mit vollständiger Integration von CyberSense® für eine intelligentere Recovery bei Cyberbedrohungen – alles im Rahmen des sicheren Cyber Recovery Vault. CyberSense geht über reine Metadatenlösungen hinaus: Es analysiert den gesamten Inhalt. So werden beschädigte Daten nach einem Angriff mit einer Genauigkeit von 99,99 % erkannt[3] und eine intelligente und schnelle Wiederherstellung ermöglicht. CyberSense nutzt unveränderliche Datenbackups, um zu beobachten, wie sich Daten im Laufe der Zeit verändern, und setzt KI-basiertes maschinelles Lernen ein, um Anzeichen von Beschädigungen zu erkennen, die auf einen Ransomwareangriff hindeuten. Außerdem erkennt CyberSense Massenlöschungen, vollständige und teilweise Verschlüsselungen und andere verdächtige Änderungen in der Kerninfrastruktur (einschließlich Active Directory, DNS usw.), in Nutzerdateien und in Datenbanken, die aus ausgeklügelten Angriffen resultieren. Sie können nutzerdefinierte Schwellenwertwarnmeldungen erstellen. Sollten Anzeichen einer Beschädigung erkannt werden, ermöglichen das Warnmeldungs-Dashboard und die forensischen Berichte nach dem Angriff eine schnelle Diagnose des Ausmaßes und der Auswirkungen der Attacke. Außerdem wird eine saubere Kopie der Daten zur Wiederherstellung Ihrer kritischen Systeme identifiziert. Benutzerdefinierte YARA-Regeln und die Malwaresignatursuche unterstützen Unternehmen dabei, sich proaktiv gegen Cyberbedrohungen zu verteidigen.



PowerProtect Cyber Recovery – Bereitstellungsoptionen

Cyber Recovery in Hybrid- und Multi-Cloud-Umgebungen

Kritische Daten eines Unternehmens können sich an vielen verschiedenen Orten befinden, sei es On-Premise, in verschiedenen Rechenzentren oder weltweit in unterschiedlichen Clouds und Regionen. Unabhängig vom Speicherort müssen die Daten sicher und unkompromittiert sein, wenn eine Wiederherstellung nach einem Cyberangriff erforderlich ist.

PowerProtect Cyber Recovery ist über Public-Cloud-Marktplätze für *AWS, Microsoft Azure* und *Google Cloud* verfügbar und transaktionsfähig, um einen schnellen Zugriff und damit den Schutz von Daten in einem Cyber Recovery Vault in der Cloud zu ermöglichen. PowerProtect Cyber Recovery automatisiert die Synchronisation kritischer Daten zwischen Produktionssystemen und dem Cyber Recovery Vault in der Public Cloud. Im Gegensatz zu cloudbasierten Standardbackuplösungen ist der Zugriff auf Managementschnittstellen durch Netzwerkkontrollen gesperrt und erfordert separate Sicherheitszugangsdaten und Multi-Faktor-Authentifizierung für den Zugriff. Daten über mehrere Clouds hinweg zu streuen und zu duplizieren, kann allerdings zu Sicherheits- und Compliancerisiken, potenziellen Synchronisationsproblemen und erhöhten Ressourcenkosten führen. Zusätzlich kann dieser Ansatz die Sichtbarkeit in Ihren verschiedenen Umgebungen reduzieren, was zu einem unzureichenden Schutz vor sich ständig weiter entwickelnden Cyberbedrohungen führt.

Dell PowerProtect Data Domain All-Flash Ready Node

Die Menge an kritischen Daten nimmt ständig zu. Darum ist es für die Gewährleistung von Business Continuity und Ausfallsicherheit bei Cyberangriffen entscheidend, in der Lage zu sein, sich schnell und effizient von einem Cybereereignis zu erholen. Unternehmen, die das Management kritischer Daten erweitern, benötigen eine zuverlässige Lösung dafür, ihre Daten aus isolierten Recovery-Umgebungen wie dem Cyber Recovery Vault abzurufen. Dell PowerProtect Data Domain All-Flash Ready Node bietet eine optimierte, energie- und kosteneffiziente Cyber Recovery-Lösung mit verbesserten CyberSense-Analysen und schnellen Wiederherstellungsfunktionen, um Unternehmens-SLAs zu erfüllen. Weniger Hardware-, Platz- und Energiebedarf bedeutet für Unternehmen, dass sie den Datenzugriff beschleunigen, die Betriebseffizienz steigern und die Datenintegrität sicherstellen können, was letztendlich zu geringeren Ausfallzeiten und einer Senkung der allgemeinen Wartungskosten führt.

PowerProtect Cyber Recovery – Schnell wieder im Geschäft

Recovery und Korrektur

PowerProtect Cyber Recovery bietet automatisierte Wiederherstellungs- und Recovery-Verfahren, sodass geschäftskritische Systeme rasch und verlässlich wieder online gebracht werden können. Die Recovery ist in Ihren Incident-Response-Prozess integriert. Nach einem Ereignis analysiert das Incident-Response-Team die Produktionsumgebung, um die Ursache des Ereignisses zu ermitteln. CyberSense bietet forensische Berichte nach einem Angriff, um die Reichweite und den Umfang des Angriffs zu verstehen. Die Lösung stellt auch eine Liste der letzten fehlerfreien Backupsätze vor der Beschädigung bereit. Wenn die Produktion dann für die Recovery bereit ist, stellt Cyber Recovery Managementtools und die Technologie zur Verfügung, mit denen die tatsächliche Daten-Recovery durchgeführt wird.

Lösungsplanung und -design

Dell Professional Services für Cyber Recovery helfen Ihnen bei der Ermittlung, welche geschäftskritischen Systeme geschützt werden sollen. Anwendungs- und Serviceabhängigkeiten können dargestellt werden und die notwendige Infrastruktur zu ihrer Wiederherstellung wird ermittelt. Der Service formuliert auch Wiederherstellungsvoraussetzungen sowie Designalternativen und identifiziert Technologien zur Analyse, dem Hosting und dem Schutz Ihrer Daten zusammen mit einem Business Case und einer Zeitskala für die Implementierung.

Fazit

Brancheninitiativen wie Sheltered Harbor nutzen PowerProtect Cyber Recovery, um KundInnen, Finanzinstitute und das Vertrauen der Öffentlichkeit in das US-Finanzsystem im Falle eines Cyberangriffs zu schützen, der zum Ausfall kritischer Systeme führt – Backups eingeschlossen. Tausende von KundInnen vertrauen auf Cyber Recovery mit CyberSense. Die Lösung gibt Führungskräften Sicherheit und beschleunigt nachweislich die Recovery von Daten im Falle einer Cyberbedrohung.

PowerProtect Cyber Recovery verschafft Ihnen die Zuversicht, dass Sie nach einem Cyberangriff zweifelsfrei funktionierende Daten schnell identifizieren und wiederherstellen und zum normalen Geschäftsbetrieb zurückkehren können.

So kann Sie nichts aufhalten.

Weitere Informationen zu Dell PowerProtect Cyber Recovery

Kontakt zum Dell Technologies Expertenteam

Weitere Ressourcen

Reden Sie mit: #PowerProtect

[1] Basierend auf einer von Dell Technologies in Auftrag gegebenen Studie von Vanson Bourne, „Global Data Protection Index 2024 Snapshot“. Oktober 2023.
[2] Eine im Auftrag von Dell Technologies durch Forrester Consulting durchgeführte Studie, „Total Economic Impact von Dell PowerProtect Cyber Recovery“, August 2023
[3] Basierend auf dem von Index Engines in Auftrag gegebenen ESG-Bericht „Index Engines’ CyberSense Validated 99.99% Effective in Detecting Ransomware Corruption“. Juni 2024