

MAI 2024

Dell PowerStore-Ausfallsicherheit

Craig Ledo, IT Validation Analyst

IT-Herausforderungen

Die Studie der Enterprise Strategy Group von TechTarget zeigt, dass die Verbesserung der Cybersicherheit und der Ausfallsicherheit bei Cyberangriffen (44 %) sowie die Verbesserung von Geschäftsprozessen und Workflows (36 %) die wichtigsten Erwägungen sind, um IT-Investitionen für das Geschäftsmanagement im Jahr 2024 zu rechtfertigen (siehe Abbildung 1).¹ Unternehmen wissen, dass sie ihre Policies für Ausfallsicherheit und Cybersicherheit verbessern müssen, aber angesichts der steigenden Anforderungen an IT-Fachleute wissen sie auch, dass sie es sich nicht leisten können, die Komplexität zu erhöhen.

Abbildung 1. Wichtigste Überlegungen zu IT-Investitionen – Verbesserung von Cybersicherheit und Ausfallsicherheit

Welche der folgenden Überlegungen werden Ihrer Meinung nach in den nächsten 12 Monaten bei der Rechtfertigung von IT-Investitionen gegenüber der Geschäftsleitung Ihres Unternehmens die größte Rolle spielen?
(Prozent der Befragten, N=903, fünf Antworten möglich)



Quelle: Enterprise Strategy Group, ein Unternehmensbereich von TechTarget, Inc.

¹ Quelle: Enterprise Strategy Group Research Report, [2024 Technology Spending Intentions Survey](#), Februar 2024.

Dieser Technical First Look der Enterprise Strategy Group wurde von Dell Technologies in Auftrag gegeben. Die Verbreitung erfolgt mit Genehmigung von TechTarget, Inc.

Dell PowerStore-Ausfallsicherheit

Dell Technologies hat kürzlich PowerStore Prime angekündigt, ein umfassendes, integriertes Angebot, das neue Fortschritte im All-Flash-Storage mit strategischen Geschäftsvorteilen kombiniert. PowerStore Prime umfasst sowohl Produkt- als auch Programmkomponenten, mit denen Unternehmen die einzigartige Position von Dell als führender Technologieanbieter nutzen können. Dazu gehören auch das umfassende Enterprise-Portfolio des Unternehmens und sein globales Netzwerk zuverlässiger Partner und Distributoren.

PowerStore Prime bietet eine Reihe von Verbesserungen bei den Ausfallsicherheitsfunktionen der Plattform, darunter:

- **Umfassendere Betriebssystemunterstützung** für die beliebte Metro-Volume-Funktion, die jetzt neben VMware auch Windows- und Linux-Umgebungen unterstützt. Metro Volume bietet Aktiv-Aktiv-Verfügbarkeit mit einem Zero Recovery Time Objective (RTO) und einem Zero Recovery Point Objective (RPO) für jede Workload, mit vollständig automatisiertem Failover/Failback über einen dritten Standort und Unterstützung für Volumes und Volume-Gruppen.
- **Neue synchrone Replikation für Datei und Block**, die eine 100%ige Datenintegrität über Standorte hinweg ohne Datenverlust gewährleistet und die Möglichkeit bietet, Volumes, Volume-Gruppen und NAS-Server (Network Attached Storage) über mehrere Cluster hinweg zu schützen.
- **Unterstützung für bis zu 3-mal mehr Snapshots und 8-mal mehr Replikations-Volumes**, um mehr Workloads lokal oder standortübergreifend zu schützen.

Diese Verbesserungen ergänzen die vorhandenen Ausfallsicherheitsfunktionen von PowerStore, die jetzt die folgenden umfassenden Schutzmethoden für lokale, Remote- und Cloud-Anwendungen sowie robuste Cybersicherheit einschließen.

Lokaler Schutz

PowerStore ermöglicht es NutzerInnen, Daten auf lokalen PowerStore-Arrays effizient zu managen, zu schützen und wiederherzustellen.

- Die **Dynamic Resiliency Engine** schützt vor gleichzeitigen Ausfällen mehrerer Laufwerke und bietet intelligentes Management von Leistung und Effizienz.
- **Sichere und unveränderliche lokale Snapshots** stellen sicher, dass ein einmal erstellter Snapshot bis zu einem vorab festgelegten Ablaufdatum nicht geändert oder gelöscht werden kann. Diese dienen als authentischer Referenzpunkt für die Datenwiederherstellung.
- **File-Level Retention (FLR)** (Aufbewahrung auf Dateiebene) hilft bei der Verwaltung und Sicherung von filebasierten Daten, indem filebasierte Daten bis zu einem bestimmten Aufbewahrungsdatum vor Löschung oder Änderung geschützt sind. Die Funktion wurde entwickelt, um die Anforderungen der Vorschrift 17a-4(f) der Börsenaufsicht SEC zu erfüllen.

Remoteschutz

Mit PowerStore können NutzerInnen sicherstellen, dass Daten über Entfernungen hinweg zugänglich und sicher bleiben.

- Die **asynchrone Replikation** schützt Block-, Datei- oder Virtual Volumes (vVols)-Daten über geografisch entfernte Rechenzentren oder Disaster-Recovery-Standorte hinweg für RPO-basierte Business Continuity, wobei Failover/Failback vollständig von Dell PowerStore gehandhabt wird.
- Die **synchrone Replikation** schützt Block- und filebasierte Daten über lokale Rechenzentren oder Disaster-Recovery-Standorte hinweg mit einem RPO von Null für Business Continuity, wobei Failover/Failback vollständig von Dell PowerStore gehandhabt wird.

- Die **synchrone Metro-Volume-Replikation** (aktiv/aktiv) ermöglicht eine erfolgskritische, unterbrechungsfreie Verfügbarkeit über größere Entfernungen (60 Meilen bzw. 100 Kilometer) für Windows-, Linux- und VMware-Workloads und umfasst eine Witness-Funktion für einen dritten Standort für automatisches Failover/Failback, wodurch „Split-Brain“-Szenarien vermieden werden.
- **Integriertes Remotebackup** auf physische oder virtualisierte Dell PowerProtect DD-Appliances ist eine einfache und effiziente Möglichkeit, Backups direkt in PowerStore zu managen.

Cloud-Backup und -Mobilität

Mit PowerStore können Unternehmen Daten für Skalierbarkeit, Kosteneffizienz oder Datenredundanz in die Cloud verschieben.

- **Integriertes Cloud-Backup** verlagert Daten auf Dell APEX Protection Storage for Public Cloud für eine kosteneffiziente Cloud-Archivierung mit verbesserter Datenreduzierung und schneller Recovery bei jedem Public-Cloud-Anbieter.
- **APEX-Abonnements** ermöglichen eine einfache Bereitstellung von Storage as a Service-Ressourcen in einer vernetzten Colocation-Einrichtung eines Drittanbieters sowie im Rechenzentrum oder am Edge-Standort des Unternehmens.
- **Bidirektionale Workload-Mobilität** zwischen PowerStore und APEX Block Storage for Public Cloud

Cybersicherheit

PowerStore versetzt Unternehmen in die Lage, den heutigen Cybersicherheitsbedrohungen einen Schritt voraus zu sein.

- Die **native Data-at-Rest-Verschlüsselung** umfasst die Unterstützung für einen externen Key-Manager und selbstverschlüsselnde Datenträger.
- **Integrierte Hardwaresicherheit** umfasst unveränderlichen hardwareseitigen Root of Trust, Secure Boot-Vertrauenskette und digital signierte Firmwareupdates.
- **Erweiterte Bedrohungserkennung** umfasst Abweichung in der Sicherheitskonfiguration, sichere Syslog-Ereignisse und -Exporte sowie Virenschutz und Ereignisveröffentlichung.
- **Zugriffskontrolle für vertrauenswürdige AdministratorInnen** bietet Unterstützung für Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrolle (Role-Based Access Control, RBAC) sowie Unterstützung für LDAP (Lightweight Directory Access Protocol).
- Zu den **Sicherheitszertifizierungen** zählen STIGs (Security Technical Implementation Guides), NIST USGv6-r1 und Federal Information Processing Standards 140-2. PowerStore steht auch auf der vom US-Verteidigungsministerium genehmigten Produktliste (APL) für den Einsatz in DoD-Informationsnetzwerken.

PowerStore ist für hohe Verfügbarkeit konzipiert. Durch Sicherstellung der ununterbrochenen Workload-Verfügbarkeit wird so ein kontinuierlicher Datenzugriff gewährleistet.

First Look

Die Enterprise Strategy Group überprüfte die neuen Funktionen der Dell PowerStore Prime-Lösung und bewertete, wie KundInnen davon profitieren würden. PowerStore Prime bietet lokale, Remote- und Cloud-Data-Protection-Funktionen, die sicherstellen, dass die Daten eines Unternehmens hochverfügbar und ausfallsicher gegen Cyberbedrohungen sind. Die Lösung bietet die folgenden wichtigen Vorteile:

- **Einfachheit:** Ermöglicht es NutzerInnen, Daten auf jedem PowerStore-Array effizient zu managen, zu schützen und wiederherzustellen.
- **Zugänglichkeit:** Stellt sicher, dass Daten über Entfernungen hinweg zugänglich, mobil und sicher bleiben.
- **Mobilität:** Verschieben Sie Daten einfach in die Cloud für bessere Skalierbarkeit, Kosteneffizienz oder Datenredundanz.

- **Stabilität:** Schutz von Daten mit 99,9999 % Verfügbarkeit

PowerStore ermöglicht es NutzerInnen, schnell und einfach Schutzebenen auf einzelne Workloads anzuwenden. In einem einzigen Workflow können NutzerInnen auf fünf verschiedene Arten von Data Protection zugreifen und nutzerdefinierte Policies erstellen, um Snapshots, mehrere Arten der Replikation und Cloud-Backups gleichzeitig auf eine beliebige Anzahl von Volumes anzuwenden.

Fazit

Die Herausforderungen, die mit dem Aufbau, der Pflege und der Weiterentwicklung von immer größer werdenden Daten- und Storage-Infrastrukturen verbunden sind, bestehen weiterhin, doch die potenziellen geschäftlichen Vorteile, die sich aus der richtigen Umsetzung ergeben, waren noch nie so aufregend wie heute. Während IT-Abteilungen auf die sich entwickelnde Cybersicherheitslandschaft reagieren, werden die Storage-Infrastruktur und der Schutz von Daten immer wichtiger. Beispielsweise sind Backups jetzt ein primärer Angriffsvektor für Ransomware, wodurch sie die besten Chancen eines Unternehmens auf eine schnelle Recovery nach einem Angriff zunichte machen. Um sich vor Ransomware-Angriffen zu schützen, sollten Unternehmen die in ihre primäre Storage-Umgebung integrierten Sicherheitstools nutzen, z. B. sichere und unveränderliche Snapshots, die eine schnelle Recovery von vertrauenswürdigen, Point-in-Time-Backups ermöglichen, sowie FLR, das die Verwaltung und Sicherung filebasierter Daten unterstützt. Es gibt keine Garantie für einen vollständigen Schutz, aber Storage wird zu einem wichtigen Tool im Rahmen einer Cybersicherheitsstrategie.

Die Enterprise Strategy Group kam zu dem Ergebnis, dass die Dell PowerStore-Lösung Unternehmen erweiterte Funktionen für die lokale, Remote- und Cloud-Data-Protection zum Schutz von Workloads bieten kann. PowerStore bietet außerdem robuste Sicherheitsimplementierungen, die Unternehmen dabei unterstützen, die Einführung von Zero-Trust-Cybersicherheitsmodellen zu beschleunigen, um ihre Daten besser zu schützen, Cyberangriffe zu verhindern und darauf zu reagieren. Darüber hinaus haben wir festgestellt, dass PowerStore umfassende Data-Protection-Funktionen bietet, die sehr einfach zu verwalten sind und dazu beitragen, die Möglichkeit von Fehlern auszuschließen.

Wenn Ihr Unternehmen seine Datenschutzfunktionen mit einem ganzheitlichen Ansatz modernisieren möchte, der lokale, Remote- und Cloud-Daten umfasst und gleichzeitig den Verwaltungsaufwand minimiert, sollten Sie Dell PowerStore Prime in Betracht ziehen.

Weitere Informationen zu Dell PowerStore finden Sie unter [Dell Technologies PowerStore](#).

©TechTarget, Inc. oder deren Tochtergesellschaften. All rights reserved. TechTarget und das TechTarget-Logo sind Marken oder eingetragene Marken von TechTarget, Inc. und in Gerichtsbarkeiten weltweit registriert. Andere Produkt- und Servicenamen sowie Logos, einschließlich BrightTALK, Xtelligent und Enterprise Strategy Group, können Marken von TechTarget oder deren Tochtergesellschaften sein. Alle anderen Marken, Logos und Markennamen sind das Eigentum ihrer jeweiligen Inhaber.

Die Informationen in dieser Veröffentlichung stammen aus Quellen, die TechTarget als zuverlässig ansieht. TechTarget übernimmt jedoch keine Haftung für diese Informationen. Dieses Dokument kann Meinungen von TechTarget enthalten, die sich ändern können. Es enthält möglicherweise Prognosen, Vorhersagen und andere vorausschauende Aussagen, die die Annahmen und Erwartungen von TechTarget gemäß derzeit verfügbaren Informationen darstellen. Diese Prognosen basieren auf Branchentrends und beinhalten Variablen und Unsicherheiten. Folglich übernimmt TechTarget keine Haftung für die Genauigkeit bestimmter hierin enthaltener Prognosen, Vorhersagen oder vorausschauender Aussagen.

Die komplette oder teilweise Vervielfältigung und/oder Verbreitung dieser Publikation in gedruckter, elektronischer oder sonstiger Form für bzw. an nicht berechnete Personen ohne ausdrückliche Zustimmung von TechTarget stellt einen Verstoß gegen die Urheberrechtsgesetze der USA dar und wird mit zivilrechtlichen Klagen geahndet, gegebenenfalls auch strafrechtlich verfolgt. Wenden Sie sich bei Fragen an Client Relations unter cr@esg-global.com.

Informationen zu Enterprise Strategy Group

Enterprise Strategy Group von TechTarget bietet fokussierte und umsetzbare Marktinformationen, nachfrageorientierte Studien, Beratungsdienste durch AnalystInnen, GTM-Strategieberatung, Lösungsvalidierungen und kundenspezifische Inhalte, die den Kauf und Verkauf von Unternehmenstechnologie unterstützen.

 contact@esg-global.com

 www.esg-global.com