DELL Technologies

Whitepaper

Dell PowerProtect

Leverage Dell PowerProtect to Enhance your Cyber Resilience Strategy

Abstract

As cyberattacks become more frequent and sophisticated, organizations need proven solutions to safeguard critical data and maintain operational continuity. The impact of these attacks spans financial losses, reputational damage, and operational disruptions, necessitating a robust cyber resilience strategy.

Dell PowerProtect solutions are designed to meet these challenges head-on, providing essential protection and recovery capabilities to help organizations stay resilient in a constantly evolving threat landscape. This whitepaper offers IT professionals, data security experts, and IT managers essential insights to strengthen organizational resilience against evolving cyber risks.

January 2026

Table of Contents

Introduction

Data is the engine of human progress. It empowers organizations to serve customers, drive innovation, and achieve their most ambitious goals. In our increasingly connected world, protecting this vital asset is more critical than ever. However, the landscape of cyber threats is evolving at an unprecedented pace. Sophisticated attacks, including ransomware and AI-driven social engineering, target organizations of every size and industry, threatening not just data, but business continuity and trust.

To counter these advanced threats, organizations must move beyond traditional security measures and embrace a strategy of cyber resilience.

What is Cyber Resilience?

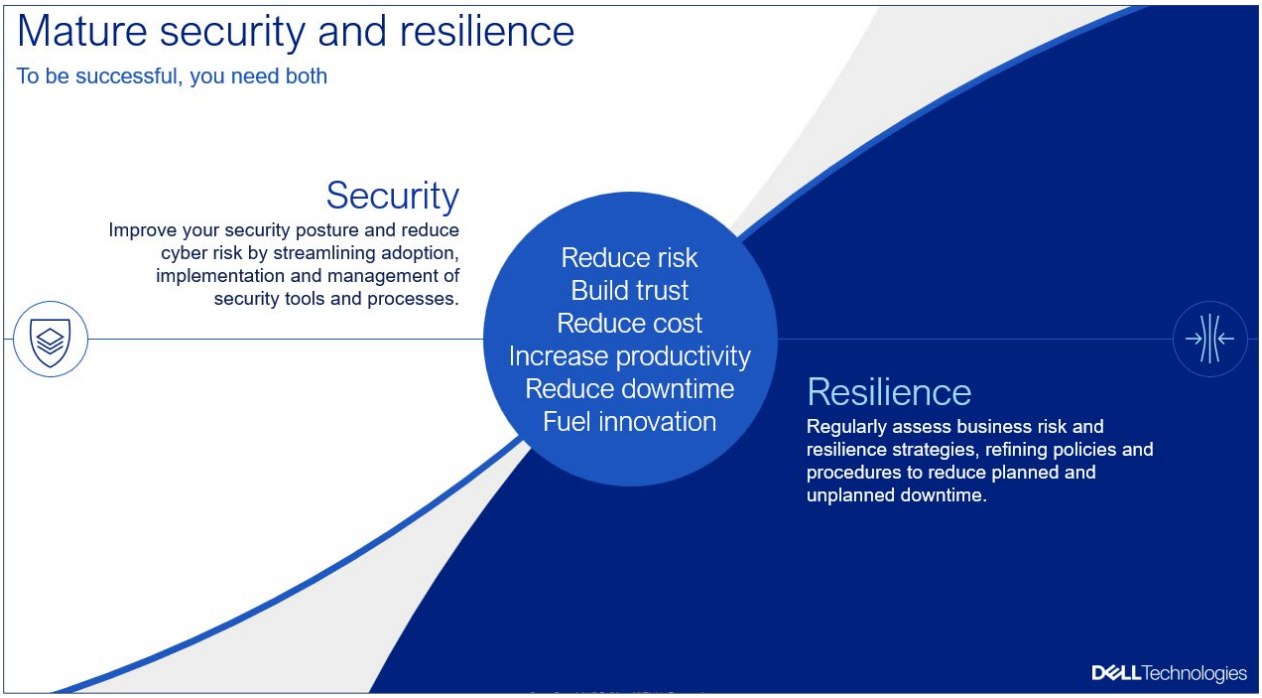
NIST defines Cyber resilience as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. It is a strategy that includes cybersecurity capabilities but focuses on ensuring business outcomes can be delivered continuously, even in the face of an attack.[1]

A cyber-resilient organization can not only defend against daily threats but also maintain essential operations during an incident and restore systems in a timely, efficient, and secure manner.

How Cybersecurity and Cyber Resilience work together?

Cybersecurity and cyber resilience serve distinct but complementary roles in protecting organizations. Cybersecurity focuses on preventing, detecting, and responding to threats by implementing controls and defense measures that safeguard systems and data. In contrast, cyber resilience emphasizes the ability to continue operations and quickly recover when disruptions or attacks occur.

When these two approaches work together, organizations not only strengthen their defenses to block and identify threats but also ensure they have robust strategies in place to adapt, recover, and maintain business continuity during any incident. This integration leads to a comprehensive security posture that not only reduces risk but empowers teams to move forward with confidence, even in the face of evolving threats.



Ransomware attacks have become the new normal for IT organizations with backup data being the prime target for hackers. From the Dell Cyber Resilience Insights Report, Organizations with mature resilience strategies are nearly 3x more likely to recover successfully from cyber threats.[2] A modern cyber resilience strategy must therefore start by strengthening the data protection environment. Capabilities such as data immutability, operational air gaps, and AI-powered anomaly detection, can empower organizations to build a resilient framework that protects their data from corruption or loss. This paper will explore how leveraging Dell Cyber Resilience capabilities can substantially enhance your organization's resilience posture and mature its recovery capabilities for a more secure future.

Secure, Detect and Recover

To build a strong foundation for cyber resilience, Dell emphasizes three critical practice areas: **Secure, Detect, and Recover**. These work together to create a comprehensive approach to protecting, monitoring, and restoring your organization's digital environment.

- **Secure** is focused on reducing the attack surface and minimizing the vulnerabilities that penetrate an organization. This includes implementing robust access controls, encrypting sensitive data, and ensuring your systems have the latest up to date patches to protect against vulnerabilities. The goal is to make it as difficult as possible for threat actors to breach your environment.
- **Detect** is focused on identifying potential security incidents and malicious activities as quickly as possible and responding to them. This involves leveraging advanced monitoring tools, threat intelligence, and analytics to quickly spot suspicious activity. Early detection is critical to minimizing the impact of an attack and preventing it from spreading further.
- **Recover** is focused on restoring the organization as quickly as possible while minimizing disruption. Even with the best security and detection measures, breaches can still happen. This practice area ensures your organization can restore operations quickly and effectively, minimizing downtime and data loss. This includes having robust backup and recovery solutions, as well as a well-defined incident response plan.

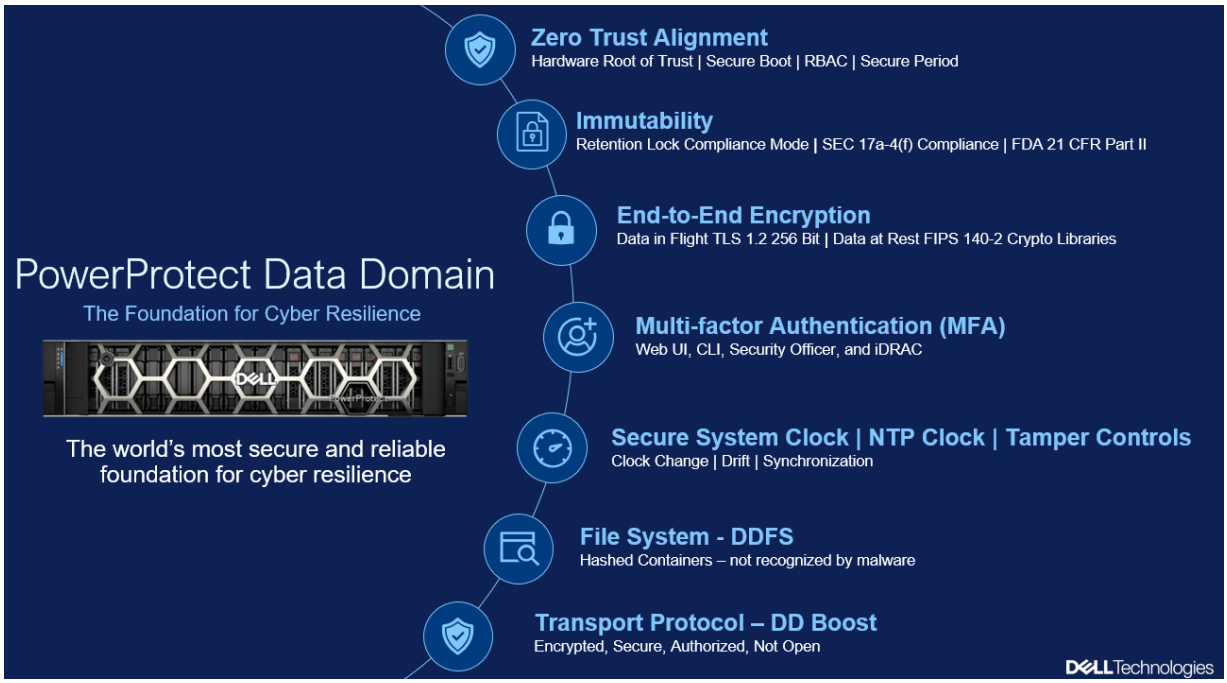
Together, these three practice areas form a holistic approach to cyber resilience, ensuring your organization is prepared to withstand and recover from cyber threats. The PowerProtect portfolio is designed with these practice areas in mind to help organizations continue business operations.

PowerProtect Data Domain, the foundation of Cyber Resilience

In an era of evolving cyber threats, taking decisive action to fortify your data protection infrastructure is not just a defensive move—it's a strategic step forward. Organizations can significantly advance their cyber resilience by leveraging the built-in capabilities of Dell Cyber Resilience solutions. Because threat actors frequently target backup infrastructure to gain leverage, hardening this environment is a critical priority.

Dell PowerProtect Data Domain series appliances provide a powerful and trusted foundation for these efforts. They are designed with innovative features that empower organizations to protect their data, adapt to new threats, and ensure recoverability.

Dell PowerProtect Data Domain systems provide an excellent foundation for these capabilities:



An organization seeking to quickly improve its cyber resilience should immediately evaluate the following capabilities which are built into Dell Cyber Resilience Solutions:

- **Enable retention lock.** Data immutability is a cornerstone of modern data protection. PowerProtect Data Domain Retention Lock helps protect data from being changed or deleted during a specified locking period. This feature is instrumental in creating a secure, unalterable copy of your critical data. The Governance mode balances operational flexibility with security, while the Compliance mode offers the highest level of protection by preventing any overrides, even by an administrator. This capability is essential for meeting stringent regulatory requirements and ensuring data integrity against sophisticated attacks.
- **Protect Against Destructive Commands.** When you enable Retention Lock in Compliance mode, you also activate additional safeguards. Certain destructive commands, such as resetting the file system, are disabled. Other sensitive commands can still be run, but they require authorization from a second, security-officer role. This dual-authorization model implements a crucial separation of duties, making it significantly harder for a single compromised account to inflict widespread damage.
- **Use DD Boost.** A common point of ransomware attacks is a CIFS or NFS share that is used by the backup data mover to write data to a storage target. DD Boost eliminates this mount point and also provides operational efficiencies.
- **Leverage deduplication.** The superior deduplication technology built into PowerProtect Data Domain dramatically reduces the storage footprint required for backups. This efficiency is not just about saving costs; it delivers a powerful security advantage. A smaller storage footprint means fewer components to manage, monitor, and protect. By minimizing the attack surface, you simplify your security posture and reduce potential vulnerabilities.

Deploy Capabilities Supporting Zero Trust Principles

All Dell Cyber Resilience Solutions are built with features that support a Zero Trust architecture, a framework that assumes no user or device is inherently trustworthy. Key features include:

- **Role based access controls.** Proper definition of roles can help to implement the principle of least privilege, which allows user to only perform functions necessary to their roles.

- **Persistent logging functionality.** Logs can be fed to the Security and Incident Event Management (SIEM) system, provide auditing trails and help with forensic reviews and investigations.
- **Encryption of data at rest and in flight.** Encrypting data is a well-established control to protect the confidentiality of information.
- **Multi-factor authentication.** Many organizations are implementing multi-factor authentication as a protection against bad actors stealing or identifying used or previously compromised credentials.
- **Local and external key management.** Key management helps to ensure that encryption keys can be rotated to protect against compromise, while also making the management of those keys safe and efficient.

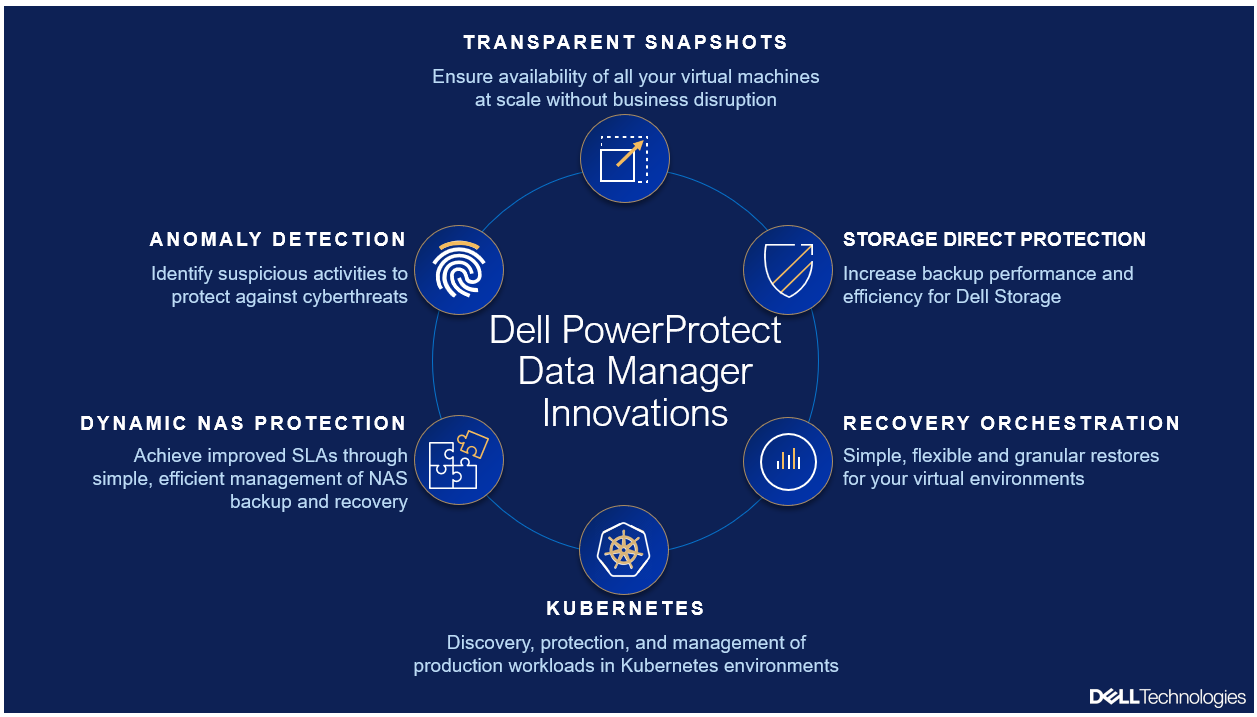
By implementing these powerful, integrated features, you can take immediate and meaningful steps to strengthen your organization's cyber resilience. Dell PowerProtect Data Domain provides the technology to not only defend against today's threats but also to build a more secure and confident future.

PowerProtect Data Manager, a cyber resilience software platform for modern, multicloud workloads

In today's complex IT landscape, cyber resilience has evolved beyond traditional backup and restore. Dell PowerProtect Data Manager delivers a software-defined platform built on three pillars: modern protection innovation, simple autonomous operations and resilient security capabilities. Data Manager protects traditional databases including Oracle, Microsoft SQL Server, Microsoft Exchange and SAP HANA, alongside Kubernetes containers, AI workloads on Dell infrastructure, virtualized environments across VMware vSphere, Microsoft Hyper-V and Nutanix AHV, distributed edge infrastructure on Dell NativeEdge and file systems spanning on-premises, hybrid cloud and multicloud deployments. PowerProtect Data Manager empowers organizations to modernize their cyber resilience strategy with automated discovery, self-service capabilities and intelligent threat detection, ensuring assets are secure, compliant and always available. PowerProtect Data Manager can be consumed as standalone software or as an integrated appliance.

Centralized Governance and Orchestration

PowerProtect Data Manager delivers a single, intuitive interface for overseeing your entire cyber resilience ecosystem. This centralized management approach reduces administrative overhead and eliminates the need to juggle multiple point solutions. From this one console, you can automate policies, monitor backup and recovery jobs and ensure compliance across all your workloads. This gives you the power to manage protection for physical servers, virtual machines, modern cloud-native applications, file systems and AI workloads with consistent, simplified oversight.



Key capabilities include:

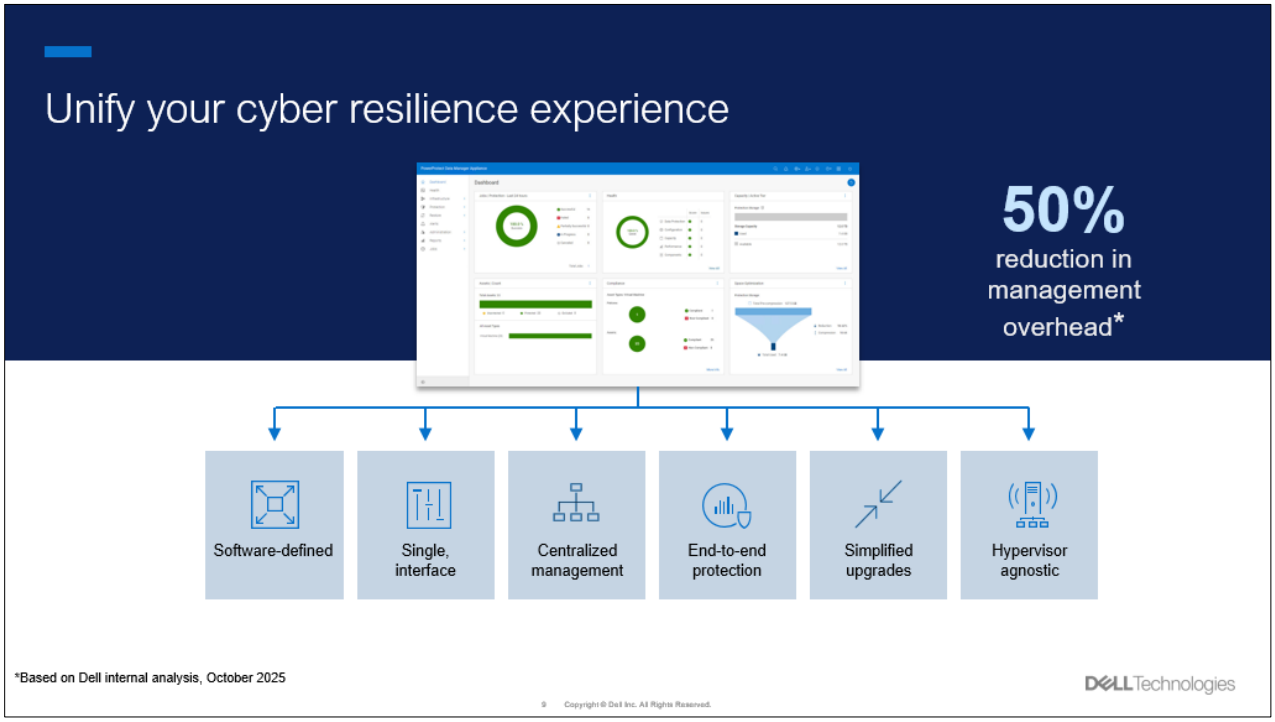
- **Automated Discovery and Protection:** Intelligently discover and protect assets across your environment, including VMs, file systems, and databases, ensuring no critical data is left unprotected.
- **Multi-Hypervisor Flexibility:** Extend consistent cyber resilience across VMware vSphere, Hyper-V and Nutanix AHV through unified management, enabling infrastructure decisions based on business requirements rather than protection limitations.
- **Edge-to-Core Cyber Resilience:** Deliver industry-first protection for Dell NativeEdge edge computing environments with image-level protection for KVM virtual machines, extending enterprise capabilities to edge deployments.
- **Anomaly Detection:** Leverage machine learning to monitor backup environments for unusual patterns and suspicious activity, helping detect deviations that may signal threats and ensuring backup data integrity.
- **Transparent Snapshots:** Provide space-efficient, rapid recovery points without disrupting operations. Eliminate application disruption during backups by removing the need to pause VMs while reducing infrastructure complexity.
- **Storage Direct Protection:** Back up databases and workloads from Dell PowerStore and PowerMax directly to PowerProtect Data Domain, bypassing application servers for improved efficiency, faster backups and simplified operations.
- **Recovery Orchestration:** Automate the recovery process across applications, databases and environments with policy-driven workflows, ensuring critical services are restored quickly to accelerate business continuity.
- **Archive to Object:** Enable policy-driven archiving to Azure, Dell ObjectScale and Wasabi for long-term retention with direct restore capability, addressing data growth challenges at no additional licensing cost.
- **Self-Service Capabilities:** Empower application owners and database administrators with self-service backup and recovery capabilities, freeing IT teams to focus on strategic initiatives while maintaining centralized governance.

Versatility for the modern data estate

Your data lives everywhere, and your protection strategy must be just as flexible. PowerProtect Data Manager is built for the modern, distributed enterprise, offering unmatched deployment versatility. Whether you are protecting traditional data center workloads, leveraging public cloud infrastructure, or operating in a hybrid model, Data Manager adapts to your needs.

It seamlessly integrates with PowerProtect Data Domain for industry-leading deduplication and efficiency. This integration extends to the cloud with Dell PowerProtect Data Domain Virtual Edition, allowing you to extend protection to and from the cloud while optimizing storage costs and bandwidth. This versatility ensures you can build a future-ready cyber resilience strategy that evolves with your business.

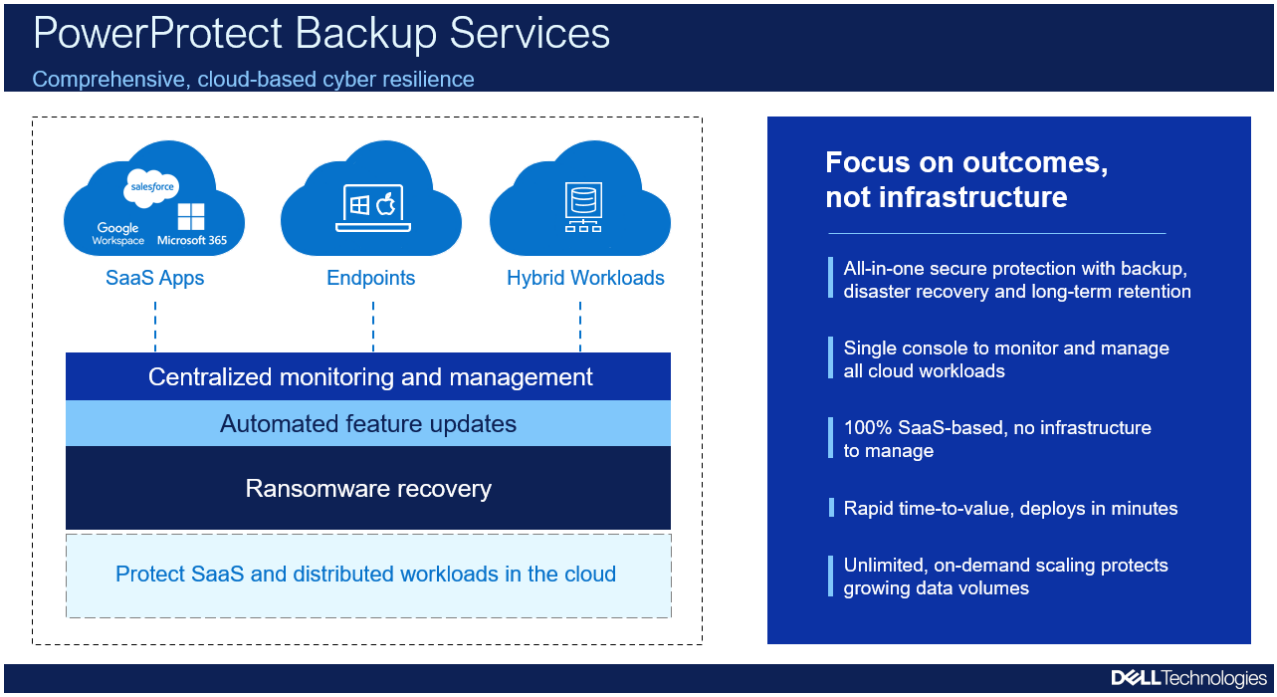
The new PowerProtect Data Manager Appliance is a software-defined solution that takes scalability, flexibility, and performance to the next level. The Data Manager Appliance is the best way to achieve cyber resilience with Dell PowerProtect via an integrated appliance offer. With a single, easy-to-manage interface, you get consistent backup and storage operations without the hassle all while reducing management overhead by 50%. The Data Manager Appliance leverages Data Domain for storage infrastructure providing data immutability and industry leading deduplication.



PowerProtect Backup Services, protect your hybrid cloud ecosystem

As organizations increasingly adopt multi-cloud strategies, protecting data across these distributed environments becomes a top priority. Dell PowerProtect Backup Services offers a simple, secure, and scalable Data Protection as a Service (DPaaS) solution, designed to safeguard your cloud workloads with confidence. This cloud-native platform empowers you to protect critical data in SaaS applications and public clouds without adding complexity or infrastructure overhead. The service provides automated, policy-driven backups to protect against data loss from accidental deletion, corruption, or malicious attacks.

With PowerProtect Backup Services, you can ensure your data is always protected and available, helping you drive your business forward with a resilient and compliant cloud strategy.



Cloud-Native Cyber Resilience for Modern Workloads

PowerProtect Backup Services is engineered from the ground up for the cloud. Its 100% SaaS-based delivery eliminates the need to deploy, manage, or scale backup infrastructure, allowing your IT teams to focus on delivering strategic initiatives instead of maintaining systems. This streamlined approach provides a single, unified solution to protect a wide range of cloud-native workloads.

Key features and capabilities include:

- **Comprehensive Workload Support:**
  - **SaaS Applications**: Microsoft 365, Google Workspace, and Salesforce.
  - **Endpoints**: Laptops, desktops and mobile devices
  - **Hybrid Workloads**: VMware, Hyper-V, Oracle, SQL, Linus, Windows and NAS environments
- **Built-in Security and Compliance:** With features like global search, eDiscovery, and robust role-based access controls, you can easily meet legal hold and compliance requirements. Your data is protected in-flight and at-rest with advanced encryption, ensuring its integrity and confidentiality.
- **Ransomware Recovery:** With advance recovery capabilities –I such as Threat Hunting – businesses can protect backup data from being compromised with rapid recovery.

Scalability and Simplicity for Multi-Cloud Environments

When protecting data, your solution should adapt as your business grows. PowerProtect Backup Services is built on a globally available, infinitely scalable architecture, providing the flexibility to protect data wherever it resides. It delivers a consistent cyber resilience experience across your entire multi-cloud landscape, simplifying management and reducing risk.

It's designed for effortless deployment and operation:

- **Rapid Onboarding:** You can begin protecting your workloads in minutes. The intuitive user interface and simple configuration process make it easy to discover data sources, apply protection policies, and monitor your environment from day one.
- **Seamless Integration:** PowerProtect Backup Services integrates smoothly into your existing IT ecosystem. It offers a single point of control for protecting workloads across hybrid and multi-cloud environments, ensuring data is secure and available no matter where it is created or stored.

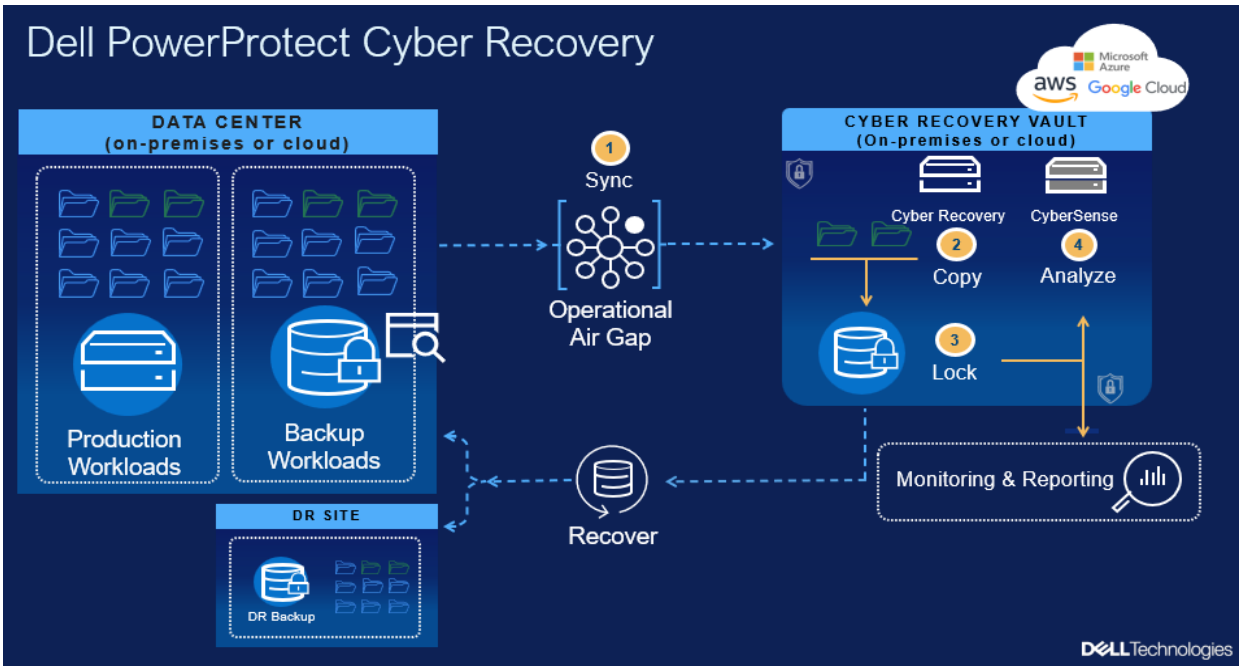
By unifying cyber resilience under a single, powerful service, you gain the visibility and control needed to confidently manage your data estate. Dell PowerProtect Backup Services provides a simple yet powerful path to ensuring data availability and resilience, giving you the freedom to innovate and achieve your goals in the cloud.

PowerProtect Cyber Recovery, isolate critical data for recovery

Dell PowerProtect Cyber Recovery is a component of an overall cyber resilience strategy. PowerProtect Cyber Recovery distinguishes itself from traditional backup and disaster recovery by providing additional layers of physical and logical security at both the solution, system and data/file level. This ensures critical data can be preserved with integrity, confidentiality and to ensure it is available when needed for recovery. PowerProtect Cyber Recovery is focused upon protecting critical data from cyber threats and away from the attack surface — and then recovering that data from an isolated environment when and if necessary.

PowerProtect Cyber Recovery focuses on protecting your most critical data whether on-premises or in the cloud and recovering your businesses following a successful cyberattack or ransomware incident. With the combination of professional services and technology, it provides the following three key elements:

- **Isolation**: PowerProtect Cyber Recovery ensures secure data protection by creating an isolated vault environment disconnected from corporate and backup networks, accessible only to authorized users. Critical business data is transferred from a Data Domain in the production environment to a Data Domain in a secure vault via an operational air gap, which remains locked to block all external access, including SSH and HTTPS traffic. The vault operates in a physically restricted area, such as a locked room, to mitigate insider threats. Data synchronization occurs through a controlled process initiated within the vault. The air gap is temporarily unlocked to sync critical data, including backup catalogs and metadata, using a single transport mechanism to minimize the attack surface. Only changed data blocks are transferred efficiently, ensuring minimal exposure. Trusted connections between production and vault systems prevent unauthorized access. This robust design ensures that even when the vault is unlocked for updates, bad actors cannot exploit the system.
- **Immutability**: Once data has been synchronized to the vault and the data path is disabled, PowerProtect Cyber Recovery creates unchangeable data copies on the Data Domain storage. These copies are space-efficient and used for recovery drills, testing, validation and analytics. Using Compliance Mode Retention Lock, data is protected from deletion or modification for a specified retention period, meeting SEC standards (34 CFR 17a-4(f)(2)). This is also available using the Data Domain Virtual Edition.
- **Intelligence**: CyberSense allows you to stay ahead of the rapidly changing threat landscape and sophisticated cyber criminals with CyberSense adaptive analytics, machine learning (ML) and forensic tools to detect, diagnose and accelerate data recovery within the security of the Cyber Recovery vault. CyberSense is fully integrated with PowerProtect Cyber Recovery and monitors files and databases to determine if an attack has occurred by analyzing the data's integrity. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, and core infrastructure. These observations enable CyberSense to track how files change over time and uncover even the most advanced type of attack. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed. Signatures are not used so regular updates are not necessary and new techniques used by threat actors can be discovered without knowing about them beforehand. CyberSense finds corruption with up to 99.9%[3] confidence and the post attack forensic reporting will quickly and safely identify a 'last known good' copy of data that can be used to recover data to resume business.



Professional Services, expert assistance

We know technology is the engine of human progress but safeguarding that engine requires more than just robust hardware and software. It requires a strategy built on expertise and vigilance. By pairing PowerProtect solutions with our specialized services, you gain the confidence to innovate without fear, knowing your data is protected by a partnership dedicated to your resilience.

Strategic Planning
True resilience begins before a threat ever emerges. Our Advisory Services work with you to align your cyber resilience strategy with your unique business goals. We help you identify gaps, assess risks, and design a roadmap that ensures your organization is prepared for the unexpected.

Proactive Defense
To maintain that security, Managed Detection and Response (MDR) for Backup provides 24/7 vigilance. We monitor your backup environment continuously to detect suspicious activity. This proactive approach allows us to:

- Identify potential threats early.
- Prevent attacks from compromising your recovery data.
- Free your IT teams to focus on strategic initiatives rather than constant monitoring.

Rapid Response
Even with the best defenses, preparedness for recovery is essential. Our Incident Response and Recovery Services provide a safety net when you need it most. If a cyber incident occurs, we do not just hand you a manual; we work alongside you. Our experts help you contain the threat and rapidly restore your critical data, minimizing downtime and impact.

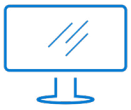
Ultimately, these services provide more than just technical support; they provide business continuity. By combining proactive planning with rapid recovery expertise, we empower your organization to move forward with certainty. You can focus on driving results and creating value, secure in the knowledge that your data foundation is solid.

Conclusion

In today's interconnected world, cyber resilience is fundamental to business success. Organizations need more than just traditional data protection; they need the confidence to withstand and recover from disruption. The PowerProtect portfolio provides this assurance by delivering a comprehensive framework for cyber resilience. With robust data security, intelligent threat detection, and automated recovery, you can safeguard your most critical assets.

This integrated approach moves your organization beyond reactive defense, empowering you to protect operations, maintain continuity, and keep your business moving forward. By building a resilient foundation with PowerProtect, you can confidently navigate the evolving threat landscape and focus on driving progress.

Explore how Dell's cyber resilience solutions can help fortify your organization at www.dell.com/cyberresilience.



Learn more about Dell PowerProtect Cyber Resilience

Contact a Dell Technologies Expert

View more Security resources

Join the conversation with #PowerProtect

[1] https://doi.org/10.6028/NIST.SP.800207
[2] Cyber Resilience Insights Report, Vanson Bourne Research, July 2025
[3] Based on an ESG report commissioned by Index Engines, "Index Engines' CyberSense Validation 99.99% Effective in Detecting Ransomware Corruption". June 2024

DELL Technologies