Dell PowerProtect Backup Services for Endpoints

Protect end-user data and safeguard your remote workforce

Protecting end-user data and safeguarding your workforce is critical in today's world. With the expansion of the workforce, corporate data is increasingly residing outside the corporate network and beyond corporate control. Ensuring business resilience while protecting your employees is a challenge, especially when data resides on geographically dispersed endpoint devices and ransomware attacks are becoming more prevalent and sophisticated. Some common challenges include ensuring that data is backed up and recoverable in the event of a disaster or data loss, protecting data from ransomware and other malware attacks, ensuring that data is secure and compliant with regulations, managing data growth and storage costs and providing employees with a seamless experience while ensuring that their data is protected.

Robust cyber resilience solution

Your backup solution for endpoints should ensure data availability by providing reliable cyber resilience that is consistent and allows you to quickly recover from all types of loss. It should also protect your backup data in isolated, immutable and encrypted snapshots that cannot be penetrated or altered by any users or malicious activities so you can rely on it for ransomware recovery.

In addition, you can realize additional value from your backup data through:

- Accelerated eDiscovery – leveraging your backup solution to proactively collect data, automate legal hold and pre-cull your data so you can cut costs and quickly submit admissible data.
- Privacy compliance – leveraging your cyber resilience solution to proactively monitor for compliance violations and remediate them per your policies.

Dell PowerProtect Backup Services for Endpoints

PowerProtect Backup Services for Endpoints provides comprehensive, scalable and cost-effective cloud-based cyber resilience for desktops and laptops. Backup data is isolated from the customer's infrastructure in the Cloud Platform by design, providing immutable cyber resilience. The cloud-native architecture prevents ransomware from encrypting your clean backup copies.

PowerProtect Backup Services provides a secure, reliable and fast endpoint cyber resilience solution, so you can always recover end-user data. Integrated backup, eDiscovery and compliance monitoring simplifies endpoint cyber resilience, ensures regulatory compliance, and improves data visibility for the mobile workforce.

Data compliance monitoring

PowerProtect Backup Services is the only integrated solution that brings visibility to end-user data and provides an automated system to proactively track, monitor, and notify of potential data compliance risks. With process automation for identifying files that may contain sensitive information, IT can quickly assess and take corrective action for GDPR and HIPAA non-compliance of end-user data.

Federated search

By consolidating end-user data and providing integrated full-text search indexing, extensive auditing, and intuitive data visibility, organizations gain greater insight into potential business data risks and to assess issues. PowerProtect Backup Services simple, integrated dashboard and easily accessible, detailed audit trails enables organizations to monitor and analyze end-user data and assess whether compliance guidelines are being met.

Legal hold management and eDiscovery enablement

PowerProtect Backup Services facilitates completeness of data discovery for legal purposes by allowing admins to centrally collect and preserve dispersed enterprise data across endpoints and SaaS applications, cutting time required for eDiscovery in half. Tight integration with eDiscovery third-party tools and speedy downloads, accelerate the data collection and delivery process. Through automated legal hold workflows, chain of custody reporting, extended metadata and file fingerprinting, PowerProtect Backup Services ensures authenticity and alignment with EDRM and Department of Justice requirements.

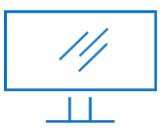
Key Features

Compliance and data governance

- Federated search across all backup data
- User-centric legal hold
- Automated and proactive compliance monitoring for HIPAA, GDPR

Security

- Customer-only access to customer data
- 256-bit AES encryption for data at rest
- TLS 1.2 encryption for data in transit
- No key management required
- Built in Managed Data Detection and Response (MDDR)
- Anomaly detection
- Orchestrated Cyber Recovery
- Certs: SOC-2 Type II, HIPAA, Privacy Shield



Learn More about PowerProtect Backup Services

Contact a Dell Technologies Expert