

Dell PowerProtect Backup Services

What to consider when protecting your endpoint devices.

To securely protect your organizations' desktops, laptops and mobile devices, you need a centralized cloud approach that offers assurance that they're protected and available, whether in the office or on the road. As you plan how best to protect these assets, keep in mind the ability for IT admins to remotely manage cloud backup and restore operations as well as the opportunity for end users to restore their devices themselves.

The expansion of the remote workforce has resulted in a rapid increase in the amount of corporate data residing outside your network and control. Ensuring that you maintain business resilience while protecting your global remote workforce is a challenge, especially when data resides on geographically dispersed endpoint devices and ransomware attacks are getting more prevalent and sophisticated.



70%
of IT decision makers
agree their organization has increased exposure to data loss from cyberthreats with remote employees¹

67%
of IT decision makers
are concerned their organization's existing data protection measures may not be sufficient to cope with malware and ransomware threats¹

¹ Global Data Protection Index, October 2022 Report"

Protecting the remote workforce

Dell PowerProtect Backup Services provides a secure, reliable and fast endpoint backup solution, so you can always recover end-user data.

Protect your data no matter where it goes.



Reimage device content within minutes



Remotely delete data from a lost or stolen device



Rapidly recover entire devices from snapshot

Remote workforces continue to increase, and as a result, your organization must address the growing risks of data loss and compliance concerns. These obstacles can make it difficult to adhere to data regulations and security standards. Failure to comply with regulations such as GDPR, CCPA, and HIPAA exposes your business to costly fines and risks. To overcome these challenges, you need to mitigate risk with regulatory compliance monitoring that helps you comply with data regulation and governance requirements.



67%
of IT decision makers
are concerned their organization's existing data protection measures may not be sufficient to cope with malware and ransomware threats¹

69%
of organizations
are concerned that they will experience a disruptive event in the next twelve months¹

Ransomware recovery

With Dell PowerProtect Backup Services, your backup data is isolated from the customers' infrastructure in the cloud platform, providing immutable data protection. The cloud native architecture prevents ransomware from encrypting your clean backup copies.

Liberate your remote workforce from ransomware.



Identify and automate data protection for key business assets



Isolate backup data from the data center network



Secure data in flight and at rest

¹ Global Data Protection Index, October 2022 Report

With the rise of global business and evolving international data privacy laws such as GDPR, there is the pressing need to understand exactly how backup data is maintained, secured and protected. To assure your organization is compliant, other certifications should also be considered such as SOC 2 type II, HIPAA, and FIPS 140-2 and FedRAMP ATO, among other audits and attestation.



Data security and compliance

Dell PowerProtect Backup Services provides integrated backup, eDiscovery and compliance monitoring. Simplify endpoint data protection, ensure regulatory compliance and improve data visibility for your organizations' mobile workforce.

Have comprehensive protection and governance without impacting user productivity.



Federated search across all backup data



Automated and proactive compliance monitoring



Data encrypting at reset and in transit

Dell PowerProtect Backup Services

Scalable, secure data protection for SaaS applications, endpoints and hybrid workloads. Enforce data governance while reducing cost and complexity.

[Visit our Website](#)[Watch the Video](#)[View the Data Sheet](#)