

# Dell PowerProtect Backup Services for Cloud-Native Workloads

## Protect your cloud-native

### Key capabilities

- **Complete protection:** Ensures protection against ransomware via secure, isolated backups with quick operational recovery
- **Secure, isolated data:** Provides secure, encrypted, and isolated backups with no egress charges
- **Reduced storage costs:** Significantly lowers storage costs by eliminating unnecessary cross-region or account snapshot copies or cross-cloud backup redundancy
- **Radical storage efficiency:** Incorporates built-in source-side global deduplication and automated cold-storage tiering for long-term retention
- **Fast recovery:** Enables fast, point-in-time restores across AWS and Azure regions and accounts in just minutes – as simple as restoring from a snapshot. Allows quick and easy recovery of Azure VMs and their associated disk storage back to your Azure subscription and region of choice
- **Easy to use:** Offers global visibility and control with simplified backup management
- **Effortless onboarding and management:** Enables swift and secure onboarding of Azure subscriptions, VM discovery, and rule creation based on organizational SLAs

In the current digital era, cyber resilience complexity has increased due to the emergence of cloud-native technologies. PowerProtect Backup Services offers cyber resilience as a service, specifically designed to tackle the unique challenges associated with securing cloud-native workloads. This solution ensures data security, ranging from robust backup strategies to simplified management, ensuring businesses can navigate the complexities of cloud-native operations with confidence.

PowerProtect Backup Services provides comprehensive cloud-native cyber resilience for your applications running on AWS and Azure Virtual Machines (VM), designed with scalability, security, and flexibility in mind. It offers global visibility, easy management, and autonomous data resilience for your organization's AWS and Azure VM environments. With reliable cyber resilience, your cloud projects can be accelerated.

### Protection your AWS workloads

Organizations back up AWS workloads and retain the data for various reasons, including the risk of backups being deleted by ransomware, insider threats, or accidental deletion. Businesses require secure, encrypted and isolated backup copies to ensure readiness for ransomware recovery. For business continuity, additional copies must be duplicated into another account or region with overheads of isolated access setup and storage costs. Consequently, managing snapshot data in multiple regions and accounts can be costly and add complexity and operational challenges.

PowerProtect Backup Services for AWS eliminates the need for additional cross-account and cross-region copies. It provides agentless, secure, isolated copies for ransomware recovery and readiness while reducing storage costs.

### Protecting your Azure VMs

PowerProtect Backup Services for Azure VMs is an agentless, cloud-native SaaS solution that provides simple, secure, and isolated backup copies for Azure VMs while significantly reducing storage costs. The solution protects Azure VM data from ransomware by creating an encrypted backup copy of your data that is inaccessible to attackers and stored in the PowerProtect Backup Services cloud.

With PowerProtect Backup Services, businesses can recover Azure VMs and their associated disk storage to their Azure subscription and regions of their choice. The unified cloud platform allows you to protect and secure backups across Azure, AWS, the data center, SaaS apps, and endpoint devices saving time and money by consolidating your backup operations.

## Key features

**Cloud-native cyber resilience:** Specifically designed for AWS and Azure VMs, ensuring scalability, security, and adaptability, with global visibility and simplified management

**Ransomware recovery readiness:** Provides secure, isolated backups for AWS and Azure workloads, protection against ransomware threats and reduces storage costs without the need for cross-account or cross-region copies

**Significantly reduced storage costs:** Features such as global deduplication, cold tier support, and predictable consumption models help to drastically lower storage expenses

### Simplified backup and recovery:

- Offers global visibility and control with easy-to-manage backups
- Provides instant access to on-demand capacity without the need for additional infrastructure

**Elimination of egress and restore costs for Azure VM and AWS backups:** Enables quick point-in-time restores across regions and accounts in just minutes, as simple as restoring from a snapshot, without incurring egress costs

### Enhanced data control:

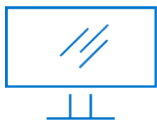
- Safeguards data from ransomware with isolated backup copies stored separately from the primary environment
- Allows implementation of immutable policies to prevent manual deletion, importing, archiving, or altering the retention of backups

**Snapshot orchestration for AWS:** Combines snapshot orchestration for rapid operational recovery with secure, isolated backups for ransomware protection

**Agentless, cloud-native SaaS for Azure VMs:** Simplifies Azure VM backups with an agentless, cloud-native SaaS solution that offers secure, isolated backup copies while minimizing storage costs

**Cross-cloud redundancy:** Ensures data integrity during Azure breaches by replicating to PowerProtect Backup Services' AWS-based cloud

**Swift recovery of Azure VMs and Storage:** Allows effortless restoration of Azure VMs and their associated storage to preferred subscriptions and regions



[Learn More](#) about  
PowerProtect Backup  
Services



[Contact](#) a Dell Technologies Expert