

Superna Disaster Recovery & Resilience Solutions for DELL Unmatched Cyber Resilience & Near Zero-Downtime Failover





The future of disaster recovery requires more than just replication it demands real-time visibility, automation, and resilience

Unmatched Cyber Resilience & Near Zero-Downtime Failover The Challenge – Why Traditional DR Falls Short

Traditional DR solutions focus on replication, but replication alone does not guarantee recovery. Organizations face major risks:

- High Downtime Costs: Gartner estimates IT downtime costs \$5,600 per minute.
- Lack of Real-Time Monitoring: Many DR solutions do not validate readiness until it's too late.
- Manual Processes Increase Risk: Human errors cause delays and incomplete failovers.
- Limited Integration: Most DR solutions fail to sync shares, quotas, or Active Directory settings.
- **No Proactive Readiness Testing**: Without continuous validation, DR plans remain unreliable.

Superna eliminates these risks with built-in automation, real-time monitoring, and seamless failover, ensuring your disaster recovery plan works when you need it most.

Gartner estimates

IT downtime costs \$5,600 per minute

Traditional DR solutions simply aren't enough. Learn how Superna's Cyberstorage approach ensures business continuity and keeps you protected.



How Superna Solves It

Superna DR ensures disaster recovery is always ready, reliable, and secure.

- ✓ Real-time Readiness Monitoring: Over 30 automated checks validate DR health across clusters.
- ✓ Automated Failover & Failback: One-click failover for SMB and NFS workloads, minimizing disruption.
- ✓ Configuration Sync: Ensures all shares, quotas, and snapshots are included in recovery.
- ✓ Automated Recovery Testing: Routine validation without disrupting production environments.
- Ransomware-Resilient DR: Integrates with Superna Cyberstorage to detect and block corrupted failovers.
- ✓ Seamless Compliance & Integration: Supports Dell PowerScale, NIST best practices, and SIEM/SOAR tools.



Gartner Innovation Insight Report: Cyberstorage Traditional security layers alone aren't enough to combat modern cyberattacks. Cyberstorage adds a crucial storage-level defense to mitigate ransomware and minimize data loss. Download the Gartner Cyberstorage Report to discover how organizations are leveraging this breakthrough technology to stay ahead of evolving threats.



Superna vs. Traditional DR

A Proven Advantage

Not all DR solutions are built the same. Here's how Superna compares to traditional and emerging DR solutions:

Feature	Superna DR Edition	Emerging DR Providers	Traditional DR Solutions
Automated Readiness Monitoring	✓ 30+ real-time checks	Limited automation	X Manual validation
One-Click Failover (SMB/NFS)	Seamless failover	A Partial automation	X Manual reconfiguration
Dell PowerScale Integration	✓ Native support	Some support	× Limited
Automated DR Testing	Fully automated, non-disruptive	4 Limited	X Disruptive, manual testing
Unified DR Dashboard & Reporting	Centralized, real-time status	4 Some integration	X Requires multiple tools
Cloud-Based 3rd Copy	Built-in support for AWS/Azuree	4 Requires add-ons	× Not supported
Ransomware Resilience & Air-Gap Vaults	Proactive protection with isolated recovery	Limited ransomware detection	X Backup-only approach

Core Features

- Failover and Failback: Automate seamless transitions between production and DR environments.
- Seamless SMB Failover: Maintain uninterrupted client access without remounting.
- **Real-Time Observability**: Proactively detect risks before they impact operations.
- Configurable DR Policies: Customize replication datasets and failover scenarios.
- Single Appliance with Unified Dashboard: Manage multi-cluster DR from one intuitive interface.
- **Comprehensive Reporting:** Track RPO metrics, sync statuses, and recovery validations.





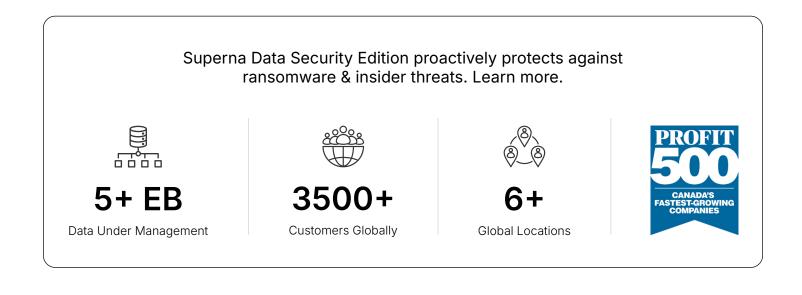


Beyond DR

Superna's Cyber Resilience Suite

Superna extends protection beyond disaster recovery with cyber resilience solutions:

- Data Security Edition: Protects unstructured data from ransomware and insider threats with automated threat detection, user behavior analytics, and real-time response capabilities.
- Air-Gapped Vaults: Isolates critical backups for ransomware-proof recovery.
- Third Copy: Enables seamless cloud replication to AWS, Azure, or on-prem S3-compatible storage.
- Third-Party Integration: Automates workflows with ServiceNow, Splunk, and SIEM tools.





A full list of supported integrations is available on our website.

Protect Your Data. Eliminate Downtime. Get Started Today.

Schedule a Demo | Speak with an Expert



©2025 Superna LLC, all rights reserved. Superna, along with the Superna logo, are trademarks or registered trademarks of Superna LLC. Other third-party brands, product names, and trademarks belong to their respective owners. Specifications are subject to change.