Leveraging High Availability and Disaster Recovery to Achieve Complete Business Resiliency

Ensuring business continuity hinges on High Availability (HA) and Disaster Recovery (DR)

When building business continuity strategies, HA and DR are crucial in ensuring business operations run smoothly. Both serve distinct purposes in managing and mitigating the impact of unexpected events, from natural disasters to cyber threats.

How HA and DR Provide Comprehensive Protection

Combining High Availability and Disaster Recovery strategies ensures robust defense against interruptions. When paired, they're key to creating a comprehensive approach to system availability and resilience.

Integrating HA and DR strategies is essential for comprehensive protection against interruptions. Together, they form a robust defense, ensuring continuous system availability and resilience. By combining HA and DR, businesses can effectively minimize disruptions, maintain uptime, recover data swiftly, and navigate unexpected events with ease.

Modern Threats Require Updated Strategies

Today's landscape demands a comprehensive approach to disaster recovery. While High Availability effectively mitigates traditional disasters, it will not suffice against cyber-attacks that have surged as the leading cause of downtime.

- HA addresses traditional disasters but **will not suffice against threat actors** moving horizontally across the networks used for HA
- Cyber-attacks have become the **primary cause of downtime**
- Modern disaster recovery strategies **include immutable data repositories and logically isolated DR sites.** *These measures thwart threat actors from compromising the recovery site, even if they have control over the entire production environment*

Learn more on how InterVision can help safeguard your business from disasters.

HA vs DR

High Availability reduces the need for recovery by minimizing disruptions and maintaining operational continuity

Disaster Recovery serves as a failover mechanism and focuses on restoring systems and data after a disruption

If your Disaster Recovery plan hasn't been updated in 3-4 years, it's crucial to reassess its efficacy against modern threats.

Learn more