da-com IT pros

Ensuring Data Protection Despite the Expanding Threat Landscape

Protect your data from loss or corruption with a robust business continuity and disaster recovery (BCDR) strategy.

Beat Data Loss With BCDR

Your business is growing, which means your information is probably scattered across different data locations, remote workers and devices, SaaS applications and the like.

A growing pile of information means a larger surface area for catastrophes to happen, such as unexpected data loss or corruption.

To ensure your business doesn't miss a beat in the face of a crisis, a BCDR solution can keep your organization running and restore your data in the shortest amount of time possible.

Without a BCDR plan, how much downtime can your business withstand?

Why Protect Your Data?

- ☑ Human error and hardware failure have been top causes for data loss over 2020.

- ☑ After their data was encrypted in a ransomware attack, only 56% of organizations got it back via backups.[1]

- ☑ IT outage cost 48% of organizations up to $130,000 per hour in various ways.[2]

- ☑ Over 52% of organizations experienced up to eight hours of unplanned IT downtime.[3]

Data Sources: [1] The State of Ransomware 2020 by Sophos

[2] & [3] Data Health Check 2020

RECOVERY ASSURANCE
Automatic recovery testing at the highest level, with detailed analytics and reporting. Testing is performed on applications or in the cloud with **zero** impact or interruption to normal operations or the need for staff involvement.

SELF-HEALING BACKUPS
Leverage intelligent SaaS remediation tools to detect and resolve common backup-related issues or problems that might lead to failed or enhanced alerting to errors in need of manual intervention.

MAINTAIN COMPLIANCE
Prove your commitment to data protection and regulatory compliance requirements with robust on-demand reporting, automatic recovery testing and end-to-end encryption.

FLEXIBILITY TO CUSTOMIZE
Customizable at a granular level to achieve all recovery time objectives (RTO), recovery point objectives (RPO) and any retention or system criticality requirements.