Defend Your Mission-Critical Data

They're coming for your data.

Fortunately, Qumulo data protection features can help safeguard your data from danger.

It's a scary world out there—from ransomware to weather events, the risk of data loss is increasing.

Every business needs a robust business continuity strategy—one that's practical and cost-effective enough to actually be used. Leveraging the cloud for Business Continuity can give you a complete, cost-effective layer of defence against data threats.

Here are some best practices to help you begin your planning journey. Talk to us — we're storage experts who can help you put your plan into action.

1

Defend: Reduce Your Attack Surface

Store your data on a purpose-built file system for business continuity featuring granular access controls (RBAC, ABE & host restrictions) and built-in data encryption. This first step will make your data a much harder target for hackers to attack.

2

Detect: Detect Suspicious Activities

The key to detection is finding everything early. Don't give malware or bad actors time to do damage. You'll need to capture activities from all devices, then store, correlate and analyze them with a modern SIEM solution. An IDS system can also help uncover suspicious network activities early. A technology partner can help set up log auditing with SIEM to detect data anomalies and bring threat detection to the next level. Simply put, if anything affects your data, you'll need to know fast.

3

Recover: Be Able to Undo The Damage

If your data is compromised, your top priority will be to roll back to its last known good version and to get up and running again. Creating snapshots, data retention policies with micro and macro timeframes, consistent backups, using the Qumulo snapshot API, and replication to secondary/tertiary sites like the cloud will add layers of defense and will speed recovery efforts.

4

Resume: Get Up and Running Again

If your business can't tolerate much (or any) interruption, business continuity is the answer to maintaining and resuming business as usual during and after an event. Take advantage of Continuous replication, File Differential Replication, read-only replication and multi-target replication to create an alternate site with known-good versions of your data, applications, and services up and running, allowing fail-over if needed. Once the issue is resolved at your primary site, simply reverse the replication relationship to place the latest content back on your primary cluster, and be back to normal with as little long-term damage to your business as possible.

5

Practice the Plan

Socialize your plan with other teams in your organization. Practice your plan on a regular basis, such as with tabletop exercises allowing your team to walk through a hypothetical event.

While "no plan survives contact with the enemy", being in practice means that even if an actual event doesn't unfold the way you may have imagined, you will be in fine form to think on your feet and improvise – and make good use of the snapshots, backups, and alternate sites you carefully planned for such occasions.

Interested in learning more?

Visit **Qumulo.com/Ransomware** to get started.

Qumulo RECOVER