Veeam NetApp

# The Importance of a Disaster Recovery Plan

More than half of enterprises surveyed have spent money on data protection due to the rise in ransomware over the last 12 months. 22% have spent 100k or more.

**Half of enterprises surveyed have created an incident response plan over the last 12 months.**

**40%** of enterprises surveyed are allocating budget on testing and validating their disaster recovery procedures over the next 12 months.

## Why is a Disaster Recovery (DR) Plan Necessary?

- **CYBERTHREATS** (ransomware)
- **RISING COSTS**
- **DATA SPRAWL** And Mobility
- **COMPLEXITIES**
- **COMPLIANCE** (regulatory/government)

## Implications of Not Having a DR Plan

### DATA LOSS

**48%**

of enterprises surveyed plan to spend, or have budgeted to spend, money on frequent backups.

### DOWNTIME

**38%**

of enterprises have implemented more regular DR testing/validation over the last 12 months.

### PENALTIES

regulatory fines, ransomware bounties

### PROTECTION GAPS

Data isn't fully secured

### OPERATIONAL INEFFICIENCIES

## How Veeam and NetApp Can Help

- Support for hybrid multi-cloud workloads
- Continuous Data Protection
- Natively immutable backups
- Integration with NetApp ONTAP snapshots; changed file tracking
  - File-level and instant VM recovery
- Automated DR orchestration and testing

**Visit vee.am/NetApp for more information**

*All data points based on Evaluator Group Ransomware Pulse Survey 2021*