

Safeguard Your Business and Stay Operational Even When Disasters S

Disasters come in many forms and our reliance on technology to conduct business means we are vulnerable when any event negatively impacts our systems and applications. From cyber attacks and employee mistakes to power outages and earthquakes, there are many forms to events with the potential to cause a potential disaster situation.

Assess Areas of Risk

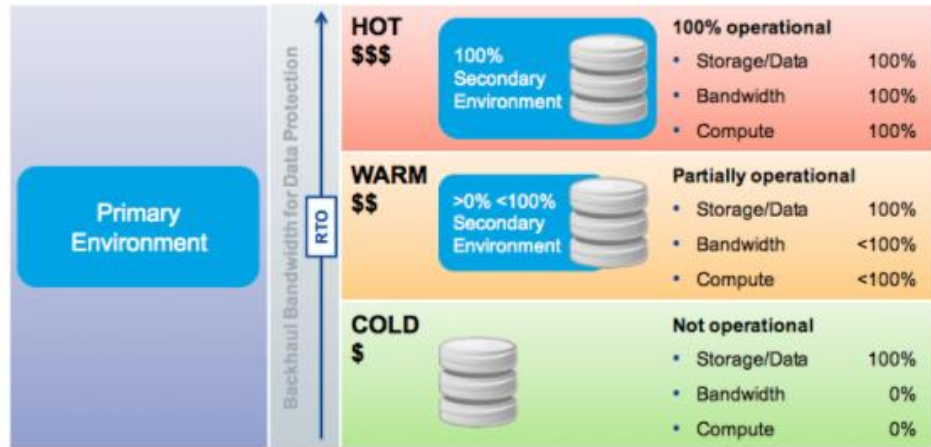
Together we identify all data and backup needs along with acceptable levels of reliability.

Protect Systems and Data

You can rely on our extensive experience deploying solutions that meet necessary recovery objectives.

Use Proven Play

Together we maintain comprehensive set of procedures taken before, during, and after a disaster.



Comprehensive Capabilities

Every business is unique and has different thresholds to design their disaster recovery strategy against. Atmosera can help identify the company's needs and create the Disaster Recovery Plan (DRP) and supporting IT infrastructure to meet those needs.

We give you options to get ahead of all events which can lead to a disaster. We help you achieve the right peace of mind for your business. Our services provide the means to replicate current production systems with various options.

As part of every deployment, customers get the following:

ASSESSMENT	Virtual and/or Physical Machine assessment and planning for replication, includes sizing VMs in Azure as well as compute, storage, and bandwidth, and replication estimates for the environment.
PLAYBOOK	Disaster Recovery (DR) Playbook creation and updates after every scheduled test.
SCHEDULED TESTING	One (1) Disaster Recovery failover/failback exercise every six (6) months.
RECOVERY POINT OBJECTIVE (RPO)	Configurable down to a minimum replication window of one (1) hour.
RECOVERY TIME OBJECTIVE (RTO)	Environment dependent with a baseline objective which is not to exceed one (1) day.
VM WARM STATE	VMs are sized and kept in a warm state in preparation for a failover event with configurable checkpoint intervals.
PHYSICAL SERVER WARM STATE	Physical Servers are sized and kept in a warm state in preparation for a migration event with configurable checkpoint intervals, where possible when replicating Physical Servers.