BUSINESS CONTINUITY/ DISASTER RECOVERY

PROTECT DATA WORKLOADS FROM DISASTER

Hackers aren't the only threat to the integrity of your business-critical data. While not as attention-grabbing as malware or DoS attacks—power outages, natural disasters, and human error are equally threatening to your data integrity. Having a disaster recovery plan that includes data replication is the best way to mitigate risk when disaster strikes. However, developing one is complex, as every organization has a distinct set of replication needs for each dataset and application. Luckily, you're not alone.

Armor's business continuity and disaster recovery (BC/DR) services, a feature of Armor Complete, are tailored to each client environment—minimizing the impact of an outage, no matter the cause. We work with you to create an effective recovery solution to ensure that you have predictable data coverage when you need it most.

ARMOR BUSINESS CONTINUITY AND DISASTER RECOVERY SERVICES DEFEND YOUR BUSINESS, RETAIN SYSTEM AVAILABILITY, AND RECOVER YOUR DATA QUICKLY WHEN DISASTER STRIKES

Continuous Data Protection

Armor BC/DR services provide proactive data protection that delivers continuous availability by dramatically reducing the impact of outages and disruptions to your business.

No Performance Impact to Ensure Scalability

We provide simplicity of disaster recovery by ensuring that our BC/DR services can keep up with higher replication loads and maintain the required latency—independent of hardware and software dependencies.

Meeting Compliance

This ensures the protection, availability, and resilience of all systems and services to meet compliance regulations such as GDPR.

Recovering from Ransomware

Armor's BC/DR services deliver a continuous stream of recovery checkpoints. In the event of ransomware or other malicious attacks, data can be recovered to just seconds before the corruption took place, reducing the impact on the business.

WHAT'S YOUR OBJECTIVE?

The first step in developing a BC/DR plan is to define your organization's acceptable level of data outage and loss, which is determined by:

- Recovery Time Objective (RTO) — The acceptable period for applications and their data to be unavailable for use
- Recovery Point Objective (RPO) — The minimal amount of back-up data that must be recovered to resume normal operations or the amount of data loss at risk

These specific values establish a baseline for the type of data replication and BC/DR solution your environment needs. Armor uses several different methodologies for addressing client requirements for RPO and RTO, helping organizations better protect their business-critical data.

TEMPERATURE CHECK

An effective BC/DR plan should be based on the readiness of your production and recovery environments.

Refer to the classifications below to determine the necessary level of data replication for your environment. Each classification correlates to the minimal amount of time your business can operate without a service's availability. Each classification represents a desired level of RTO. The spectrum ranges from "little to no tolerance" to "a higher tolerance" for service unavailability.

HOT-COLD

Covers the basic needs for business continuity in a separate region, but it also has the longest RTO.

HOT-WARM

Provides a medium RTO; a full restoration of services can range from minutes to a few hours.

HOT-HOT*

Offers maximum failure resiliency and is the benchmark of disaster prevention and business continuity.

**HOT-HOT datasets require a custom replication solution. This service is provided by Armor as a professional services engagement and offers a completely redundant deployment, custom-built for each organization.*

THE CLOUD AFTER TOMORROW

ARE YOUR BUSINESS CONTINUITY AND DISASTER RECOVERY PLANS READY?

For most organizations data loss, service interruption and lost sales are unacceptable. But has your organization developed a proven and repeatable disaster recovery and business continuity plan? Explore how this is executed, traditional deployment models and the four critical assessments you need to ask before getting started.

https://www.armor.com/white-papers/the-cloud-after-tomorrow/

ARMOR DISASTER RECOVERY AS A SERVICE

ENABLE RAPID RECOVERY THAT HELPS REDUCE ERRORS, RISKS AND DEPENDENCIES

Armor's BC/DR service works with our Armor Complete secure cloud-hosting service to provide complete security protection, featuring our proven secure-managed virtual private cloud (VPC).

Learn more about Armor Complete.

THE RIGHT SOLUTION

All offerings synchronize data and/or applications between servers, preferably at different physical locations, but each service relies on a different synchronization method. In addition, Armor provides custom HOT-HOT solutions as a professional services engagement that can be customized based on the environment.

PROTECTION	ADVANCED BACKUP WITH OFFSITE REPLICATION (HOT-COLD)	CONTINUOUS SERVER REPLICATION (HOT-COLD/WARM)
Impact	Single and/or multisite (data replication only)	VM level or instance level
Cost (based on currently quoted environment)	$	$$$
Intended Use	The backup and recovery manager service is intended to protect against accidental data deletion or loss from corruption or a data center disaster. Partial or total data restorations can be targeted to a datacenter designated as a backup by the user.	Continuous server replication is intended to fully replicate a production environment, including security, network, infrastructure-as-a-service (IaaS), and application/data layers. It allows a company to recover from complete datacenter disaster with reduced RTO or effort. The protected virtual machines (VMs) in recovery would begin operation in a geo-diverse datacenter.
Description	The backup and recovery manager service involves a controller appliance and host-based agents. Armor assists the client in configuring the appliance to identify all the data sources that need to be protected. Agents are installed on each VM. Once connected to the appliance, the source appliance will begin an initial seed backup and, thereafter, capture/back up any block deltas. The backup and recovery manager appliances are optionally hosted in a geo-redundant datacenter. The client can initiate partial or full restores by interacting with the backup appliance and targeting restores to new or existing machines. For this deployment, it is strongly recommended that the backup and recovery manager appliance reside in the production datacenter, using a secondary backup server in an alternate datacenter. Built-in replication functionality provides for geo-redundancy.	Continuous server replication is a BC/DR solution that simplifies disaster recovery by using software-defined networking and continuous replication to enable a complete recovery of an IT environment into a separate datacenter. The Armor service will perform a seed/initial backup, then capture and replicate new block deltas over time. Restoration of the BC/DR environment would occur only in the event of a BC/DR test or a true BC/DR emergency, at which point Armor will activate the recovery process, enabling full production traffic to be served from the BC/DR datacenter as long as necessary, all within a four-hour recovery window. This is a fully managed service.
What It Protects	User-defined data blocks/files only	All servers and data (plus continuous deltas), networking, firewalls, and access. (All components and data in a production environment)

PROTECTION	ADVANCED BACKUP WITH OFFSITE REPLICATION (HOT-COLD)	CONTINUOUS SERVER REPLICATION (HOT-COLD/WARM)
RTO	This solution can provide line speed (assuming network restore performance of 500Mb/s), files can be restored at a maximum rate of 3GB per minute. This would assume large, contiguous blocks of data. File restores of many small (1KB) files will slow performance, potentially as much as 60%. Recovery time is fully dependent upon the situation causing the data restoration, the amount of data being restored, and the condition of the target server. For reference, hypothetical examples are: 1) Data deleted or corrupted: You can expect recovery transfer at a rate of up to 3GB per minute, assuming no performance degradation from server performance. 2) Data loss from server corruption: Once the server is restored via snapshot you can restore deltas between the snapshot and the secure backup repository at the same rate listed above (3GB per minute).	Approximately 4 Hours
RPO	As per client policy	As per client policy, 30 minutes plus transfer rate based on data volume.
When to Invoke	User unintentionally deletes files/folders; doing business as (DBA) has unintentionally dropped a database.	Complete service disruption from primary datacenter expected to last longer than 4 hours.
How to Invoke	Client-managed	Client provides authorization via ticket.
Recovery Process	Files and folders can be restored to destination server of choice.	Armor handles the failover on the backend and will provide client with go-ahead for domain name system (DNS) update.
Recovery Managed By	Client	Armor

ARMOR DISASTER RECOVERY SERVICES DELIVER BUSINESS RESILIENCY

Armor's BC/DR service helps clients simplify IT transformation by eliminating the risk and complexity of modernization and cloud adoption.

- Enjoy enterprise-grade scalability and continuous protection backed by a BC/DR service that meets the needs of your business.
- Go beyond relying on snapshots for rebuilding your environment when disaster strikes.
- Get access to time-tested security and compliance experts monitoring your IT environment 24/7/365.