BCDR ESSENTIALS: PREVENT BUSINESS DOWNTIME AND DATA LOSS DISASTERS

In today's ever-evolving business landscape that has zero tolerance for downtime, a cyberattack, natural disaster or even a simple human error could bring your business to a standstill. That's why having a comprehensive business continuity and disaster recovery (BCDR) response plan is key to business resilience and organizational survival.

A business continuity strategy without a disaster recovery plan would be ineffective. On the other hand, disaster recovery alone does not ensure business continuity either. Both BC and DR plans need to work together to mitigate the business impact of a potential disaster.

A good business continuity plan ensures that business-critical functions are unhindered when disaster strikes and requires a disaster recovery plan that ensures all IT systems, software and applications are accessible and recoverable. Both business continuity and disaster recovery are equally important since they provide specific procedures and strategies on how an organization can resume business after a crisis.

The checklist below covers important aspects you need to consider when selecting a BCDR solution:

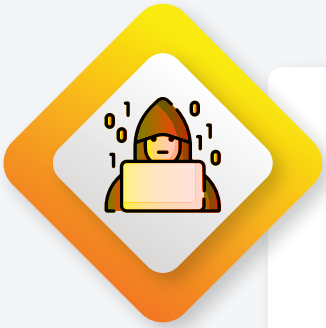
PROTECTION FOR ALL SYSTEMS, DEVICES AND WORKLOADS

CAPABILITY	DESCRIPTION
☐ Coverage across an expansive variety of business assets	Protect the data and the unique configurations, programmatic settings and integrations or workflows for IT/network programs, applications and endpoints.
☐ Policy-Based Management	Admins should be able to choose how backups are scheduled, either by entering a specific schedule or by using intelligent, policy-based scheduling technology.
☐ Data Reduction	Data reduction (deduplication, compression) reduces the overall size of files and eliminates redundancy among stored blocks, making movement, management and storage more efficient.
☐ Global Deduplication	As stated above, considering solutions that offer global deduplication across the entire backup volume will enable more efficient storage utilization than job-based duplication, which reduces blocks on a per-job basis. Since the probability of having duplicate data on VMs with the same OS are relatively high, per-job deduplication misses out on efficiency unless you put all VMs into a single backup.
☐ Support/Integration With Hyperscale Clouds	Today's solution should easily integrate with hyperscale clouds, such as AWS or Azure, to protect IaaS workloads, store backups for long-term retention requirements and enable disaster recovery.
☐ Purpose-Built Cloud	A cloud provider offering a dedicated cloud provides a turnkey solution specifically tuned to meet the needs for long-term retention and disaster recovery. Key functions are delivered as a service, thereby reducing the reliance on internal IT to develop DR as a core IT competency.
☐ Full Protection Solution (all-in-one)	Reduce risks via fewer touchpoints or attack surfaces.

AVOID DOWNTIME, DISRUPTIONS AND DATA LOSS

CAPABILITY	DESCRIPTION
☐ Flexible Recovery Options	Your solution should be flexible in how you can recover assets as well as where you can recover the data to. Look for solutions that support a wide range of recovery modes including physical-to-virtual (P2V), V2V, V2P and replicas.
☐ Quick Recovery from Local Disasters	If a server, VM or data center rack goes offline or fails, your appliance should be able to orchestrate failover to bring applications back up from your most recent backup with a near-zero RTO.
☐ Bare Metal Recovery	Bare metal restores enable application recovery across servers from different vendors and hardware configurations.
☐ Manage Protection of Multiple Sites	A single user interface should provide you with a global view to manage the protection of on-premises assets, remote offices, SaaS apps and endpoint devices.
☐ Data Loss Prediction	Utilize intelligent tools that simulate different disasters and outage scenarios to determine what types of and how much data would be lost in a downtime event so you can refine your strategy and ensure RPOs are being met.
☐ Application Downtime Prediction	Leverage deep application testing to identify, simulate and test the multiple steps required to recover complex applications to ensure RTOs and uptime SLAs are being met.

GROWING SECURITY RISKS AND EVOLVING CYBERTHREATS



CAPABILITY	DESCRIPTION
Physical Security	Computers and servers should be in secured, locked locations. An alarm system should be in place for after-hours security as well as continuous visual security for office systems.
Password Protection	Computers and servers should be password protected. Passwords should not be viewable by visitors and office goers.
Identity and Access Management	Identify, authenticate and authorize every person trying to access any IT resources.
AES Encryption	AES encryption secures data privacy both at rest and in-flight. In addition to data backups, office email should be secured and any Personally Identifiable Information (PII) sent via email should be encrypted. Any removable storage devices (HDDs, USB drives) should be encrypted. Staff should be trained adequately in encryption procedures.
Ransomware Prevention	Consider a solution written in hardened Linux. Ransomware targets Windows applications and common utilities (i.e., VSS writers) due to their popularity and the fact that Windows is an open architecture.
Threat Detection	Your solution should use machine learning to detect in near real-time, an active infection. Artificial Intelligence (AI) establishes a baseline of heuristics, such as change rate prediction, data entropy and randomness, to identify anomalies in data that antivirus and firewalls do not catch. Automatic notifications alert admins, enabling them to take immediate action to slow the spread and speed up recovery efforts.
Anti-Phishing Defense	Empower employees to defend against phishing and account takeover attacks. Solutions that provide visual cues (i.e., banner notification) alert employees to external senders, spoofed and/or imitated users and enable them to quarantine suspicious emails, which helps to automate workflows and feedback loops to streamline IT review.

REGULATORY COMPLIANCE

CAPABILITY	DESCRIPTION
☐ Internal Anomalous Monitoring and Detection	Secure servers, data and networks with an AI-augmented solution that identifies threats, such as misconfigurations, unauthorized logins, new devices being added to the network, gaps in backups and admin rights being granted, that firewall and antivirus solutions cannot detect.
☐ Immutable Audit Logs	Immutable logs and routine monitoring ensure that the data being handled by your backup and recovery systems is being appropriately handled and accessed by staff.
☐ Role-Based Access Control	When dealing with highly proprietary data, not all backup and recovery users may require access. A solution that limits the scope and capabilities of admins and other users ensures that backup schedules and/or recoveries are only performed by authorized personnel.
☐ Long-Term Data Retention	Depending on your state, you may be required to retain records (such as tax records) for several years. Your solution needs to be able to accommodate long-term data retention, whether locally, to a cloud location or a secondary target (i.e., NAS device or tapes).

DON'T WAIT UNTIL IT'S TOO LATE! DATA LOSS AND DOWNTIME CAN NEGATIVELY IMPACT YOUR BUSINESS. CONTACT US NOW TO SELECT A BCDR SOLUTION THAT'S RIGHT FOR YOUR BUSINESS.

RESTECH SOLUTIONS

Contact Us:
713-936-6855
info@restech.solutions
https://restech.solutions/contact