RESTECH
SOLUTIONS

WORK LESS, DO MORE

Follow this checklist to spend less time on backup & disaster recovery and more time on the things you love

RESTECH
SOLUTIONS

10 WAYS UNIFIED BCDR OPTIMIZES BACKUP, DISASTER RECOVERY AND BUSINESS CONTINUITY

Introduction

Data is the lifeblood of modern businesses. One of the most important responsibilities of IT is to safeguard corporate systems, networks, IP and data. Today, data lives in more places than ever before; on-premises, on endpoints, in clouds and in SaaS applications. The need to protect increasingly dispersed workloads places tremendous pressure on IT. Fortunately, technologies have emerged that help simplify and automate the daily drain backup and recovery can have on IT schedules. Less time spent on backup and recovery is more time spent on pursuing strategic initiatives, developing new applications, and working with other lines of business to increase productivity, revenue and customer satisfaction. Leverage the following tools and methodologies that are available in today's best-of-breed business continuity and disaster recovery (BCDR) platforms, and you'll get to decide what you do with all the time you save.

1 DEPLOY LESS, PROTECT MORE

Safeguard All Workloads With a Unified Platform

Your environment may be complicated but protecting it doesn't have to be. You need to protect everything your users rely on to do their job, regardless of whether the workloads are physical, virtual, deployed on-premises, at remote locations or in SaaS applications. New technologies, such as hyperconverged infrastructure from Nutanix and Cisco and cloud-based infrastructure-as-a-service (IaaS) from Amazon Web Services (AWS) and Azure, have gone mainstream and can further complicate data protection. Legacy backup tools generally protect only a limited set of technologies. Today's modern backup and recovery solutions break down silos and eliminate the fragmented approach to data protection by providing comprehensive protection for all workloads, regardless of deployment method or physical location. Needless to say, using three different protection tools means three times the complexity, thereby increasing risks of interoperability and recoverability when you need it most.

2 SEARCH LESS, INDEX MORE

Fast Recovery of Lost or Deleted Files

User error and accidental deletion consistently tops the charts as leading causes of data loss. Organizations need to ensure their data protection solution enables easy file recovery. Indexing and cataloging of physical and virtual machine backups provides quick search and restoration capabilities. The solution's UI should be easy and intuitive so that any member of the team can perform file restoration without consulting a manual. With role-based access control (RBAC) and end-user self- service, even employees can search through backups of their account and restore lost or deleted emails and files in just a few clicks. Being able to quickly address file recovery will minimize interruptions, empower end users and free IT to focus on more pressing projects.

3 MANUALLY TEST LESS, AUTOMATE MORE

Recovery Assurance Validates Backups at the Application & Services Level

Recovery testing is a practice that many organizations aren't able to do as often as they would like to or as often as they know they should be doing. It can be time consuming and costly. The only way to know you're not wasting time, energy and money on a recovery strategy is to test it regularly and see the results firsthand. A new generation of tools will automatically test and certify full recovery of simple and complex environments with no manual involvement from IT staff. Using backup files, the entire infrastructure is recreated on the backup appliance, a sandboxed environment, or in the cloud to ensure that all data and application dependencies are recovering correctly and functional. Detailed reports showing each step of the recovery process, Recovery Point and Recovery Time Actuals and any potential recovery issues are automatically sent to administrators via email. Since testing is fully automated, you simply have to set up the testing to run at the frequency that's right for your business. Once configured, automated reports are sent to you for 100% proof and confidence that you will recover from a downtime event.

4 WORRY LESS, DETECT MORE

Machine Learning and Artificial Intelligence Thwart Ransomware in Its Tracks

Ransomware is one of the most significant threats to any IT infrastructure today. Attacks have exploded in frequency and cybercriminals are constantly inventing new ways to slip past traditional security and backup defenses. Recovering from a ransomware attack can take days or even weeks. Enterprise-class data protection solutions should have the ability to quickly identify ransomware behavior as a part of every backup. New ransomware variants create an attack loop by building in periods of gestation, or dormancy, to hide their behavior in hopes of being backed up alongside legitimate data. Countering their subterfuge is artificial intelligence, newly developed algorithms and machine learning to identify anomalous patterns in backup data. Running against every backup, the AI looks at a number of heuristics, from rates of change, data entropy (randomness), encryption and more. Upon detection, email and dashboard alerts are sent immediately to administrators and suspected backups are flagged with purposeful icons to prevent users from attempting to recover from infected files. In combination with Recovery Assurance testing, you can quickly identify your most recent, clean, fully tested point of restore.

5 JUMP THROUGH HOOPS LESS, SEE MORE

Global UI Provides Unparalleled Insight Into All Protected Workloads

A single, global dashboard should be all that is required to manage all aspects of backup and recovery. One user interface (UI) enables greater familiarity with the commands and fewer clicks to accomplish your goals regardless of whether you're protecting data center assets, remote endpoints or cloud-based workloads. Jumping through different logins and having to enter credentials each time impedes IT time and increases time to resolution of even common issues. Using different UIs as part of a stitched-together solution may mean that disparate applications have been cobbled together in a crude attempt to look like an integrated platform. The UI should allow you to see, in a single glance, the complete health of all deployed appliances, sites managed and any risk exposure. Centralized management and intelligent alerting help quickly cut through the noise, focus on what matters most and ensure all data is protected.

6 CO-LO LESS, DRAAS MORE

Embrace Cloud-Based DR Technologies to Reduce Overheads and Management

Purpose-built cloud service providers tune their cloud operations specifically for cloud backup and DR. This approach takes much of the risk out of cloud adoption and shortens the learning curve for organizations looking to use the cloud for the first time. Disaster-Recovery-as-a-Service (DRaaS) is a service that has evolved greatly since its early iterations. World-class DRaaS providers today provide “White Glove” services that free up enterprise IT from having to learn, manage and deploy cloud-based recoveries. White Glove DRaaS providers work hand-in-hand with you, right from DR planning and incident response to configuration of the recovery environment that includes networking, firewalls, QoS, provisioning of public-facing Ips and other levels of customization. Recovery is initiated by a simple phone call to the service provider who does the heavy lifting to bring the DR environment online and help you reroute user traffic through secure tunnels such as an SSL VPN. Some DRaaS providers offer contractually guaranteed recovery SLAs based on Recovery Time Object (RTO) like, for example, RTOs of 1-hour or 24-hours for application recovery. This high-touch version of DRaaS can be managed and deployed from any location and protect remote sites around the world. Regular testing and reporting provides proof and confidence these SLAs can be met.

7 SCHEDULE LESS, BUILD POLICIES MORE

SLA Policy Automation Streamlines Scheduling Based on RPO

Arbitrary backup scheduling is becoming a thing of the past. IT Administrators are required to align data management and availability tactics to business policies, many times without a full understanding of how details such as file locations and backup schedules impact availability and recovery. SLA Policy Automation greatly simplifies the way users define and manage backups. Rather than sifting through a multi-step wizard to define all the different settings, backup appliances should be able to define backup schedules in streamlined, policy-based objectives to align data protection within established thresholds for data loss. SLA Policy Automation allows administrators to define and schedule backups based on specific recovery requirements (RPO and backup copy replication). The backup appliance then automatically defines and manages the steps required to comply with the policy. This greatly reduces the effort and confusion required to define backup schedules and dramatically increases the ability to meet data protection and business continuity mandates.

8 SNAPSHOT LESS, INSTANTLY RECOVER MORE

Instant Recovery and Replicas Provide Proactive, Lightning-Quick Recovery

Native VM snapshots are not backups – they are change log files of the original virtual disk and are tied to the base disk. If base disks are deleted, snapshot files are rendered useless. In the event of a server failure or other localized outage, instant recovery can keep your business running smoothly. Instant recovery options for Windows (image-level) and virtual machines enable recovery of a failed or corrupted virtual machine or physical server within seconds by leveraging appliance resources as part of the recovery process. For a more proactive approach, standby copies of Windows servers and virtual machines, and replicas, can be created and stored in alternate locations where they’re kept up to date by applying each new backup of the original asset as they run. This means production applications are quickly accessible and users can continue working shortly after a downtime event. Other recovery technologies that depend on rebuilding the virtual disk on targeted storage will be slower to bring failed applications back online.

9 TROUBLESHOOT LESS, SELF-HEAL MORE

Predictive Analytics and Autonomous Environmental Remediation Save Management and Maintenance Time

Predictive analytics enables devices to understand what is inside the range of normal performance and predict hardware breakdowns. As intelligent devices gain greater knowledge from analyzing larger volumes of data, they will more accurately predict failures so recovery tactics can be taken before users are affected. Self-healing disks in appliances identify, diagnose and eliminate a variety of common sources of disk failure. Predictive analytics automatically monitors and analyzes performance trends to predict and prevent hardware failures. If an anomaly can't be prevented, look for a solution before failures affect backups. Advanced solutions are starting to bring more automation in the infrastructure use case as well. By monitoring and autonomously remediating environmental errors that could affect backups from occurring, you can ensure success criteria is met before backups are ever run. Self-healing technologies can be deployed via a no-touch SaaS model, saving you time and effort in troubleshooting the environment without increasing management overhead.

10 GUESS LESS, PLAN MORE

A Well-Documented DR Plan Is Critical to Rapid Business Recovery

A well-documented DR plan is critical to rapid business recovery. Including it in a list of time-saving tools may seem counterintuitive since creating a DR plan takes a fair amount of time. However, this recommendation is more about saving time when it matters most – speeding up recovery after a downtime event. Working with other line-of-business leaders ensures all individuals within the organization are on the same page when it comes to expectations and realities of recovery. Setting recovery objectives without consulting business line managers is the number one cause for misalignment. It is imperative that you involve them in this process to ensure the business can recover properly during a disaster. The key here is to understand business needs and provide a differentiated level of service availability based on priority. Now that you have that information on hand, it needs to be translated into recovery objectives to be included in your disaster plan. Organizations can use a free tool, such as BCDR Link (https://bcdrlink.com), to build and customize a DR plan. This planning template follows the most up-to-date guidelines of ISO 22301 that specifies security requirements for DR preparedness and business continuity management systems (BCMS) and includes all steps necessary for a comprehensive recovery plan. During a downtime event, this tool ensures that everyone knows the steps required of them to accomplish the fastest recovery possible.

Conclusion

Your BCDR journey does not have to be arduous, though it does demand considerable time and effort on your part. Having an experienced MSP on your side, such as us, can take a great weight off your shoulders and allow you to focus on what you enjoy. Feel free to contact us for a no-obligation consultation.

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