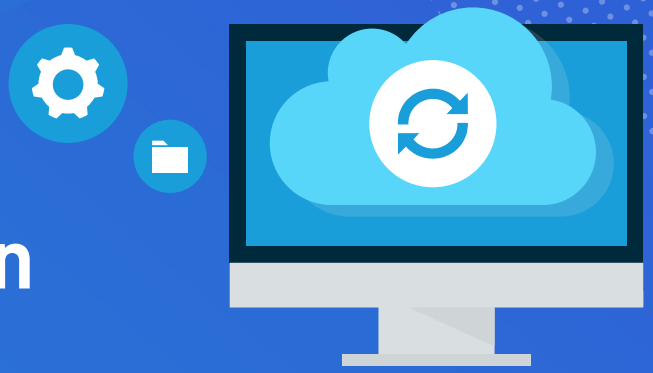
5 Essential Tips for Azure Data Protection



Businesses like yours are gravitating to Microsoft Azure in ever-greater numbers. Azure offers high degrees of scalability, flexibility, ease of access to Microsoft's vast app ecosystem, sophisticated automation, and AI readiness.

These are all attractive qualities for any business that wants to innovate and grow.

Despite these benefits, Azure also has drawbacks common to public cloud platforms. Many businesses overlook the fact that cloud servers have vulnerabilities that mirror those of on-premises servers. User error, hardware failure, data corruption, and ransomware all can take down systems you depend on to do business. As hard as Microsoft works to make Azure a solid and reliable platform, your data will be better protected if you replicate it to an independent cloud, one specifically designed for business continuity and disaster recovery (BCDR).

As a managed service provider that works with growing businesses, we want to protect our clients' Azure virtual machines (VMs). Some of Azure's flexibility comes from hosting business applications and middleware such as databases on VMs rather than directly on physical server hardware, allowing them to be resized, reconfigured, and replicated dynamically. We can take advantage of that architecture, enabling a VM to be mounted from a backup, outside of the Azure cloud if necessary, allowing normal business operations to continue.

Our solution, based on Datto Continuity for Microsoft Azure (DCMA), meets five essential requirements for protecting VMs in Azure.

1. Speed — We can restore VMs within minutes, instead of hours or days.

2. Predictability — Backups are only useful if you have confidence that they will work. DCMA's advanced backup verification confirms that VMs will mount correctly in the BCDR environment, with all data and applications intact. Backups are also scanned for ransomware — essential, given that recent research indicates almost 70% of service providers like us see ransomware as the most common malware threat to their clients.

3. Efficiency — We monitor many systems for many different clients, so anything that can streamline operations makes a difference in response/recovery times and the quality of service we can deliver. DCMA is part of an all-in-one cloud backup solution unifying backup and disaster recovery for both cloud and on premises resources within a single, cohesive system.

4. Instant virtualization — To minimize downtime that gets in the way of you doing business, we specified a system that lets us quickly boot recovery Azure VMs from a backup location in an independent cloud. Typically, the recovery VM is in use for a short time while the primary VM is being restored. This optimizes recovery time objective (RTO) and minimizes downtime, two of the primary goals of BCDR planning.

5. Flexibility — We can choose to restore from the most current Azure VM backup or any previous backup, for increased flexibility around recovery point objectives (RPO). This is key when performing a ransomware recovery since it lets you select a "clean" backup image you can restore from. Additionally, we can use a variety of data restoration methods to meet different recovery scenarios. We can capture backups as frequently as every five minutes, and restore individual files or entire system images.

When it comes to protecting Azure VMs, there's clearly a lot to consider. Use this checklist to compare what we offer against any other solution in the market.

We would love to tell you more. Contact us today. Or download our **eBook**, Achieving Business Resilience with BCDR and MSP Support, to learn more.

www.etechcomputing.com | contact@etechcomputing.com | 647-361-8191