AWS-native backup and disaster recovery creates a new data protection paradigm for IT systems

By Joe Merces

As IT infrastructure moves ever more quickly to the cloud, decades of the same old legacy backup solutions are being upended. A new paradigm for enterprise backup and disaster recovery is emerging within Amazon Web Services (AWS). This paradigm is exemplified by the Cloud Daddy Secure Backup application, available on the AWS Marketplace. The solution offers a holistic approach to data protection, embracing backup and recovery, advanced security features and infrastructure management as a native application for AWS cloud users. It is available in five service levels, depending on the number of instances an organization is running.

The move to a unified AWS-native solution reflects today's changing IT landscape, combining what had previously been siloed functions. This approach for bringing backup, infrastructure management and security together into a single comprehensive solution for disaster recovery effectively closes the gaps among what traditionally had been stand-alone IT functions. As a result, overall disaster recoverability can be greatly improved.

Historically, disaster recovery was planned around the notion of natural disasters impacting on-premises data centers. In today's world, however, the frequency of ransomware and cybercrime join natural disasters in making secure backup and recovery an everyday concern. Cyber-disasters like those caused by ransomware, to take just one example, have unfortunately become IT catastrophes occurring with increasing frequency.

Part of the problem has always been insufficient testing of disaster recovery plans. If these plans were in fact actually tested across enterprises to work with conventional legacy solutions, you wouldn't hear about government agencies and private companies being down for days or weeks to recover from attacks on business-critical servers. Enterprises need solutions that provide agility, not only to periodically test backup and recovery, but to address data protection needs holistically. Just performing backup and hoping it works whenever you're faced with a disaster is not enough.

In addressing today's data protection needs, a holistic, AWS-native data application can simplify periodic testing of backup and recoverability within AWS. More importantly, it can facilitate the recovery of business-critical data at a moment's notice by leveraging the elastic cloud capabilities of AWS, taking advantage of multiple geographical regions and accounts worldwide to quickly backup, replicate and recover data.

The simple truth is that migrating your infrastructure to AWS isn't enough to guarantee secure backup and disaster recovery. In fact, AWS specifically calls out a "Shared Responsibility Model" in which AWS is responsible for security *of* the cloud, but the

customer remains responsible for security *in* the cloud. An AWS-native secure backup solution enables backup, restoration and replication, while incorporating advanced security countermeasures and infrastructure management for comprehensive end-to-end data protection that complies with AWS' Shared Responsibility guidelines.

While some competitors are starting to emerge in this space, the Cloud Daddy solution is unique particularly when compared to traditional backup solutions, because of the added advanced security countermeasures that can protect an organization's capacity to recover from both natural as well as cyber-disasters.

In the cloud, agility combined with security is required. A unified application for recovery, security and infrastructure management offers truly modern data protection for today's elastic cloud world. It is the new paradigm that enterprise IT so sorely needs.