How does cloud-based disaster recovery work, and how can agencies use this approach to protect their technology infrastructure?

Many state and local government agencies may not differentiate between backups and actual disaster recovery. A backup makes a copy of the data, whereas disaster recovery solutions not only protect your data, but also provide a method for recovering the application or workload.

Cloud-based disaster recovery allows agencies to quickly recover in the cloud, reduce downtime and data loss, and increase their resilience. A huge advantage is that agencies can typically recover in minutes without having to procure, manage, or operate a secondary site, such as an on-premises or colocation data center.

This approach also provides a unified solution to protect and recover databases and applications in case of disaster. Agencies can easily replicate their data — whether it is stored on physical, virtual, or cloud servers — in a separate environment at a lower cost.

What are the cost benefits?

The move to the cloud offers cost and operational benefits. The inherent approach of the cloud is you pay as you go. It’s very easy to scale. With cloud-based disaster recovery, you don’t need to provision or pay for duplicate hardware and software. Agencies can also leverage automation to reduce demands on IT staff. Less tangible is the reduced time to recovery agencies experience when events occur.

How does moving disaster recovery to the cloud also make it easier for agencies to test their environment?

The cloud provides on-demand capacity to test at any time, so you can run disaster recovery drills much more frequently. This gives organizations visibility into the frequency of testing, the ability to run tests more often, and opportunities to validate strategies ahead of issues. With cloud-based recovery, you can run more tests without impacting your users and your IT team doesn’t need to spend weekends in a data center running drills. It all can be done remotely.

How can agencies migrate disaster recovery processes to the cloud?

Agencies can start off small, and review and categorize the requirements they have for various applications and workloads. Migrate the critical applications and workloads first, get them protected from a disaster, and test and validate them to ensure they operate in the cloud as expected.

Secondly, and even more importantly, when you move disaster recovery to the cloud, it doesn’t interfere with existing methods. For example, if an agency is replicating [its data] in another data center or ‘colo,’ there is no disruption or conflict with the way they’re doing business today. It really reduces complexity in shifting their disaster recovery strategy from on-premises to the cloud.

How can cloud-based disaster recovery accelerate the public sector’s move to the cloud?

At AWS, one of the things we’ve seen with cloud disaster recovery is that it gives agencies the opportunity to dip their toe in the water to run and test their workloads in the cloud. Once they are ready from a knowledge and operational perspective, they can use solutions, such as CloudEndure Disaster Recovery, to fail over to the cloud and shift production workloads. It can be done over time. It’s not an all-or-nothing approach.

State and local government agencies have a responsibility to protect their data, and the data of their citizens, to maintain trust and security. A strong disaster recovery strategy is an essential part of this effort. An effective solution — cloud-based disaster recovery — can help agencies achieve this goal while gaining operational efficiencies.

In this interview, Alex Berkov, manager of solutions architecture for CloudEndure Disaster Recovery, a leading cloud-based disaster recovery and business continuity solution offered by Amazon Web Services (AWS), shares the key benefits of moving disaster recovery to the cloud and how agencies can successfully make this transition.