Data protection in **hybrid cloud environments**

Robust strategies to protect mission-critical data and apps address availability, integrity and resiliency

Mike Malaret

Veritas

Some eye-opening statistics from the commercial sector should serve as a reminder to government agencies about why it's vital to protect against data loss and ensure they do not succumb to ransomware and other types of attacks.

According to statistics gathered by Veritas Technologies, 43% of companies that experience a catastrophic data loss never reopen. Furthermore, 51% close within two years, and only 6% survive long term. Although an agency could financially recover from a hack or ransomware attack and continue to operate, the cost of recovery could potentially impact funding priorities for years and result in a loss of services to the public. Depending on the agency, lives could be at risk if data is destroyed.

It's essential for agencies to establish a detailed plan for responding to a data breach and quickly reinstating the data and applications that are critical to providing services to the public.

Resuming operations as quickly as possible

Such a plan goes beyond data management. Instead, we're talking about a comprehensive strategy for the availability, integrity and resiliency of data and the applications agencies need in order to use that data.

A large part of the IT infrastructure is moving toward the cloud, and there are security benefits associated with cloud-based data. However, cloud providers and agencies share responsibility for security, and many security tools provided by the cloud entity do not extend to the agency's on-premises systems. Therefore, agencies should have data protection and recovery solutions that can operate seamlessly and cost-effectively in a hybrid-cloud agency.

Those solutions should include the ability to deploy artificial intelligence and anomaly detection so the agency can identify when an attack occurred so it can safely recover data without being re-infected. Those solutions should also enable agencies to operate effectively as soon as possible after an attack. Colonial Pipeline, for example, had a data protection solution in place when the company was hit with a ransomware attack last year, but it could not recover its backup data in a timely fashion and wound up paying a multimillion-dollar ransom for the return of its data.

Choosing scalable, automated solutions

Colonial Pipeline's situation is something of an anomaly because one study showed that 96% of companies with a trusted backup and disaster recovery plan were able to survive ransomware attacks. However, only 31% of organizations test their disaster recovery plans, which is crucial to ensure that agencies understand the steps involved and can respond effectively in a crisis. Therefore, agencies should choose data protection solutions that include

Marjan Blan

> **Only 31% of organizations test their disaster recovery plans,** which is crucial to ensure that agencies understand the steps involved and can respond effectively in a crisis."

the ability to conduct automated disaster recovery rehearsals on a regular basis. The key to any disaster recovery solution is automation. Without automation, a timely wide-scale recovery is not achievable.

Agencies should also be aware that many commercial solutions were born in the enterprise data center and run on architectures that do not support autonomous solutions that scale up or down based on the client's demand. By contrast, a cloud-native or container-based infrastructure responds to the government's demands as they evolve over time, which ensures that agencies are taking advantage of the most cost-effective solutions for operating in the cloud.

Data protection is an endeavor that spans the enterprise, so it is vital to consider how those solutions operate and whether they can be fully automated. By all accounts, ransomware threats will continue to grow, but by implementing a comprehensive strategy now, agencies can protect the data and applications at the heart of government services. ■

Mike Malaret is director of sales engineering for public sector at Veritas Technologies.