Datrium Ransomware Protection

SOLUTION BRIEF

Highlights

- Failproof on-demand ransomware protection using Datrium DRaaS with VMware Cloud on AWS
- Instant RTO and ability to restart workloads in a clean environment
- Built-in and immutable cloud backups for ransomware recovery
- Continuous compliance checks every 30 minutes to ensure your DR plans work when needed
- Plug and Play architecture that supports any VMware-centric primary storage

The Challenge

According to the report, The State of Enterprise Data Resiliency and Disaster Recovery 2019, one in two companies has experienced a DR event in the past two years, and ransomware was the leading cause. Analysts estimate that 75% of organizations hit with ransomware were running up-to-date endpoint protection tools. From hospitals to schools, state and local governments, service firms, and small and medium businesses to enterprise companies, cybercriminals are targeting organizations in almost every industry, and prevention strategies haven't been enough to protect against these attacks.

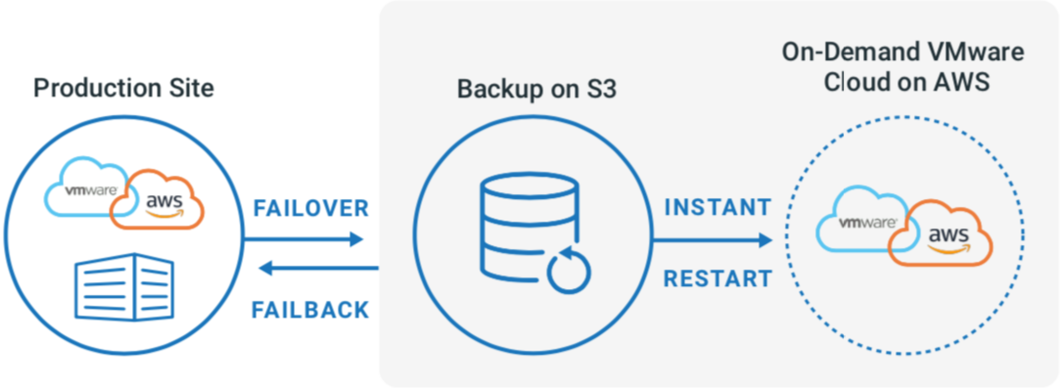
When ransomware hits, companies can either pay up or fight back. Unfortunately, as many as 70% of the infected businesses had no choice but to pay the ransom to recover their data. That's because fighting back requires rapid recovery in an uninfected and protected environment. However, traditional backup software is too slow, and legacy DR solutions that restore to a secondary site are too expensive, complex, and unreliable.

You need a new approach for fast recovery in a clean environment.

The Solution

Disaster Recovery (DR) solutions are the only ransomware protection that's 100% reliable, provided it includes tamperproof backups, a reliable DR site with clean ESXi hosts, and easy failover and failback.

Datrium DRaaS with VMware Cloud on AWS delivers ransomware protection, so you don't have to pay a ransom to recover your data. It includes built-in cloud backup, DR orchestration, and on-demand DR sites in VMware Cloud on AWS. DRaaS eliminates the need for costly physical DR sites as you only pay for DR resources when disaster strikes or for testing. It keeps data safe and secure, and continuous compliance checks enable users to confidently execute failover and failback in case of an attack.



Key Benefits:

Built-In Cloud Backups

Get built-in tamperproof backups for ransomware recovery. Backups, created every few minutes, every hour, or every day, are always deduplicated, compressed, encrypted, and stored in their native VM format in low-cost S3 storage on AWS. You get lower storage and egress costs and a more robust solution.

Instant RTO

Instantly restart thousands of VMs with unique live-mount capability that turns cloud backups, which can be minutes old or up to 7 years old, into a live cloud-native NFS datastore. For cases where ransomware has gone undetected for days, weeks, or even months, use live-mount to instantly restore snapshots from different recovery points and test each for infection. That enables you to restore from the most recent and uninfected point in time, giving you the lowest RPO for ransomware recovery.

Cloud Orchestration

Create DR runbooks and backup policies for ransomware recovery with an easy-to-use, cloud-native UI, and orchestrator. Test your ransomware protection runbooks in an isolated environment without any effect on production workloads by specifying separate test mappings for data stores, folders, compute resources, IP addresses, and any other resources appropriate to test a DR plan.

One-Click Failover and Failback

Start your ransomware recovery with an easy, one-click failover to the VMware Cloud on AWS. Because VMs are started in a new VMware SDDC on AWS, you can be sure that you have a clean environment and ESXi hosts for failover. To keep the cloud and egress costs low, use one-click failback to shut down the on-demand cloud resources, copy only the changed blocks, and restart VMs in the primary site.

Continuous Compliance

Ransomware protection hinges on the successful execution of DR runbooks. With automatic compliance checks that run every 30 minutes, you can be sure your ransomware recovery plans are up to date and will work when you need them the most.

Plug-and-Play Architecture

DRaaS delivers ransomware protection for all virtual workloads running on any VMware-centric primary storage. Its plug-and-play architecture helps you get started in as few as 10 minutes.

Conclusion

Using Datrium DRaaS with VMware Cloud on AWS, IT teams can rest easy knowing they have the best ransomware protection with instant RTO, built-in cloud backups, clean ESXi hosts, continuous compliance checks, easy-to-use UI, and plug-and-play architecture that works for all VMware-centric primary storage.

Customers

ULTRA UP PETROLEUM

> “We can instantly restart any workload from S3 after a disaster, and that gives us protection from things like ransomware.”

Josh Rein
Network Manager, Ultra Petroleum

BL

> “With Datrium, we have a full backup and recovery solution for ransomware or any other disaster.”

Gray Huggins
Director of Technology, Bishop Lynch High School

Datrium®