Ransomware:
The Call You Don't Want to Make

RANSOMWARE RECOVERY STORY

The Attack

On a Sunday morning at 10:00, we got a call from our customer, an IT Director of a services firm, who said, "We've been hit by ransomware... again." The firm had been hit by ransomware earlier in the year, and they spent weeks recovering their data using a legacy backup solution. Backup is fundamentally different from disaster recovery. Backup systems aren't built for mass recovery because they typically have to convert the VMs into a cloud-native format. It can take days or weeks to rehydrate data from S3 when there's no built-in backup and instant RTO (Recovery Time Objective).

The Recovery: Instant RTO

Fortunately, this firm had eliminated its legacy backup solution and adopted Datrium DVX, which delivers primary storage with built-in backup. Once the firm identified the ransomware threat, the IT team leveraged DVX Instant RTO, and with a few clicks in the easy-to-use UI, they were able to restore all of their virtual workloads. Once the operating systems booted, they were back up and running in about an hour. Many employees in the company had no idea that the firm had been hit by a ransomware attack.

How to Speed Up Recovery: Built-In Backup with Immutable Snapshots

Preventing a ransomware attack is incredibly difficult, but with Datrium products, recovery is easy. DVX and Disaster Recovery as a Service (DRaaS) with VMware Cloud on AWS both come with built-in backup that provides immutable snapshots. Snapshots are tamperproof. IT teams can restore from recent snapshots or backups that are up to seven years old.

Through a simple UI, teams set backup policies and disaster recovery (DR) runbooks. Tamper-proof backups, also known as immutable snapshots, can be created every few minutes, every hour, every day – whatever makes sense for the business. Backups are deduplicated, compressed, and encrypted, and then they're stored in their native format in S3. Compliance checks run every 30 minutes to make sure they work when needed.

When disaster strikes, an IT staff member initiates failover to Datrium DRaaS, which automatically provides VMware resources and an SDDC in VMware Cloud on AWS. The stored backups are instantly powered on via a live cloud-native NFS datastore mounted by an ESX host in that SDDC, resulting in instant RTO. Unlike legacy backup-only solutions, there's no time wasted waiting for backup data to be copied into an SDDC before any VMs can be restarted.

Likewise, an organization could choose to recover from ransomware by failing over to a secondary DR site or from a DVX snapshot.

Learn More

To learn more about built-in backup and how Datrium can help you recover from ransomware, visit www.datrium.com, and contact us to get a demo.