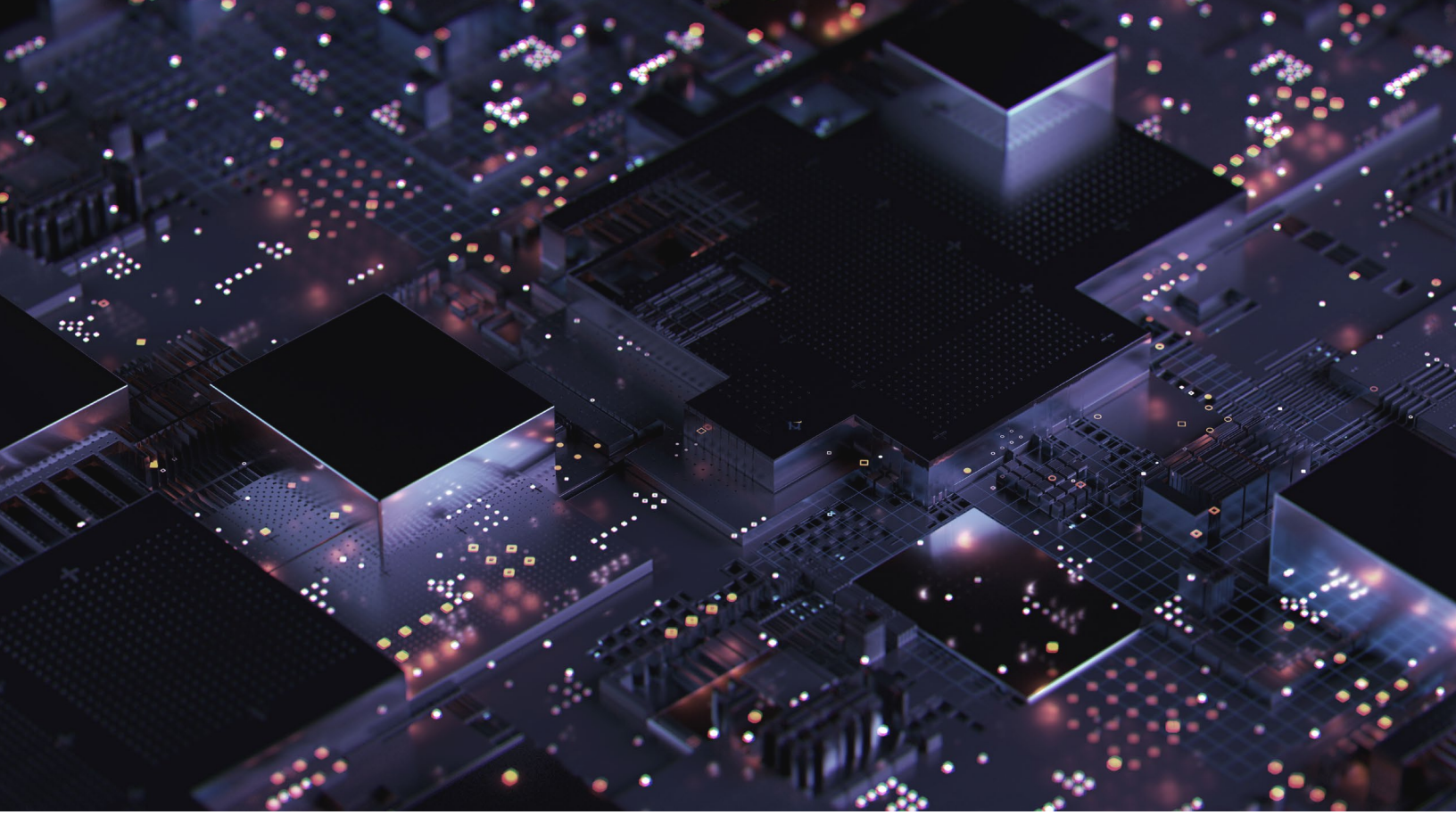

Cloud Rewind™
Formerly Appranix

Commvault®

CUSTOMER STORY

LEADER IN EDISCOVERY

eDiscovery Leader Recovers from Ransomware Attack on MS Azure with Commvault Cloud Rewind

Industry
eDiscovery Services

Key Metrics
Successful recovery of entire Azure account with 18 subscriptions and multiple applications in under 36 minutes

BACKGROUND

Leader in eDiscovery provides solutions, employing advanced technologies, for corporate litigation strategy and crisis management. The company's resources and operation systems are organized into two operating segments - eDiscovery Business and AI Solutions services. It mainly offers eDiscovery and forensic services, such as data collection, data processing, data review and document production. The company primarily serves law firms, corporate legal departments, government agencies and other professional advisors who require innovative technology, responsive service and deep subject-matter expertise. Geographically, the company receives maximum revenue from the United States.

> **With the Commvault Cloud Rewind platform, we have successfully recovered from a major cyberattack. Without Commvault Cloud Rewind's support, it would have been a huge loss to our business besides paying the ransom as well as an unknown damage to the company's reputation. I would be happy to provide references to Commvault Cloud Rewind anytime."**
>
> CIO
> eDiscovery Leader, USA/Japan.

CHALLENGE

When the company migrated workloads from the on-prem to Azure, the Cloud and IT teams wanted to make sure that their eDiscovery platform is resilient against any kind of cloud environment disasters, including ransomware attacks. All their services are hosted in Azure, spanning across 1500 plus Azure resources including Virtual Machine's, VMSS, Load Balancers, Application Gateways and Storage Accounts, and many other associated cloud services. Considering the complexity of the architecture, even after enabling multiple backup systems, achieving resilience against disasters was still questionable.

Adding to the problems is the constant threat of encryption attacks across enterprises at the verge of global crisis on multiple fronts including the cloud skill shortage and the period of great resignation, war in Ukraine, which created multitudes of risks. The IT team was unsure and unaware of their own environment, which was designed, setup, configured and maintained by the previous teams. Moreover, the CIO wanted complete visibility on the resilience for the environment to recover applications from any failure. The company is required by law to be compliant with SoX and other mandates both in the USA and in Japan.

"With the Commvault Cloud Rewind platform, we have successfully recovered from a major cyberattack. Without Commvault Cloud Rewind's support, it would have been a huge loss to our business besides payingthe ransom as well as an unknown damage to the company's reputation. I would be happy to provide references to Commvault Cloud Rewind anytime." CIO, eDiscovery Leader, USA/Japan.

SOLUTION

Rebuild Environments, Not Just Restore Data

This eDiscovery leader uses Commvault Cloud Rewind, for their 1500 plus Azure cloud environment resources to achieve resilience for their multiple applications running a wide variety of eDiscovery services for their customers. A typical application hosted in Azure includes their eDiscovery for financial, legal institutions, its own data management platform, and the IT infrastructure hub services. Commvault Cloud Rewind is enabled to protect all the application resources spanning across multiple Resource Groups running in the south-central US region.

Unfortunately, one regular day, the environment was compromised and brought down by 2 am in the morning. None of the Azure subscriptions could be logged into. All the accesses have been revoked as Active Directory was taken over by the attackers. All the managed disks were encrypted and inaccessible. In short, the business was brought down completely. Within a short span of time, Commvault Cloud Rewind was called for help to recover. The Commvault Cloud Rewind team quickly dialed into the call and started to do some situation analysis. As the Commvault Cloud Rewind platform maintains the copies of metadata and the state of all the application environments as immutable copies elsewhere and away from the customer environments, it was easy to initiate the recovery quickly. The first step was to identify the healthy point-in-time copy from the immutable data timeline. Commvault Cloud Rewind with a single click of a button was able to spin up each day's environment quickly by recovering a couple of the crucial systems to check if the data is in a healthy state.

Once the healthy timeline (the date and time just before the virus creeped in) was identified, the company could recover all other subscriptions resources and environments using Commvault Cloud Rewind's single click entire environment recovery. A single IT operations person was able to recover to a completely different vNet in the same region, isolating the recovery and allowing production to resume. The customer also kept the infected old production environment for further security forensics so the hackers can be prevented from entering again.

Overall, Commvault Cloud Rewind restored 18 subscriptions, including all applications, associated resource groups, and dependencies, in under 36 minutes. The recovery could have been completed in about 15 minutes with parallel initiation of environment recoveries. However, additional time was taken to carefully prioritize the recovery process, ensuring the most critical assemblies were restored first and less urgent ones were given appropriate attention.