

Minimizing Ransomware Risk for a Highly Diverse IT Infrastructure

Veritas and Azure team up to provide efficient—and effective—data protection.

Challenge

Cyprus Trading Corporation Plc (CTC) was using five different data protection solutions to back up and recover information across a disparate IT infrastructure. For resiliency purposes, the company engaged a third party to transport tape backups offsite. Efficiency suffered in this environment, as management and monitoring of data protection required one full-time equivalent (FTE) in staff time. The approach also raised compliance concerns and risked substantial data loss in the event of ransomware or other disasters.

Solution

CTC deployed a Veritas NetBackup™ Appliance in each of its two on-premises data centers and a NetBackup software instance on a virtual machine (VM) in each of its two Microsoft Azure cloud environments (North and West Europe Microsoft Azure sites). On-premises data backs up to a physical appliance first, then NetBackup Auto Image Replication (AIR) replicates the backups from the on-premises data centers to the Azure cloud. Veritas Resiliency Platform orchestrates the VM replications between all four sites (two on-premises and two in Azure). Meanwhile, the CloudPoint feature of the NetBackup VMs provides Azure-native snapshot backups for the company's cloud applications.



Cyprus Trading Corporation Plc

INDUSTRY

Retail

EMPLOYEES

Approx. 2,000

HEADQUARTERS

Nicosia, Cyprus

WEBSITE

ctcgroup.com



We needed a solution to provide us with peace of mind from ransomware attacks whilst at the same time provide efficiency and resilience for our day-to-day operations. The bonus that was presented through the Veritas solution was the ability to have live replication to our Azure cloud disaster recovery site that could readily use either the current data or, in case of an attack, the protected backed up data, natively."

George Louca, Finance and Information Technology Director, Cyprus Trading Corporation Plc

Outcome

The Veritas solution has reduced the amount of staff time CTC must dedicate to data protection to less than an hour a day, eliminating almost all of the FTE previously required. Backups and data restores complete in a fraction of the time they required previously, and the efficiency of NetBackup's approach to backup storage has reduced the company's spending on Azure storage by 25%. Most important, stakeholders throughout the organization have a renewed confidence in CTC's ability to recover should a ransomware or other disaster strike.



We test regularly, so we know every VM that is crucial to the organization is ready to take over day-to-day operations from within our Azure cloud."

George Kentas, Infrastructure and Network Manager, Cyprus Trading Corporation Plc

Diverse Infrastructure in Need of Standardized Protection

Established in 1929, Cyprus Trading Corporation Plc (CTC) has grown over the past century to encompass a wide array of products and services. Its lines of business range from department stores, fashion and beauty outlets, and home improvement retailers to distribution and logistics providers to automotive, property development, and airport management companies. CTC has operations in Cyprus and Greece, with plans to expand into additional European countries.

The diversity of CTC's operations strengthens its financial resiliency and bottom line. At the same time, though, the corresponding diversity in the corporate technology infrastructure has potential to create risk for the organization.

"Ransomware is a major concern for us," says George Kentas, Infrastructure and Network Manager for CTC. "All aspects of the organization's infrastructure must continuously be available to users and management." The centralized IT team is responsible for network and infrastructure operations groupwide. "Although the individual business units have their own IT teams, we manage security and backups across all business groups."

A few years ago, CTC relied on five different solutions for backup and recovery across its varied IT environment. This created several challenges. One was that managing the different data protection systems required the dedicated effort of two people for half a day, every day."

"Prior to NetBackup, we had to log into five different platforms daily to check on backup success," G. Kentas explains. "Then, if we had a failure, we would have to investigate the problem. Since most of the solutions were outdated, we didn't have support on them. We would have to dig into online forums to figure out how to resolve the problem."

Worse than the inefficiency, this approach opened the door to concerns about data recovery. The data protection solutions were slow, so the IT team ran full backups of each system twice a week. Had CTC experienced a ransomware attack or other crisis, it might have lost multiple days' worth of data.

For long-term, offsite retention, staff would remove tapes from drives, contact an external service provider to pick them up, then hand them off for transport. This process compounded security and compliance concerns. "We store a lot of personal and sensitive information, including customer contact information and transaction data," G. Kentas says. "The implementation of GDPR [the European Union's General Data Protection Regulation] led to a lot of compliance concerns in our internal audit department."

Data Protection Needs: Reliability, Efficiency, Azure Connectivity

When the company began upgrading its aging IT infrastructure, data protection was a clear candidate for improvement. "Our solution selection revolved around the products' ability to protect our infrastructure from ransomware," G. Kentas says. "We were looking for a

single platform that could cover a variety of systems, with both backups and replication that could move live servers from one site to the other with minimal downtime.”

Security measures, such as encryption, were imperative. So was tight integration with Microsoft Azure. “Modernizing our network architecture was going to involve transitioning to virtual machines [VMs] and cloud-based applications and data,” G. Kentas says. However, the public cloud was not a good option for most CTC systems. “Communications networks in Cyprus have high latency, so moving critical applications to the cloud would impact our ability to do business.

“We decided to move to an Azure Stack Hub, hosted within our data center, for our major operations in Cyprus,” G. Kentas adds. “After testing in multiple sites, we decided that Azure would be the fastest and most reliable option. The Azure roadmap was also important to us. For our Greek operations, we moved many applications to the Azure cloud because Greece doesn’t have the same latency issues as Cyprus.”

Adds George Louca, Finance and Information Technology Director for CTC, “We needed a solution to provide us with peace of mind from ransomware attacks whilst at the same time provide efficiency and resilience for our day-to-day operations. The bonus that was presented through the Veritas solution was the ability to have live replication to our Azure cloud disaster recovery site that could readily use either the current data or, in case of an attack, the protected backed up data, natively.”

The needs for efficiency, Azure integration, and—most important—reliable and secure data protection led CTC to Veritas.

Minimizing Resources Required for 12-Year Retention

CTC consolidated data and applications in two Cyprus data centers. One houses the Azure Stack Hub, where most of the company’s core solutions reside. The other runs a Hyper-V virtual environment. CTC also built two Azure cloud environments, one in West Europe and one in North Europe.

Both on-premises data centers back up to local Veritas NetBackup Appliances. Veritas Resiliency Platform orchestrates replication of the primary backups from one data center to the other, and NetBackup Auto Image Replication (AIR) technology performs the replication. For this process, CTC uses a dedicated fiber connection that bypasses the performance-challenged Cypriot communications networks. NetBackup AIR also replicates the on-premises backups to NetBackup VMs in both Azure public cloud environments and, in parallel, the solution replicates some data from the Azure Stack to the Azure cloud for long-term storage. Veritas Resiliency Platform orchestrates all these steps.

The on-premises data centers retain backups for 14 days. The West Europe Azure environment retains backups for three months, while the North Europe Azure environment—which serves as the company’s long-term data retention facility—stores backups for 12 years. “That’s our disaster recovery plan in case something happens on the on-prem side,” G. Kentas reports. “We have predefined playbooks, which we test regularly, so we know every VM that is crucial to the organization is ready to take over day-to-day operations from within the instance in our North Europe Azure cloud.”

For the Greek business unit’s cloud applications, the CloudPoint functionality within the NetBackup VMs on Azure takes Azure-native snapshots and replicates those snapshots to the Azure-based long-term retention site. G. Kentas is impressed with the efficiency of this approach.

“Other data protection solutions require a certain amount of storage per VM or service,” he says. “Customers have to allocate space for the maximum size of each system’s backups over the entire retention period. But CloudPoint deletes the snapshots to minimize required storage. Combined with NetBackup deduplication and compression, this feature has reduced the cost of Azure storage for our backups by 25%.”



The Azure Stack backups are both scalable and efficient due to the Veritas solution's parallel streaming framework. As the needs of the cluster grow, and CTC adds more data nodes to increase processing power and storage capacities, NetBackup Parallel Streaming enables CTC to also add more backup hosts to meet the growing needs of the cluster. This backup-and-recovery scalability mirrors the needs of the cluster environment without requiring CTC to install clients or agents on name node or data node servers.

"Because NetBackup Parallel Streaming technology is built directly into NetBackup," G. Kentas says, "we are taking full advantage of its familiar UI [user interface] for policy-based administration; job scheduling; data movement, monitoring, reporting, cataloging, storage allocation, MSDP pools; and granular recovery of individual files or folders, all through the NetBackup console."

Veritas Solution Breeds Confidence

Across the board, the Veritas environment accelerated CTC's backups. "It's amazing how much faster the system is running," G. Kentas says. "Our database backups complete in about one-third the time they took in our legacy environment. They always complete within the backup window and are almost always successful. If we were to face a crisis like ransomware, there would be much less data we could potentially lose."

The IT team is thrilled with the reliability and single-pane-of-glass backup management across the diverse IT infrastructure. "One team member approached me the other day and said, 'George, I want you to know I am very happy about the new backup solution. We don't have a single failure on our daily backups. It's running so smoothly, I don't have to do anything anymore,'" G. Kentas says.

"Now, the team spends 20 to 25 minutes every morning making sure backups finished successfully, with another half hour or less checking replications," he continues. "We're saving the equivalent of one FTE [full-time equivalent] by eliminating a half day's work for two people every day."

The same data takes about 50% longer to restore than to back up, which G. Kentas says is twice as fast as in CTC's previous data protection solutions. The team's routine tests of data restores do occasionally encounter a failure. G. Kentas says that these are mostly due to misconfigurations on the CTC side—and that they have highlighted the effectiveness of Veritas Support Services. "When we have a failure on a data restore, we contact Veritas Support to get advice on how to change our policies," he says. "We open a ticket, spend a little time on the phone with the support group, and together we solve the problem."

Ultimately, the consolidation of data protection across the company's diverse technology infrastructure provides peace of mind for the entire IT team and CTC at large. "The Veritas solution eases our internal audit team's concerns around GDPR and other compliance issues," he says. "We presented the solution to them, and they understand that our backups now comply with their standards for protection against ransomware. Having the Veritas and Microsoft Azure solution in place gives my team, and CTC's entire management team, greater confidence in our ability to recover should ransomware or other disaster strike."

For More Information

Please contact your local Veritas Sales Representative or Business Partner, or visit [Veritas NetBackup Appliance](#)

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 87% of the Fortune Global 500—rely on us to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match Veritas' ability to execute, with support for 800+ data sources, 100+ operating systems, 1,400+ storage targets and 60+ clouds through a single, unified approach. Powered by our Cloud Scale Technology, Veritas is delivering today on its strategy for autonomous data management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact