

Creating a Single-Vendor Backup Environment Aligned with the 3-2-1 Rule

Essential Veritas solutions for achieving cyber resilience.

The Mizkan Group, which handles the planning, development, manufacturing, and sale of household and commercial food seasonings, processed foods, and natto (fermented soybeans), is working on creating an environment to achieve cyber resilience with data protection across multiple environments, to protect itself from increasing malware threats such as ransomware. The chosen foundation for this includes NetBackup Flex Appliance, which is equipped with intrusion detection and prevention features, and Veritas Alta Recovery Vault, the cloud-based, fully managed data-retention service.



Mizkan J plus Holdings Co., Ltd.

Mr. Takashi Kumada, Section Manager, Information Systems Department, Administration Division (right)
Mr. Kotaro Seki, Information Systems Department, Administration Division (left)

Strengthening the backup environment is necessary for business continuity

Mizkan Group began in 1804 when Matazaemon Nakano, the founder of Mizkan, took on the challenge of making kasuzu vinegar from sake lees produced during sake brewing. Today, the company has expanded its business outside of Japan to Asia, North America, and Europe. In its medium-term management plan for 2024, the company defined its mission as "Bringing flavor to life," its vision as its "Future Vision Statement," and its value as "Together."



Company Overview

Mizkan Group

<https://www.mizkanholdings.com/ja/>

Number of Employees: Approximately 3,700
(the entire group as of April 1, 2023)

Industry: Food products

Business overview: Development, manufacturing, and sale of household and commercial food seasonings such as vinegar and ponzu, as well as processed foods and natto. The company also operates globally with international brands, offering products such as pasta sauces and sweet pickles.

Implemented products:

NetBackup Flex Appliance
Veritas Alta Recovery Vault

Challenges:

Increasing threats such as ransomware required a review of the backup environment. The company was aiming to enhance their cyber resilience by establishing a backup environment in line with the 3-2-1 backup rule, including the use of cloud solutions.

Solution:

Strengthen ransomware countermeasures with NetBackup Flex Appliance, which features WORM storage units that can prevent data from being deleted or altered. Data stored in the cloud using Veritas Alta Recovery Vault undergoes data deduplication and utilizes encryption options during transfer to further enhance data security. Seamless replication to the cloud ensures a robust backup environment in line with the 3-2-1 backup rule.

Benefits:

Enhanced ransomware countermeasures with appliances featuring WORM storage units.
A robust backup environment in line with the 3-2-1 backup rule.
Rapid backups with high deduplication, enabling storage capacity compression.
A flexible restoration environment, allowing for full restores and file-level recoveries.

The Mizkan Group is also developing the brand "ZENB," which offers a future-oriented, well-being diet that uses as much of the plant as possible to provide delicious and healthy food that contributes to the health of people, society, and the planet. They will continue to provide new, high-value products such as ZENB noodles, which have been developed as a new staple food.

Mizkan had previously implemented a backup environment for data protection for its business systems. However, for its virtual infrastructure built on VMware, data protection primarily relied on snapshots using storage features, meaning that backups were not taken as complete images of the virtual machines. "When I joined the company and reviewed the backup environment, I found that while it was possible to revert to the point when snapshots were taken, there was a risk of being unable to recover if a fault occurred in the overall virtual infrastructure," recalls Mr. Koutarou Seki from the Information Systems Department, Administration Division at Mizkan J plus Holdings. Relying solely on storage features meant that recovery was not possible without the underlying infrastructure, and so there was a need to enhance the backup environment to enable recovery for other services.

Recently, the threat of ransomware has been increasing, and there have been reports from other companies in the same industry about the considerable time and effort required for recovery from ransomware attacks. "The concept of the '3-2-1 backup rule' for backups, which involves securely keeping multiple sets of data in different environments, including remote locations, was not fully recognized within our company. Therefore, we decided to raise awareness through internal training sessions and push ahead with strengthening our backup system," says Mr. Takashi Kumada, section manager of the department. This marked the beginning of a project to establish an environment aimed at achieving cyber resilience.

Evaluating Veritas: a single vendor for a "3-2-1 backup rule" environment

The new environment required a mechanism that could prevent encryption in the event of a ransomware attack, whether it was an on-premises or a remote backup environment. Additionally, it needed to have measures in place to minimize damage to the backup system itself, including safe data storage in a cloud environment isolated from the existing network. The company therefore considered mechanisms capable of establishing such a comprehensive backup environment.

During the process of evaluating multiple solutions, Mizkan were introduced to Veritas' solutions. One of the solutions was NetBackup Flex Appliance, which offers high fault tolerance against ransomware and other threats using tamper-proof WORM storage units. Another solution was Veritas Alta Recovery Vault, which enables seamless data storage in cloud environments. "With other solutions, we would need to procure and design hardware or cloud environments separately, which would make it costly and time-consuming to meet our requirements. With Veritas, we can prepare an all-in-one setup with on-premises appliances and cloud environments. We highly valued their ability to create a backup environment through a streamlined mechanism, including hardware, without complicating the configuration," says Mr. Seki.

Mr. Seki had experience of using NetBackup in his previous job and already knew that the solution was easy to use. "With NetBackup, you can perform full restores, restore specific files, or check the contents before restoring to ensure server health. This flexibility in selecting implementation methods was one of the major features of NetBackup that met our needs."

During solution evaluations, Veritas performed the best compared to other offerings, not only for meeting backup requirements but also for security and system functionality requirements. "What concerned us at the time was avoiding a situation where the data we had acquired would become contaminated. If the data isn't usable when we want to restore it, it would be like storing garbage. The fact that Veritas had numerous features that provided us with a sense of security, such as the ability to detect anomalies and malware during backups, was significant," says Mr. Kumada. Additionally, Mizkan was reassured by Veritas's leadership position as validated by external research firms.

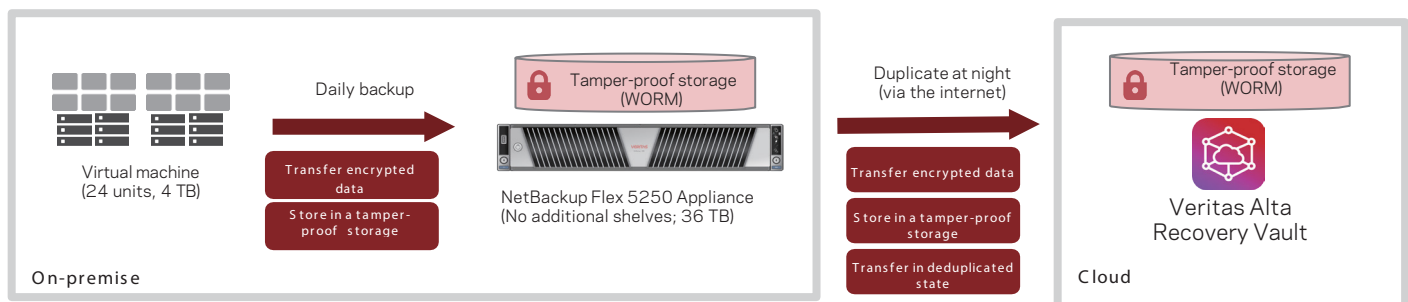
As a result, Veritas solutions combining both NetBackup Flex Appliance and Veritas Alta Recovery Vault were selected as the infrastructure for a backup environment aimed at achieving cyber resilience.



Cyber resilience with high recovery capabilities are enhanced with Veritas

Veritas solutions are currently used to back up around 24 VMs (totaling approximately 4 TB) running critical systems such as EDI, order systems, and domain controllers on VMware. The solutions use about 2 TB of capacity on an appliance with a total capacity of 36 TB, thanks to advanced deduplication. Daily backups are obtained on the NetBackup Flex Appliance after business hours. These are replicated to the Veritas Alta Recovery Vault, a cloud-based storage solution, in order to perform remote backups. "We currently store about 10 generations, but due to the high deduplication rate, we only use about half of the storage space. Considering the ransomware incubation period, we plan to increase the number to 30 generations," says Mr. Seki. In the future, there are plans to scale the NetBackup Flex Appliance for flexible expansion while gradually broadening the scope of business operations covered by the backup.

[Backup environment according to the 3-2-1 backup rule]



One of the benefits of implementing the new environment is the increased number of restoration options available in case of infection. "If a single virtual machine gets infected, not only can we restore it from local storage, but also from NetBackup. Being able to increase the number of options is significant," says Mr. Kumada. As a result, this has led to enhanced cyber resilience with the ability to recover quickly. Although the operational workload for backup acquisition has not changed significantly, the increased restoration options have made the recovery process simpler.

There are plans to create an environment that ensures business continuity at a minimum operational level by using other cloud environments for restoration in the event of damage to the entire virtual infrastructure. "If the infrastructure itself is damaged, recovery would normally take several weeks, including hardware procurement and backup system reconstruction. Moving forward, we will be able to create an environment that allows for flexible recovery, including the use of cloud environments, which will greatly reduce lead times for business continuity and minimize opportunity losses," says Mr. Seki, who praises this approach.

NetBackup's intuitive web-based dashboard displays backup status, making it simple for anyone to identify issues. "Policies can be set up easily, and adding virtual machines is as simple as a single click. Even new team members can operate it without any difficulties," says Mr. Seki. Although it generally takes more time to store backup data in the cloud as the volume of data increases, the high deduplication rate means that remote backups can be performed as quickly as backups to local storage. "The ability to sync backup data to the cloud in almost real-time is one of the great features of NetBackup with its high deduplication rate," says Mr. Seki.

The Veritas Technologies LLC's support team, who was integral to the implementation, has also been highly praised. "When we first consulted with them, they took the time to earnestly propose solutions. They provided comprehensive information for our internal training sessions, covering everything from backup concepts to the latest trends. They actively engaged in educational activities, not just product support. We are very grateful for their thorough support," says Mr. Seki. Mr. Kumada adds, "We encountered unforeseen issues due to factors on our end, but they provided expert knowledge and worked diligently to resolve them quickly. We appreciate their sincere support."

High expectations for broader backup coverage, more generations, and cloud integration

In the future, Mizkan plans to further expand their use of the system, with a view to extending its usage beyond specific virtual environments, while increasing the number of generations of backup data. "Currently, we are focusing on critical systems, but there are still many systems where backups have not yet been implemented according to the 3-2-1 backup rule. Considering the cost, we cannot back up indiscriminately, so we need to discuss and reach a consensus across the company," says Mr. Kumada.

The system not only includes on-premises environments but also business environments utilizing IaaS and SaaS platforms, and the company plans to promote consolidation using Veritas solutions wherever possible. "In the future, there will likely be cases where we deploy our system infrastructure to the cloud, making it essential to synchronize backups effectively. In the event of an on-premises failure, we will consider switching to the cloud immediately to resume and continue operations," says Mr. Seki enthusiastically. There are also high expectations for new solutions, including Veritas Alta solutions.

About Veritas

Veritas Technologies is a leader in multi-cloud data management. Over 80,000 customers—including 95 percent of the Fortune 100—rely on Veritas 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 the ability of Veritas 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 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 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