ORACLE

CIO
Strategic Marketing Services

PROTECTING THE DIGITAL ENTERPRISE

PURPOSE-BUILT STORAGE SOLUTIONS DRAMATICALLY LOWER COSTS AND RESOLVE DATA RECOVERY WOES—WHILE ENSURING THAT YOUR ENVIRONMENT IS CLOUD-READY.

INTRODUCTION

Enterprise data protection has grown unwieldy, with systems from various vendors claiming to protect all of an enterprise's data—and none of them doing a particularly good job of addressing mission-critical data recoverability requirements. It's a situation that introduces risk and raises concerns about IT's ability to recover in a timely manner and without data loss from outages caused by cybercrime, system failures, or human error.

An integrated strategy that focuses on the complete data recovery needs of an enterprise can eliminate data loss, cut recovery times, and reduce IT complexity—while ensuring data security and positioning the enterprise to seamlessly take advantage of the cloud.

RECOVERY IS EVERYTHING

The ability to quickly and reliably recover data is paramount, given the threats and requirements that organizations face—including cyberattacks and ransomware, regulatory issues, and compliance audits.

Consider, for example, the forthcoming European Union (EU) General Data Protection Regulation (GDPR), which applies not only to companies based in the EU but also to any company that holds information about EU residents. One of its requirements is "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." Noncompliance is not an option, with fines as high as €20 million (about US$21 million) or 4 percent of annual revenue, whichever is larger.

In today's regulatory and security environment, enterprises must take steps to ensure that they not only reliably back up data but, more importantly, can also recover it *fully* when needed. It's an increasingly important issue, given that researchers such as IDC project digital data to grow at a compound annual growth rate of 30 percent through 2025. Furthermore, 10 percent of this data will be hypercritical to business survival.

Against this backdrop, success will likely depend on shedding the complexity and costs of maintaining and managing a different data protection system for every data source. In choosing a new strategy, companies need to balance cost with the business risks associated with data loss and downtime, including the loss of sales, decrease in employee productivity, penalties from failure to meet regulations, and damage to brand reputation that can result from an incident. In addition, even if cloud-based data protection is still a future direction, all new solutions should be cloud-ready.

The best way to meet all these needs is with a hardware/software solution that is engineered to work together with the application or database whose data is being protected. Instead of layering generic software on generic servers, this engineered approach reduces loads on application and database servers while simplifying management. The result: reliable, repeatable recoverability that doesn't miss a critical part of a multistep backup or recovery—reducing business risk.

CURRENT STATE OF RECOVERABILITY

Businesses often buy general-purpose, underperforming backup systems with limited scalability—leading to backup system sprawl. What's more, these systems tend to focus on backup, not recovery, without understanding the underlying data or whether it is even recoverable.

Recovery may be excruciatingly slow as generic backup systems sort through days, months, or even years of data to piece together the information needed by an organization. The recovery process and validity of the data underneath it are rarely tested because it takes so long, which means many organizations don't even know whether their data can be reliably recovered.

Some organizations speed up recovery by using a different backup system for every database and application, limiting the amount of data a single backup system has to search through. But relying on multiple

With general-purpose backup systems, data recovery ends up being slow as the system sorts through days, months, or even years of data to piece together the information needed for recovery.

standalone systems leads to costly management challenges and security risks, with more personnel likely required to manage and secure more systems, each with its own set of processes and homegrown scripts. With such an unwieldy setup, it's not unusual for a backup system or process to fail and for the failure to go unnoticed until it's too late, leading to unrecoverable data.

In short, the situation leaves companies exposed to multiple business risks, including:

- Short-term data loss
- Unrecoverable backups
- Noncompliance with industry and government regulations
- Lengthy recovery periods and extended downtime
- Loss of sales, revenue, and employee productivity
- Security gaps and exposure to ransomware and cyberattacks

FIVE ENTERPRISE DATA PROTECTION REQUIREMENTS

A true enterprise-ready data protection solution must focus on the recovery needs of the organization while ensuring the security of data, reducing IT complexity, and lowering overall costs. The following five requirements are critical to a data protection environment that effectively balances cost and risk:

Recoverability to any point in time

It was once acceptable to back up data once per day and periodically record intraday changes. Perhaps a log file that held transactional information was backed up every four hours. So, in the case of a disruption, you could lose as much as four hours of data.

For most organizations, losing multiple hours of business-critical data is no longer acceptable. Financial organizations and companies with lots of valuable transactions certainly need to be able to recover data to any specific point in time without data-loss exposure. This requirement extends to organizations such as manufacturing firms that must be able to track all their materials and finished goods throughout various automated processes, and retailers that must keep track of inventory for in-store as well as online transactions.

Companies may also need to recover to a specific point in time to meet compliance requirements or to avoid having to pay ransomware, even if that point was three months or three years ago.

Verifiable and reportable recoverability

A shortcoming of most backup solutions is that silent data corruption is common—backups appear to be successful, but an attempted restore reveals that the original data is corrupted. At best, IT organizations have to jump through hoops to restore it; at worst, the data is lost—most likely forever.

An enterprise-ready data protection solution should automatically verify the viability of every backup. It should also be able to produce reports that show the status of each backup; whether it can be restored; and, if so, to what point in time. Such automated reports help businesses understand their risks and ability to meet compliance requirements.

Minimized recovery times

For several reasons, recovery times with legacy systems can be lengthy. For one, the data may be located in many different files that have been created over months or years and must be reassembled during the recovery process. Then the system operators must sort out which incremental backups need to be applied and make sure that they are also copied back to the system being recovered—all of which takes time. Stories abound of even moderate-size recoveries that take days, if they succeed at all.

Databases can be the most challenging type of data to recover from legacy backup systems, because each database has multiple pieces that must be recovered in a specific order. Legacy backup systems don't understand database structure, so they depend on the database server to manage the recovery process. A data protection system that actually runs a database internally will be able to identify, locate, and assemble the exact blocks of data required to fulfill a recovery request—and do so quickly.

Reduced security risks

Employing a different data protection system for each application and database inherently increases the security risk to an organization. More systems have to be secured, and more people have to be allowed access. As a result, the risk of complexity-induced human error or intentional wrongdoing is increased exponentially.

Aggressive cost management

An effective data protection solution helps keep costs down. For instance, a data protection solution should be able to efficiently deduplicate and compress data without requiring unencrypted data sources, thereby reducing the amount of data that has to be stored while maintaining security. It should also scale effectively, in terms of both capacity and performance, to avoid sprawl and keep recovery time down, minimizing indirect costs from loss of productivity and sales.

The ideal data recovery solution should also tightly integrate with the company's software and hardware management environment to obviate the need for staff dedicated to operating it. If a system is meant to protect a database, for example, it should come with management tools a database administrator understands.

Databases can be the most challenging type of data to recover from legacy backup systems, because each database has multiple pieces that must be recovered in a specific order.

ARCHITECTED FOR SUCCESS

Numerous enterprises are taking advantage of the benefits Oracle data protection platforms provide.

Specialized Bicycles Components experienced significant performance improvements with Oracle ZFS Backup Appliance. The average time to back up production databases dropped from eight hours to nine minutes. In addition, system administrators saw a 12-fold increase in the speed with which they could clone databases in their development and testing environment. Click here to read more.

KEB Hana Card, a leading credit card provider in South Korea, achieved similar results with the Recovery Appliance. It can now back up data 13 times as fast as with its previous solution while achieving a 65 percent capacity savings, which has enabled the company to eliminate two-thirds of its backup storage footprint. Most importantly, it is now processing US$850 million per month in payments with zero data loss.

"Only Oracle could offer the incremental-forever backup feature, enabling us to eliminate data loss exposure and ensure data security," says Iljoon Lee, senior manager of KEB Hana Card's IT team. Click here to read more.

THE ORACLE APPROACH: PERFORMANCE, CONSOLIDATION, INTEGRATION

Oracle has developed an approach that addresses all the requirements of an enterprise data protection solution. It starts by recognizing that the most-valuable data stored in your databases is the most likely to be under attack and therefore needs the best-possible protection and recoverability. The approach then integrates high-performance solutions that reduce the complexity and cost involved in protecting the rest of your corporate data.

Deep storage integration drives more functionality, improved performance, greater efficiency, and increased simplicity.

CONSOLIDATE AND PROTECT CRITICAL DATA WITH ORACLE STORAGE

PROTECT ORACLE DATABASES WITH ZERO DATA LOSS RECOVERY APPLIANCE

- Up to 10x faster data recovery
- 18x performance and 100x capacity scaling
- Real-time recovery status
- Recover to any point in time
- End-to-end data validation
- Millions in savings

BACK UP ALL OTHER DATA ONTO ORACLE ZFS BACKUP APPLIANCE

- Restore data 2x to 5x faster than legacy purpose-built-backup-appliances
- Half the cost
- High availability
- Oracle Database optimizations
- Flexibility to also support dev/test and production

Protection of business-critical data

Because the most-critical data is typically housed in an Oracle Database instance, it needs the best protection available. That's why the Oracle Database development team created the Zero Data Loss Recovery Appliance (Recovery Appliance) as a data protection extension of Oracle Database.

The Recovery Appliance supports recovery to any point in time, eliminating the risk of even short-term data loss. It also validates all backups, delivering confidence that data can be recovered if necessary. And it helps reduce the financial risks associated with an outage, by recovering data up to 10 times as fast as legacy solutions.

Recovery Appliance also helps reduce the total cost of ownership, by enabling companies to consolidate multiple existing standalone backup systems into a single, scalable, high-performance data protection solution that leverages its built-in Oracle Database deduplication and compression technology. It also efficiently protects databases secured with Oracle Transparent Data Encryption technology, so data never has to be decrypted by the appliance. Such antitheft data protections can help companies comply with data protection requirements, including GDPR.

General-purpose data protection

Once mission-critical data is protected, the next step is to migrate general-purpose data from other standalone systems onto an Oracle ZFS Backup Appliance, which can protect all user, application, and database data.

The Oracle ZFS Backup Appliance makes it less likely that non-database backups will be unrecoverable, by more rapidly performing backups and restores, leaving time for backup validation so they are known to be good, and encrypting them so they can't be stolen. It also includes self-healing technology that ensures that any validated backup remains restorable. Customer testing has shown that using the Oracle ZFS Backup Appliance results in higher recovery success rates and also enables restores to complete two to five times as fast as on legacy systems, at one-half the cost.

The Oracle ZFS Backup Appliance has six times the capacity of competing systems, enabling significant system consolidation for longer-term archiving where performance is less of an issue. In addition, it supports use cases beyond data protection, including application development and testing, business analytics, reporting, and more—helping companies gain more value from their data protection investments.

Cloud-ready data protection

Whether or not the cloud is an important part of your current approach to data protection, it inevitably will play a major role. Both the Recovery Appliance and the Oracle ZFS Backup Appliance are inherently cloud-ready, with complementary and equivalent services available in the Oracle Public Cloud. Oracle is the only vendor to combine both on-premises and cloud capabilities so your investments will be cloud-ready when you are.

For more information, go to **www.oracle.com/engineered-systems/data-protection-recovery.html**