DLT

WHITEPAPER

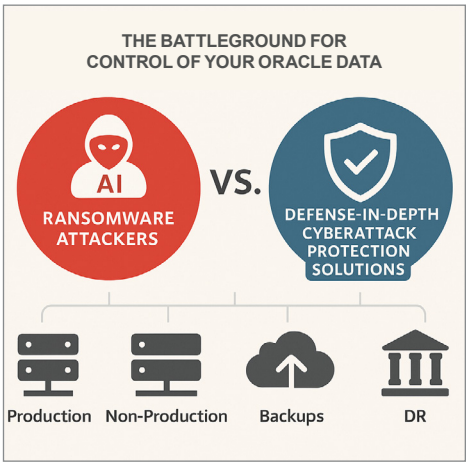
Oracle Database Cybersecurity Architecture Protection Against Ransomware

ORACLE | Partner

An Oracle Database Cybersecurity Architecture for Protection Against Ransomware Attacks:

Oracle Zero Data Loss Recovery Appliance

The battleground for control of your data includes ransomware attackers and other cyberattackers vs your defense-in-depth cyberattack protection solutions. Cyberattacks are a proven and on-going risk for all organizations. Besides the traditional best practices and even new methods for securing the network and access to your databases, the database itself must be treated as an integral part of your defense-in-depth cyberattack protection for the inevitable instance when the attackers get through to your database.



As we have seen over the years in many news reports, sensitive and/or mission critical data is a prime target for profiting by cyber or ransomware attacks. In many risk frameworks, including NIST, the risk is modeled as the product of threat, vulnerability, asset value, and impact. To reduce the risk to their data, organizations must take a holistic approach that incorporates the database as a critical layer in defense-in-depth cyberattack protection, leveraging a maximum security architecture for protection and ensuring reliable recovery.

- First, protect the data from being stolen while making it unusable by outsiders if it is stolen even when privileged, DBA, or other user's credentials are used or stolen to access the data
- Second, prepare for the inevitable cyber or ransomware attack by ensuring your data can always be quickly and reliably recovered with no data loss with the least impact to the organization

For an Oracle Database, the first aspect is well documented in the Oracle Maximum Security Architecture (see link below). While encryption is essential, it alone is not sufficient because stolen credentials from DBAs or others can still grant unencrypted access to the data. The architecture therefore outlines additional built-in data protection features that can be enabled at relatively minimal or no additional cost, whether you adopt an on-premises Oracle Database, a cloud-based option such as Oracle Autonomous Database, or a hybrid of both. Example data protection features for Oracle Database: Encryption, data masking, privileged user access controls, activity monitoring, auditing, etc. See details at:

https://oracle.com/security/database-security/

https://blogs.oracle.com/cloudsecurity/post/oracles-maximum-security-architecture-for-database-security

This paper will focus on the second aspect. However, only Oracle provides the full and complete protection required for both aspects.

Prepare for inevitable cyber and ransomware attacks with automated, rapid, and reliable data recovery that ensures zero data loss and minimal impact to your organization.

In the battleground for control of your data, one or both sides might use AI to help them in the battle to find and attack all of your data that's on your network including production, non-production, backups, and in your disaster recovery (DR) site. When they find vulnerabilities and/or steal credentials and take advantage of them that leads to a ransomware event or other data loss, you hope that your cybersecurity/ransomware insurance (if you have any) covers the cost of data recovery including the ransomware payment. But insurance can't change how others view your organization after the damage is done. It also doesn't cover situations where the required payment is more than your insurance coverage, when ransomware attackers fail to release the data even after the ransom is paid or leave all of your data including backups and DR corrupt and unrecoverable.

With traditional database backups using non-Oracle tools, the impact of a single unrecoverable transaction (from bad file or tape) can cascade to other dependent transactions, affecting data integrity across applications and other databases. Ransomware and other cyberattacks contribute to potentially unrecoverable data. This ultimately puts data quality and production operations at risk given the extreme time and costs of data recovery, if recovery is even possible. With traditional data backup and business continuity methods, full or even partial data recovery might not be possible depending on the extent and spread of deleted or corrupted data either directly by the attack or via traditional replication of the affected data to backups, DR sites, etc.

Confidence that database backups are indeed recoverable requires database-aware backup validation at the transaction-level and not just one-time when the data is being backed up. For Oracle Databases, Oracle Zero Data Loss Recovery Appliance (Oracle ZDLRA or Recovery Appliance) provides an Oracle Database cybersecurity architecture for protection against ransomware attacks. It provides extreme Oracle Database-aware real-time protection against ransomware and other cyber threats, with advanced security, isolation, immutable backups, frequent auto-healing validation of previously backed up data, and recovery capabilities. Data recovery should be an integral part of everyone's defense-in-depth security strategy. Oracle ZDLRA provides this by mitigating risk and ensuring rapid point-in-time recovery without the shortcomings of traditional backup solutions such as missing or corrupt incremental files/tapes (including data rot), complexity/cost of recovery using 3rd party tools, vulnerability to ransomware and other cyber threats, etc.

When a ransomware attack against Oracle Databases happens with Oracle ZDLRA protecting these databases, **don't pay the ransom**, just recover the database from Oracle ZDLRA with no data loss.

ZDLRA can be deployed in a network-isolated vault "Cyber Vault" location where physical network connections are restricted to periodic backup synchronization. This allows airgap backup copies (Golden Images of current data) to be created in a secure location, safe from ransomware attacks on your Oracle Databases. The Recovery Appliance's design allows for a much shorter time needed for the Recovery Appliance within the Cyber Vault to synchronize compared to traditional RMAN backups. (RMAN is Oracle Database's built-in tool for performing backups and recovery tasks)

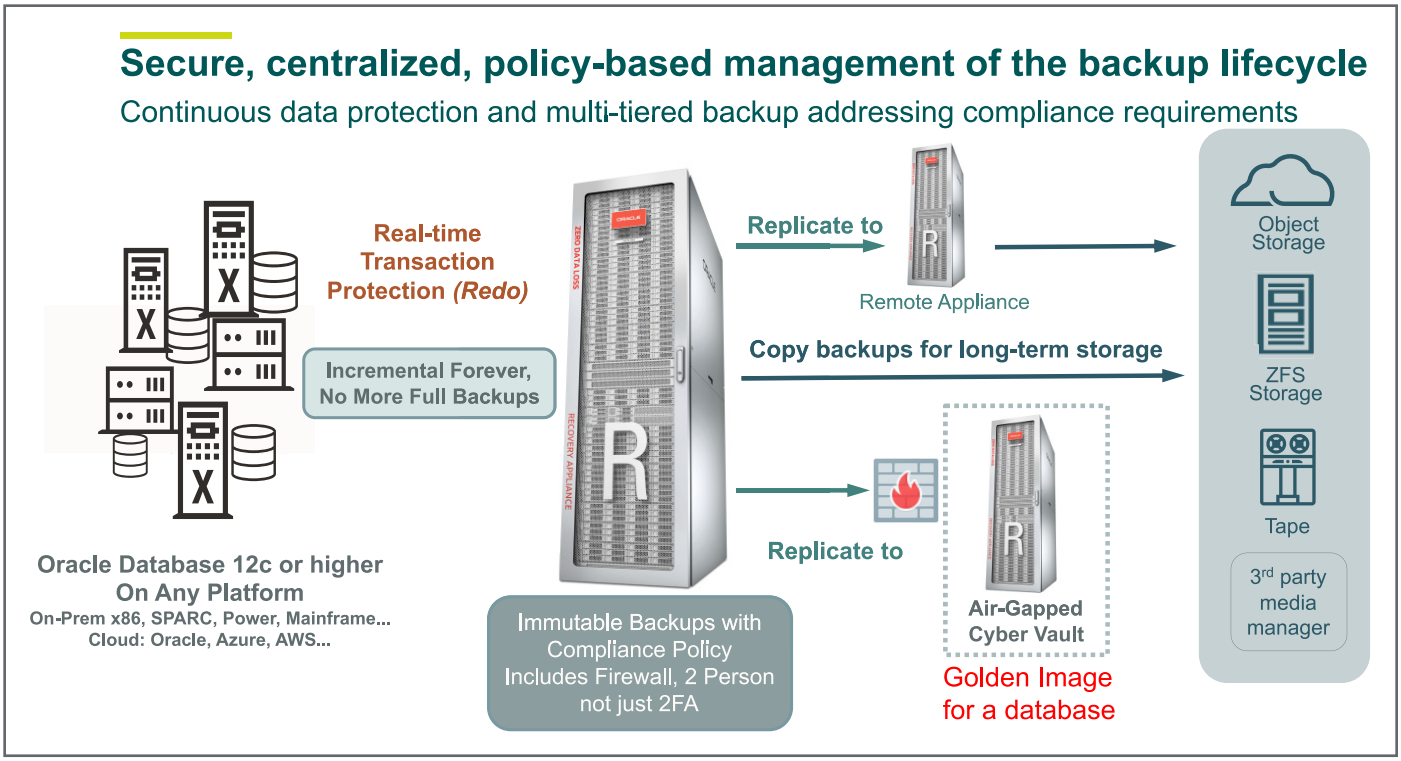
Oracle ZDLRA's incremental forever model and real-time redo transport reduces the need for intensive long backup windows as well as off-loading much of the backup, compression, deduplication workload from the server and uses less network resources vs other backup solutions.

The ZDLRA delivers significant reductions in processing compared to traditional RMAN backups by offloading tasks such as full backup synthesis, validation, compression, and catalog management to the appliance. This approach minimizes CPU, memory, and I/O consumption (both storage and network) on the database server, improving performance and resource efficiency. Leveraging its incremental forever backup model and real-time redo transport, ZDLRA further reduces the impact on server and network resources, eliminating the need for intensive, long backup windows. By integrating seamlessly with Oracle RMAN, ZDLRA enhances Oracle database backup and recovery processes, offering a more reliable and efficient solution.

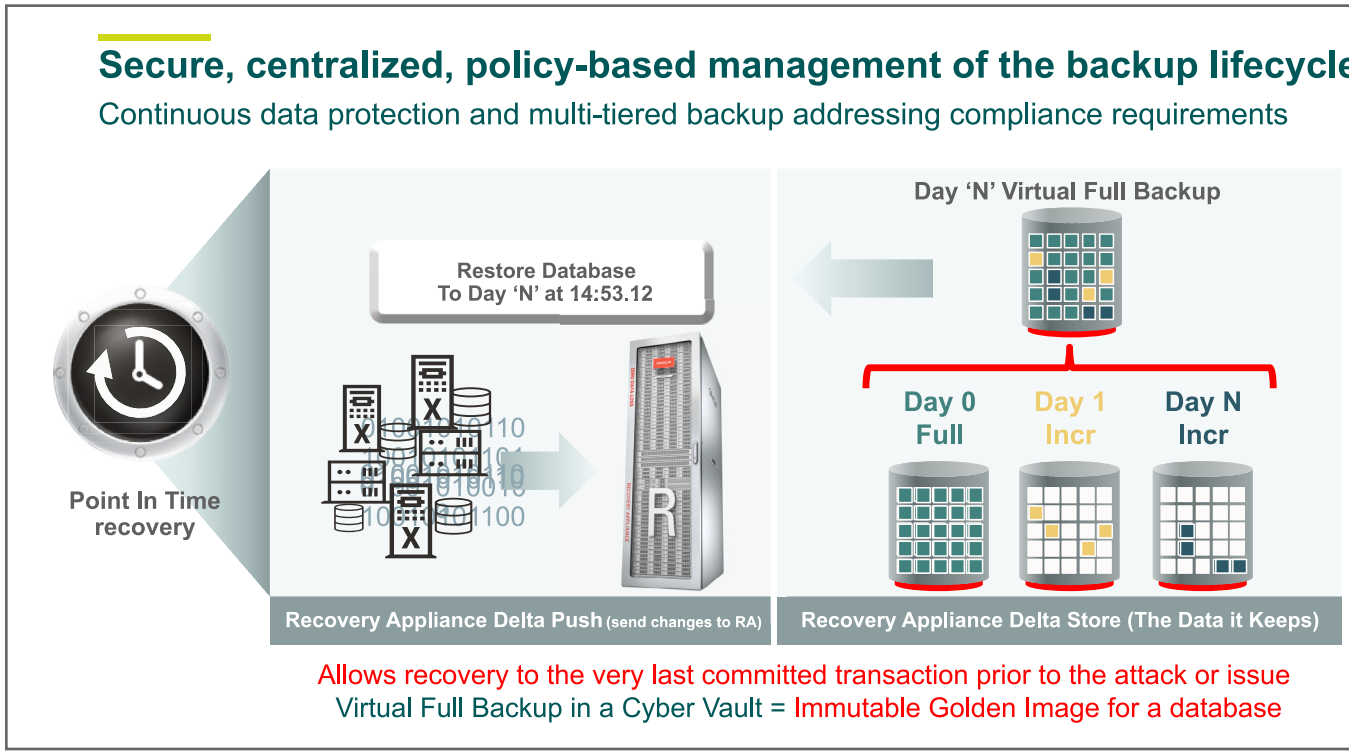
Oracle ZDLRA is an Oracle engineered system designed specifically for Oracle database protection. (It's an enhanced Oracle Exadata) The X4 version was introduced in 2014 and upgraded/enhanced almost annually to version RA23, which is the 8th generation Recovery Appliance and is the current version as of August 2025. The Recovery Appliance tackles these modern threats with innovative resilience, extreme performance, secure separation/isolation, transaction-level protection, and end-to-end automated recovery auto-healing-validation capabilities not available with any other solution in the market. These capabilities ensure successful database recovery whenever needed to any point-in-time that saves time and costs in data recovery.

As the premiere Oracle Engineered System for protecting all your Oracle Databases, ZDLRA is fault-isolated from the production database, so if a cyberattack hits the database, the appliance is not compromised. The Recovery Appliance inherently provides designed-in superior resilience and recovery capabilities against database cyberattacks. These include but are not limited to:

- Real-time protection for all your Oracle Databases across any platform
- Zero data loss recovery if your Oracle Database is hit by an attack
- Immutable Backups
- End-to-end recovery validation (both validation when backed up and frequent auto-healing validation of previously backed up data)
- Airgap Cyber Vault protection (deployment choice)
- Incremental forever paradigm (minimizes the amount of data replicated to the Cyber Vault and helps keep the Cyber Vault connection time window as short as possible lowering the impact of backup on server and network)
- If a Full Recovery is needed, a Virtual Full is derived from the Incrementals greatly saving restore times, complexity, and ability to restore since nothing is missing or corrupt
- Extreme separation of duty (RBAC and more)
- Exadata-based security resiliency, HW & SW hardened, high-availability features, extreme performance helps minimize the impact of backup on server and network and the time needed for Cyber Vault connection, etc)
- Limited network access
- Follows documented Oracle Maximum Availability Architecture
- And many more



High-Level example with multiple choices for Cyber Vault, Cloud, ZFS storage, and/or Tape



A single step recovery is via virtual full derived from the Incrementals

Also available as an Oracle Cloud Service, Oracle Database ZDLRA is a fully managed data protection service for Oracle databases running on Oracle Cloud Infrastructure (OCI). Low costs based on the amount of data being protected mean that zero data loss resiliency is available to organizations of any size and virtually any budget. Only Oracle offers comprehensive protection to keep your data secure even if credentials are stolen while enabling rapid, reliable recovery with zero data loss.

Only Oracle offers comprehensive protection to keep your data secure even if credentials are stolen while enabling rapid, reliable recovery with zero data loss.

Additional Information

- Oracle ZDLRA datasheet:
  https://oracle.com/a/ocom/docs/engineered-systems/recovery-appliance-ra23-datasheet.pdf
- Oracle ZDLRA website:
  https://oracle.com/engineered-systems/zero-data-loss-recovery-appliance

About DLT

Since 1991, DLT Solutions has been a trusted Oracle partner for the Public Sector. We combine deep expertise across Oracle technologies including software, infrastructure, Oracle Support renewals and Oracle Cloud with dedicated professional services to deliver mission critical solutions that support your mission. We also provide multiple contract vehicle options to simplify procurement of Oracle products and services, including but not limited to SEWP for federal and DoD customers and OMNIA for state and local entities.

2411 Dulles Corner Park, Suite 800, Herndon, VA 20171

Main: 800.262.4358 | eFax: 703.709.8450

DLT.com/Oracle

ORACLE | Partner