



Engineered Data Protection for Oracle Database

Oracle's Zero Data Loss Recovery Appliance



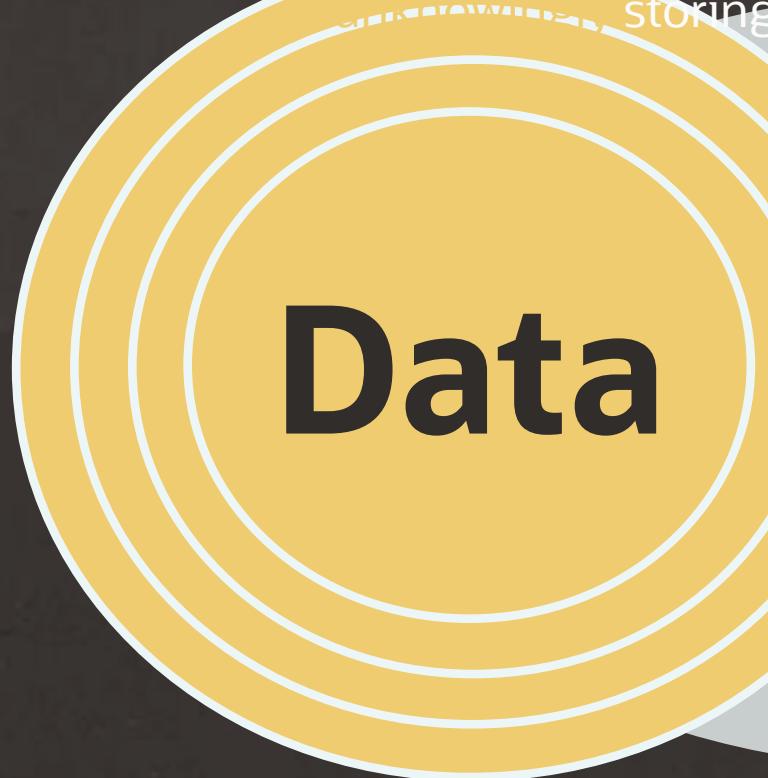
Alexandre Fagundes

LAD Partner Enablement

May, 2022

Your data's safety net

The only thing worse than not protecting data is
storing and relying on invalid backups!



Data

Protection

Protect against corrupt files and human error
and ensure data integrity across databases

Provide assurance for long-term data

Minimize the cost and expense to recover from a
disaster or security attack

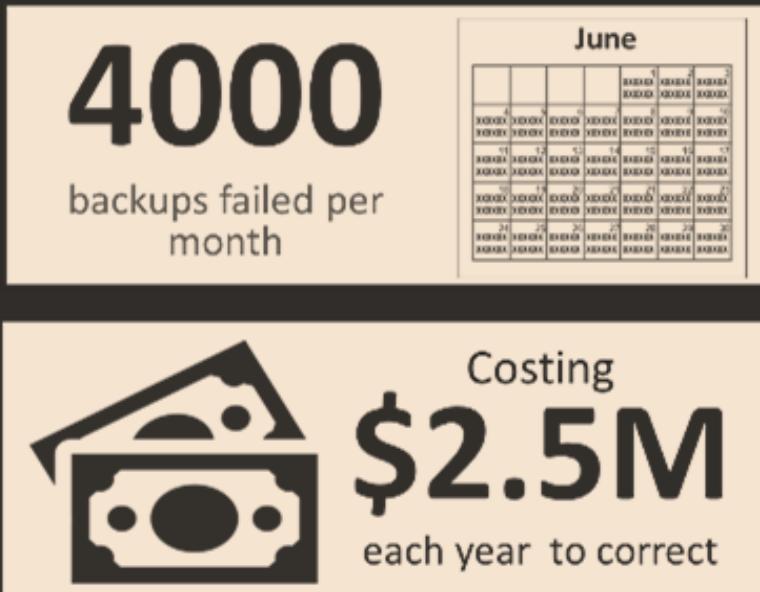
*"Would you rather assume or **know** backups are valid?"*

Lack of data recovery ability is an expensive proposition

Leading global financial services company experiences



60%
of all restores failed



Regulatory Compliance Backup / Recovery Issues

- Massive, costly offsite tapes
- Missing / corrupt backups
- Slow, complex recovery
- Non-compliance penalties

The value and impact of business transactions and data

- **Transactions drive revenue**
 - Trades
 - Purchases
 - Passengers
- **Trust impacts reputation**
 - Social security numbers
 - Credit cards
 - Health records
- **Downtime disrupts business**
 - Customer churn
 - Missed deadlines
 - Regulatory compliance violations



What is your data protection strategy?

Ransomware is the modern day version of a bank robber in the wild west

Resilient recovery with no data loss is a foundational requirement for data-driven businesses



Over **4,000** attacks
daily
([source: FBI](#))



US organizations
lost more than **\$7.5**
billion in 2019
([source: Emsisoft](#))



Average total cost
of remediating
\$1.85M
([source: Sophos](#))



19-day average
downtime
([source: Coveware](#))

One minute of data loss due to ransomware attack could impact 100s / 1000s of database (e.g. business) transactions.

What's your confidence level?

Your business depends on data and data recovery depends on valid backups

- **Backup and restore failure is common**
 - Some failures can succeed upon retry; some cannot
- **Restore is typically much slower than backups**
 - Slow restore and recovery increases costly downtime
- **Backup processes can impact production**
 - Full backups, deduplication and other backup processes consume database server resources degrading performance



**Recoverable
Backup?**

Leadership in database recovery and backup management

Oracle's Zero Data Loss Recovery Appliance

- Provides recovery assurance
- Reduces business risk
- Simplifies antiquated data protection complexities
- Saves personnel time
- Reduces infrastructure overhead freeing up resources

*Innovation moving beyond
traditional backup appliances*

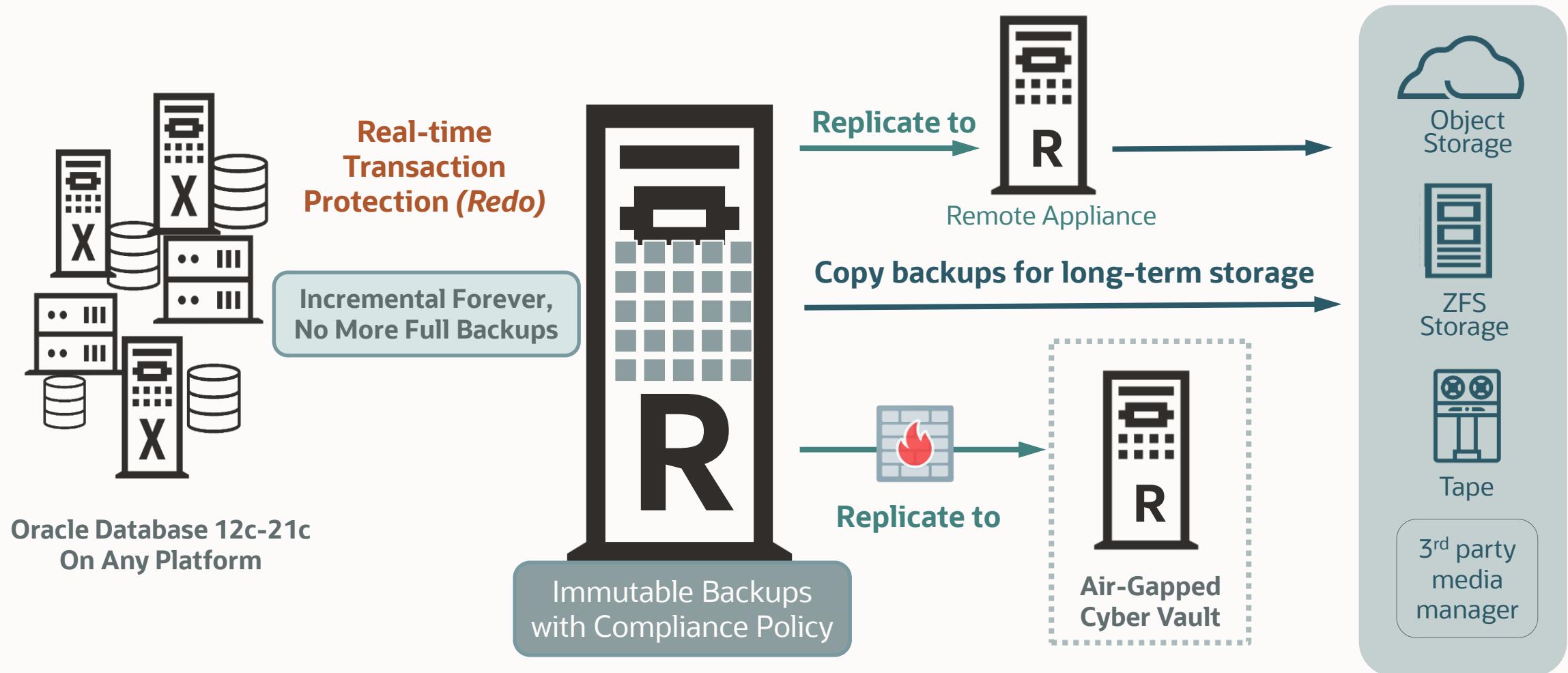


for Oracle Database protection



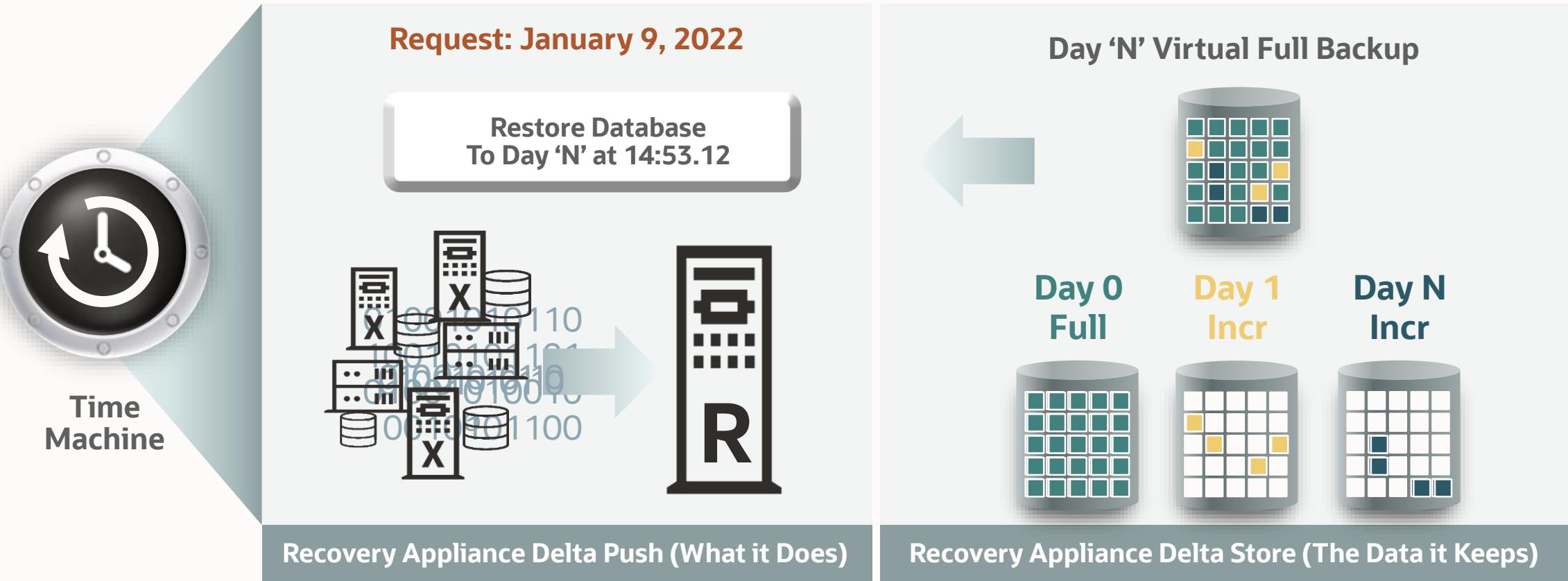
Centralized, policy-based management across the backup lifecycle

Continuous data protection and multi-tiered backup addressing compliance requirements



Minimal impact incremental forever backup with virtual full restore

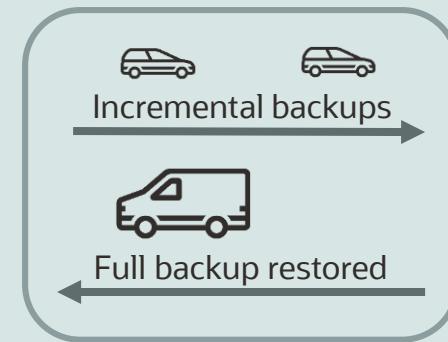
Pointer-based representation of physical full backup at incremental backup time



Recovery Appliance uses less personnel and infrastructure resources

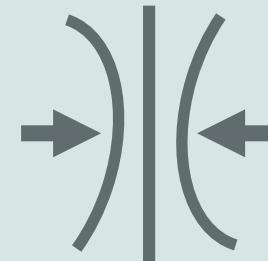


Applications
run faster



Less overhead on DB servers

Most backup / recovery processing is offloaded from database servers thereby freeing up resources for other operations



Less LAN/WAN traffic

Incremental forever backups and virtual full restore send less data over the network than periodic full backups and restore requiring a full backup *plus* incremental backups

Less storage consumption

Blocks are only stored once (e.g. deduplicated) and backups are compressed on the Recovery Appliance to further reduce storage consumption



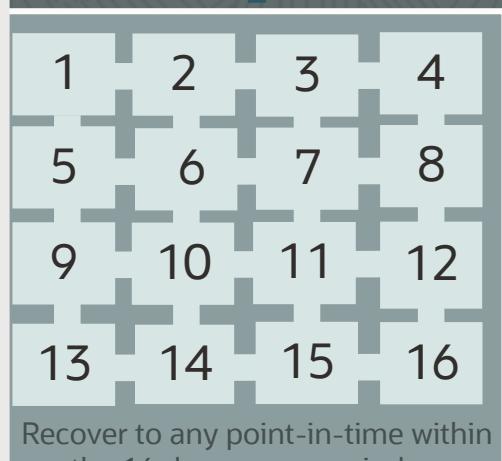
Less personnel time needed

Simplifies backup management by standardizing backup processes along with automated operations

Create adhoc or scheduled backup copies for long-term retention



Recovery Appliance



Recovery Window = 16 days
(Example)

Copy specific backup
(e.g. end of month/year)

Create full backup recoverable to 12:00pm on <date> (e.g. day 3)

Define retention period for backup (e.g. 7 years)

Schedule ongoing backup copies

- Weekly Full
- Daily Incrementals and Archived logs

Retention defined within Protection Policy

Choice of longer-term storage media:



Object Storage



ZFS Storage



Tape

3rd party media manager

Protection policies define how backup are managed across lifecycle

Controls how long backups are stored by location as well as automatic purging methodology

Protection Policy

Recovery Appliance

Recovery Window for backups stored on Recovery Appliance

Recovery Window Goal

- Automated purging based on available disk space
- Incoming backups take priority over oldest backups within recovery window

Recovery Window Compliance

- Automated purging based only on time
- Ensures backups within the recovery window are never purged
- If there is insufficient space to meet window, incoming backups will be rejected

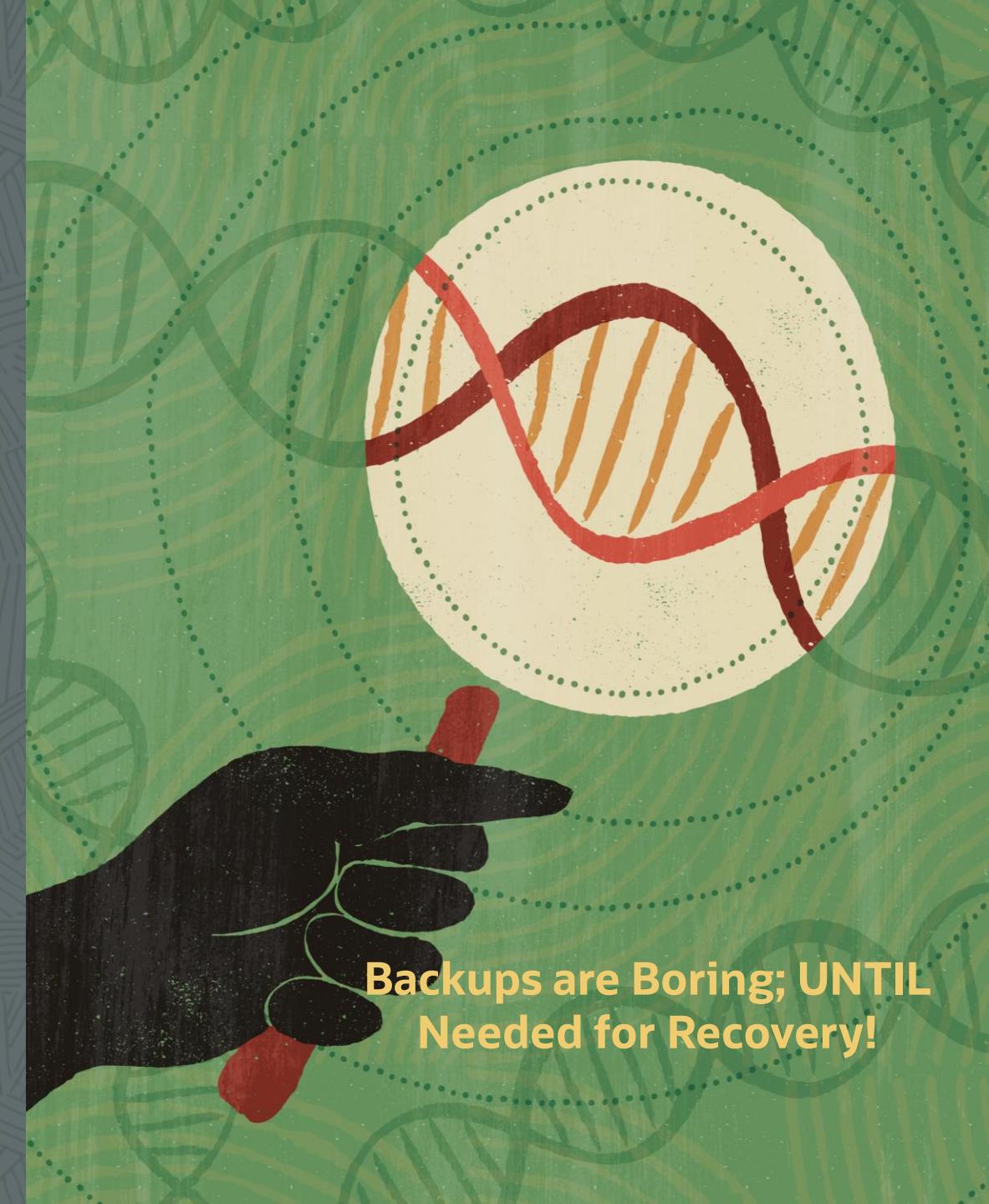
Recovery Window for backup copies on Cloud/ZFS/Tape

- Automated purging based on time
- Recovery Appliance notifies the external storage when backup copies may be deleted

- Protection policies are created on each Recovery Appliance
 - Enables replicated backups to have different backup retention on replica

Questions businesses should confirm; NOT assume

- **What % of backups are validated?**
 - Data-aware validation or storage checksums?
- **What is current data loss exposure?**
 - How do you know?
- **What is point-in-time recovery capability?**
 - How do you know?
- **How quickly can data be restored?**
 - Has this been tested?
- **Is critical data isolated from non-critical data?**

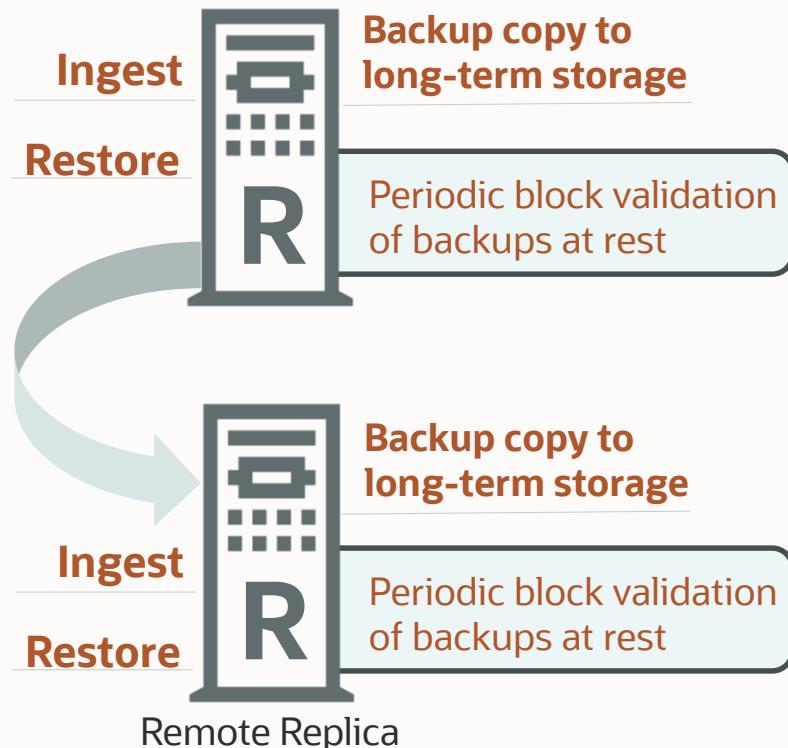


End-to-end data-aware validation

Recovery Appliance is built on a maximum availability architecture (MAA)

End-to-End Block Validation

Data **validated** at every touch point



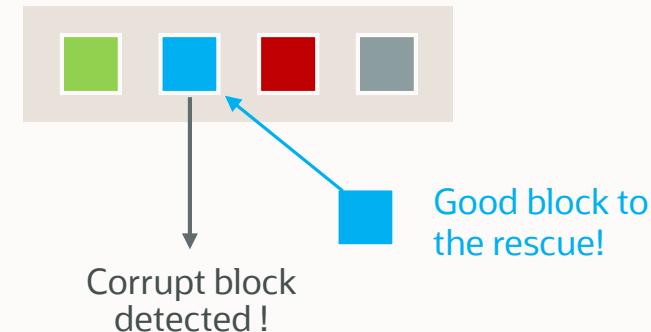
Built-in Redundancy

No single point of failure architecture

- Data is striped and mirrored on Recovery Appliance disk
- Recovery Appliance servers are clustered providing automatic failover—eliminating a single point of failure

Self-Healing Architecture

Automatic block repair from the mirrored copy



Real-time database recoverability status

Recovery Appliance provides extensive recovery monitoring, alerting, and reporting

Real-time recoverability status for all databases at your finger tips:

Target Name	Database Size (GB)	Goal (days)	Recovery Window		Unprotected Data Window	Errors/Warnings	Redo Shipping	Copy-to-Tape	Replication	Last Complete Backup
			Current (days)	Needed Space (GB)	Threshold	Current				
store32	573.0	2.0	6.2	465.4	24.0 hrs	5.7 hrs				Sep 4, 11:12 PM PDT
store33	473.0	2.0	6.4	449.0	24.0 hrs	< 1 sec				Sep 4, 11:16 PM PDT
store34	463.0	2.0	6.4	444.5	24.0 hrs	< 1 sec				Sep 4, 11:19 PM PDT

↑
Current point-in-time-recovery (PITR) window

↑
Current data loss exposure

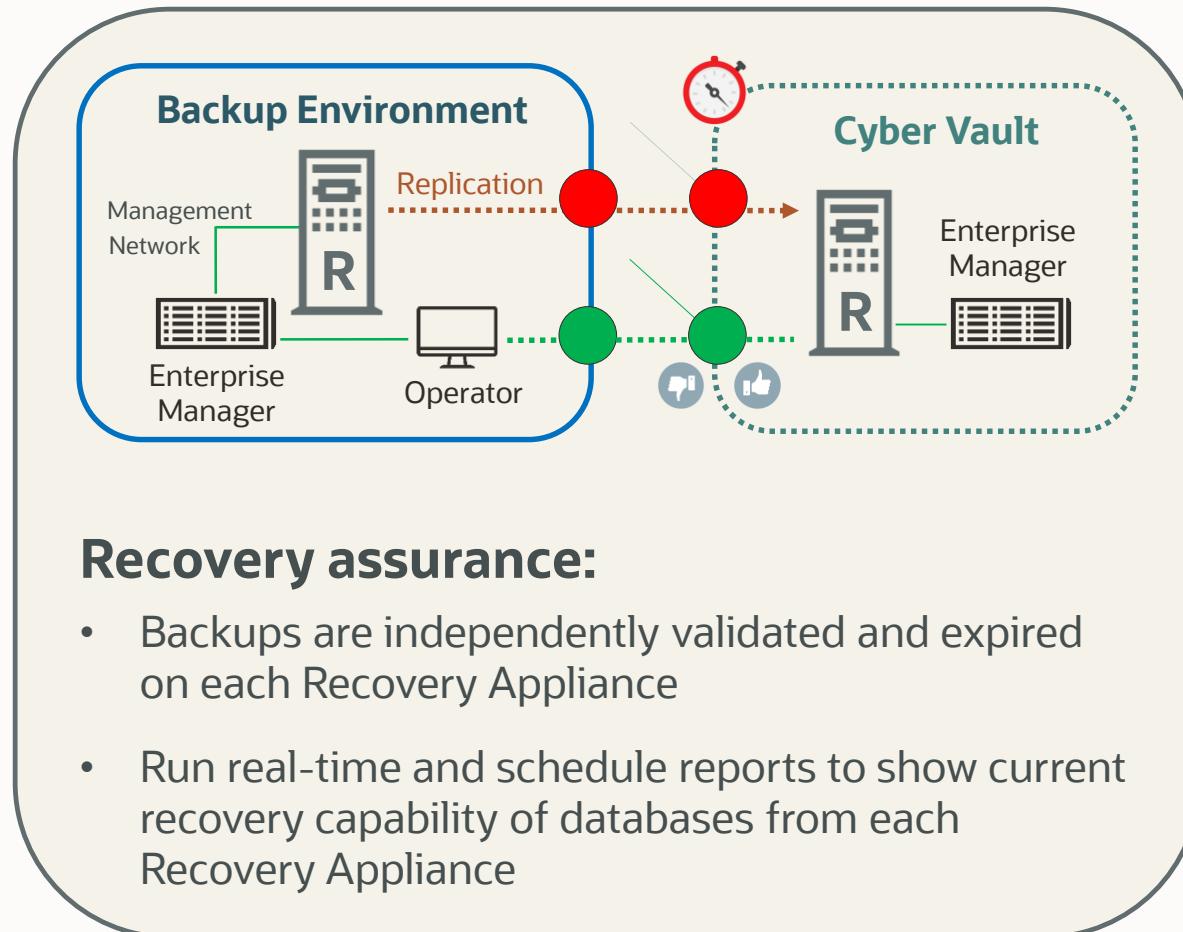


Proactive monitoring and alerting of potential business risks

- Data loss exposure exceeds user-defined threshold
- Recovery Window out of goal
- Capacity usage reaching expected upper limit
- Validation of backups at rest outside of normal schedule

Ransomware protection you can depend upon

Recovery Appliance cyber vault architecture



- Cyber vault access is air-gapped
 - Network access control by operator
- No single user account has access across the architecture
 - Access control is siloed per zone
- Databases are protected in real-time in the backup environment
 - Upon cyber vault opening, the latest immutable backup is automatically replicated

Note: Encrypted databases using TDE have no impact on the backup validation process.

Database recovery is all that Matters

Most backup products and appliance focus on backup not recovery

Traditional Backup Products

Many Backup Silos

Diverse scripts, multiple backup methodologies and overhead

NOT Recovery-Aware

Assume backups can be restored and recovered

90% at Risk

Most companies only test about 10% of backups for validity

Slow Restore Times

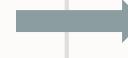
Only promotes and publishes backup performance rates



Recovery Appliance

1 Strategy

Incremental Forever with Full Restore, consistent results with minimal impact



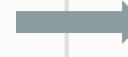
Known Recovery Status

Real-time recovery status, alerts monitoring and reporting for all databases under management



100% Backups Tested

Oracle-aware validation at every touch-point and periodically at rest



Predictable and Fast

Same backup and restore rates, linear performance with scale-out and results published so customers can plan accordingly

Summary



**Zero Data Loss
Recovery Appliance**

oracle.com/zdlra

1

Eliminate Data Loss

- Real time Transaction Protection
- End-to-End Ransomware Protection and Immutability

2

Ensure Database Recoverability

- Continuous Backup Validation
- Database Protection Monitoring

3

Reduces Infrastructure Utilization

- Incremental Forever & Compression
- Eliminate Backup Overhead

4

Resilient Architecture

- Database-integrated Hardware & Software
- Cloud-scale Growth Path

Next steps to data recovery confidence

Your business depends on data, data recovery depends on valid backups

- Test drive the Recovery Appliance
- Learn more about Oracle's Zero Data Loss Recovery Appliance:

<https://oracle.com/recoveryappliance>



What is your data protection strategy?

ORACLE

