ORACLE

Ransomware Protection and Cyber-Resilience with Zero Data Loss Recovery Appliance

Cyber-attacks are one of the top concerns for today's CIOs. They take the form of ransomware attacks, data breaches, and other malicious events that disrupt the availability of business-critical services. The average cost of such attacks was estimated at ~$4.45M in 2023 (Source: CSO). Building a strong data protection and recovery strategy is essential to mitigate the impact of cyber-attacks and minimize service disruptions; in many countries, ransomware protection has also become a regulatory requirement from governing bodies and authorities.

What is Ransomware Protection and Cyber-Resilience Strategy?

A Ransomware Protection and Cyber-Resilience Strategy is a plan on how to mitigate, contain and respond to a cyber-attack to maintain business resiliency. Such a plan requires preparation on two levels: prevention and recovery.

- Prevention aims to reduce the possibility of an attack being successful, covering user training, physical and network access control, application security, data encryption, etc.

- It is also imperative to establish a rapid operational recovery strategy following a cyber-attack incident. This includes immutable local backups, offsite backups, air-gapped copies, and a clean-room setup. This is particularly important for Oracle databases since they manage critical business data for companies worldwide. Just like any IT application requires specific recovery processes, business workloads using the Oracle database also require a process specific to database recovery guidelines.

Why Zero Data Loss Recovery Appliance is Essential for Ransomware Protection and Cyber-Resilience of Databases

Zero Data Loss Recovery Appliance (Recovery Appliance) is an Engineered System designed specifically for maintaining storage-efficient continuously-validated backup copies of the Oracle database, enabling reliable, performant recovery if needed, without data loss. Protecting and recovering an Oracle Database is not the same as protecting generic file system data. A generic file system backup is a collection of independent files that can also be partially restored. Instead, an Oracle Database backup is made of multiple objects that must all be consistent, a single corrupted or inconsistent object may prevent a restored Database from opening. The Recovery Appliance is aware of the data structure and recovery needs of an Oracle database, providing a set of capabilities that are essential to a robust Ransomware Protection and Cyber-Resiliency Strategy.

The Recovery Appliance architecture is natively integrated with, and optimized for, the Oracle database. the Recovery Appliance engine understands the data structure of an Oracle data block, and the complexity involved in restoring and recovering Oracle databases. This sets Recovery Appliance apart from generic backup solutions, which take a lowest common denominator approach towards protecting data, whether the data resides in file systems or databases, and thus fall short of the Recovery Appliance

in terms of protecting Oracle databases. For example, Recovery Appliance uniquely provides the following capabilities:

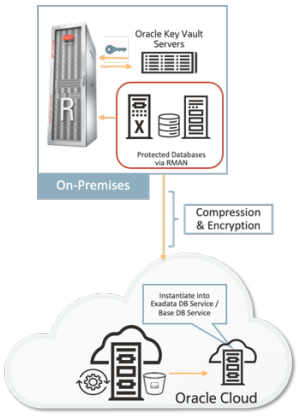
- Detects Oracle block-level anomalies in the backup data stream in real-time to ensure recoverability is not compromised
- Continuously validates on-disk backup data for Oracle block and file consistency anomalies that can disrupt recovery
- Enforces backup immutability, preventing deletion/alteration of backups and retention policies
- Separates duties by role, preventing a single user from being able to both delete/modify active and backup data
- Enables recovery up to the last sub-second before prior to a cyber-attack or other data loss event
- Enables fast restore with space-efficient, **encrypted** virtual full backups created from daily incremental backups
- End-to-End TDE encryption maintained across the complete lifecycle: active on Database, at-rest on Recovery Appliance and on long-term retention storage like OCI Object Storage. Encryption keys always remain with the Database

Recovery Appliance Deployment Architectures for Ransomware Protection and Cyber-Resilience

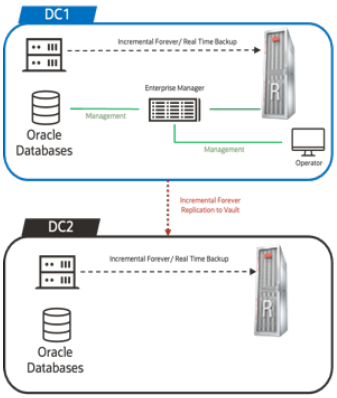
The set of base functionalities described in the previous section is available with every Recovery Appliance. However, the Recovery Appliance architecture enables a flexible deployment model with the possibility to expand the architecture over time as Ransomware Protection and Cyber-Resilience needs evolve, going from a single Recovery Appliance to a pair, with or without a virtually air-gapped offsite backup copy, to a third Recovery Appliance deployed in a physical network-designed air-gapped Cyber Vault. The following sections describe these configurations in further detail.

Ransomware Protection and Cyber-Resilience: Single Recovery Appliance

The previously mentioned Recovery Appliance features protect from cyber-attacks, even with a single appliance. For example, immutability can be enabled on the appliance, protecting backups from any deletion or alteration. Offsite backup copies can be sent to Oracle Cloud Infrastructure (OCI) Object Storage immutable buckets. These backup copies are encrypted and protected from on-premises attacks, supporting restores to OCI or on-premises databases. This architecture offers virtual air-gap protection, as the backups in the buckets cannot be deleted or overwritten while encryption renders them useless if exfiltrated.



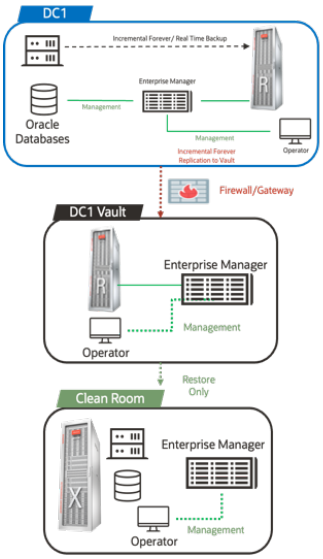
Ransomware Protection and Cyber-Resilience: Recovery Appliance Replication Pair



Using two Recovery Appliances in a replication pair is recommended for Disaster Recovery, but it also enhances protection from cyber-attacks. Immutable backups can be enabled on each appliance, and the separation of duty framework allows for distinct Recovery Appliance administrators to independently manage their respective appliances . A malicious actor fraudulently obtaining the credentials of one Recovery Appliance administrator would not be able to access both systems. The backups are also independently validated on each appliance. For additional protection, backups may be independently archived in OCI immutable buckets. This strategy improves isolation from cyber-attacks, making the deployment even more robust.

Ransomware Protection and Cyber-Resilience: Recovery Appliance Cyber Vault

The Cyber Vault architecture is the recommended solution for creating the most comprehensive data protection strategy that includes a physical air-gapped backup location.
The Recovery Appliance deployed in the Cyber Vault (DC 1 Vault) is not accessible from the corporate network but only from the production appliance (DC1) and only at certain time intervals. Separately, network connectivity into the vault is controlled by a firewall/gateway to create the 'air gap'. Backups from the primary appliance are replicated into the vault as soon as the network opens and leverage an incremental forever strategy, thus minimizing the possibility of intrusion. As with the single appliance, backups are independently validated for recovery in each appliance, so any compromised data on the primary appliance will be detected when it reaches the vault. This vault architecture further isolates management and access control, so no single admin account has access across the configuration.
If a Clean Room environment is available, restores will be performed directly from the Cyber Vault while forensics are performed on the production site (DC1). A Clean Room can reside on a separate site, or simply be a network-restricted environment in the vault location.



Conclusion

The Recovery Appliance provides unique database-integrated features to detect anomalies through block-level validation, establish immutability policies to prevent alteration and deletion of backup, enforce separation of duty among database and appliance administrators, and speed recovery to a transactionally consistent point-in-time prior to an attack. Such database-integrated capabilities are not available in general purpose backup solutions.
Besides the core capabilities, deployment architectures with one or more Recovery Appliances can be chosen based on the level of protection required. From a single appliance configured for immutable backups and archiving to OCI immutable storage, all the way to an air-gapped backup copy in a Cyber Vault location, the Recovery Appliance deployment model remains flexible and can evolve over time as protection needs change.
With a compelling set of database protection features coupled with flexible deployment architectures, Recovery Appliance serves as the foundation for a holistic Ransomware Protection and Cyber-Resilience strategy. Companies with business-critical data in Oracle databases are strongly recommended to evaluate how Recovery Appliance can uniquely and efficiently meet their data protection requirements. Further details can be found at https://www.oracle.com/engineered-systems/zero-data-loss-recovery-appliance.

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle