ORACLE

Defending Oracle Database from Ransomware

How Zero Trust and Oracle Database strengthen ransomware resilience and speed recovery

March 2026, Version 1.0

Public

Purpose statement

This document provides an overview of Oracle Database security features and related products, highlighting how they enable organizations to defend against the evolving threat of ransomware. It aims to help security professionals understand available tools and best practices for preventing, detecting, and recovering from ransomware attacks while ensuring the confidentiality, integrity, and availability of critical data assets. This technical brief is written for CISOs, database administrators, and security architects responsible for Oracle Database environments who need both quick wins and a sustainable path to comprehensive security.

This technical brief provides guidance based on current best practices and Oracle product capabilities as of the publication date. Security threats evolve continuously, and organizations should maintain ongoing assessments of their security posture and recovery capabilities.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

ORACLE

Table of contents

ORACLE

Executive summary

Ransomware is the most immediate cybersecurity threat facing organizations today. Attackers use artificial intelligence and Ransomware-as-a-Service (RaaS) platforms to scale attacks faster and with greater precision. Robust prevention and rapid recovery are essential, particularly for enterprise databases that store critical data assets.

This technical brief presents a phased framework for ransomware resilience. It prioritizes immediate, high-impact defenses before longer-term architectural changes. The core premise is clear: organizations need fast, measurable wins that counter ransomware's two primary tactics (data destruction and data theft) before committing to a full Zero Trust transformation.

Phase 1: Immediate high-impact defense focuses on two critical capabilities that can be deployed quickly and deliver immediate protection:

- **Encryption and key management:** Transparent Data Encryption (TDE) paired with Oracle Key Vault (OKV) renders stolen data unreadable, neutralizing double and triple extortion tactics where attackers threaten to publish exfiltrated data.
- **Immutable recovery infrastructure:** Zero Data Loss Recovery Appliance (ZDLRA) and Oracle Database Zero Data Loss Autonomous Recovery Service (ZRCV) provide synchronized, immutable backups that ransomware cannot destroy, enabling recovery without paying a ransom.

Phase 2: Zero Trust journey represents a sustained and continuous improvement. Zero Trust principles, including configuration monitoring, attack surface minimization, authentication hardening, granular access controls, and activity monitoring, create overlapping defensive layers that reduce both the likelihood and blast radius of a successful attack. These initiatives require ongoing organizational commitment and are best approached as iterative improvements rather than one-time projects.

Deploying Phase 1 encryption and recovery capabilities first gives organizations immediate risk reduction while providing time to execute the Zero Trust transformation.

Understanding the ransomware imperative

Major cybersecurity agencies worldwide, including the European Union's Agency for Cybersecurity (ENISA), the United States' Cybersecurity and Infrastructure Security Agency (CISA), and the United Kingdom's National Cyber Security Centre (NCSC), consistently rate ransomware as the most immediate and disruptive threat organizations face today. Criminal groups leverage ransomware to generate revenue, while state-backed actors increasingly deploy it to cause widespread damage, distract defenders from parallel operations, and funnel funds into economies operating under international sanctions.

Defining ransomware and its evolution

Ransomware is a type of cyber-attack where criminals seize control of your systems or data and demand payment to restore access or to keep stolen information from going public. In many campaigns, attackers encrypt files to block access. Others skip encryption entirely and rely purely on data theft and extortion to compel rapid payment.

The origins of ransomware stretch back decades. The first widely recognized attack surfaced in 1989, when Dr. Joseph Popp distributed malware-infected floppy disks to roughly 20,000 researchers at a World Health Organization AIDS conference. Dubbed the AIDS Trojan, it encrypted files and demanded US$189 for decryption. This predated the dark web; victims sent payments by mail to a post office box in Panama.

Ransomware activity exploded around 2015. Cryptocurrencies such as Bitcoin made ransom payments easier to route and harder to trace, while Ransomware-as-a-Service (RaaS) platforms lowered the barrier to entry, enabling a wider pool of actors to build and distribute ransomware at scale.

Modern campaigns target servers as aggressively as user workstations. Most ransomware variants both encrypt files and exfiltrate them to remote servers. Even if victims pay, there is no guarantee attackers will delete the data or refrain from selling it in underground markets. Payment also offers no assurance of successful file recovery.

AI-powered ransomware attacks

The integration of artificial intelligence into ransomware attacks marks a significant escalation in cyber threats. AI-enhanced reconnaissance tools automatically scan vast amounts of public and leaked data to identify vulnerable systems, map database architectures, and extract credentials in hours rather than weeks. Once inside a network, AI-powered malware adapts to defensive responses in near real time, modifies its own code to evade detection, and optimizes lateral movement toward high-value targets, in one documented case achieving domain dominance on a corporate network in under an hour with no human intervention.

Beyond initial compromise, AI transforms post-breach exploitation: automatically categorizing exfiltrated data, generating tailored extortion notes, and deploying chatbots to negotiate ransoms around the clock. These capabilities allow threat actors to operate with greater speed, precision, and scale across every phase of their campaigns, from crafting convincing phishing emails to executing final-stage encryption.

Organizations should recognize that traditional signature-based defenses and static security rules fall short against AI-augmented threats. This reality makes the pairing of encryption (to guard against data theft) and immutable recovery (to guarantee restoration) even more vital, since these defenses hold firm regardless of how sophisticated the attack becomes.

A two-pronged strategy for database ransomware defense

Organizations need both immediate tactical wins and long-term strategic depth. This technical brief lays out a two-phase approach.

Phase 1: Immediate high-impact defense through encryption and recovery

These are comparatively low-effort, high-impact measures that directly counter the two primary database-level ransomware threats:

- **Data loss through encryption:** Ransomware encrypts data files and renders databases unusable.

- **Data theft for extortion:** Attackers exfiltrate data and threaten public disclosure unless ransom is paid.

Phase 1 solutions neutralize both threats: encryption makes stolen data worthless, and immutable backups can enable recovery without paying ransoms. Organizations can typically deploy these capabilities quickly and deliver immediate, measurable risk reduction.

Phase 2: Zero Trust journey of continuous improvement

Zero Trust represents a sweeping architectural transformation that assumes breaches are inevitable and aims to eliminate implicit trust throughout the environment. While these practices dramatically reduce the likelihood of successful attacks, they demand sustained organizational commitment, cross-functional coordination, and iterative refinement. Most organizations treat Zero Trust as an ongoing program rather than a finite project, steadily improving their security posture over months and years.

The following sections detail both phases, beginning with the immediate, high-impact measures that yield quick wins before turning to the longer term Zero Trust journey.

Phase 1: Immediate high-impact defense

Phase 1 concentrates on deploying two critical defensive capabilities that can be stood up relatively quickly and deliver immediate protection against ransomware's most damaging tactics. By putting encryption and recovery infrastructure at the top of the priority list, organizations neutralize the attacker's primary leverage: the ability to destroy data and extort payment by threatening to leak stolen information.

These measures serve as a final line of defense that substantially improves the likelihood of organizational survival when preventive controls fail. Even if attackers breach perimeter defenses and compromise accounts, properly implemented encryption and recovery capabilities prevent catastrophic data loss and eliminate the incentive to pay ransoms.

Neutralizing data theft and extortion through encryption

Data theft has become a hallmark of modern ransomware. Many campaigns forgo encrypting data altogether. Instead, attackers steal it, show proof, and monetize the theft by threatening public disclosure.

Ransomware gangs employ increasingly inventive data monetization strategies:

- **Simple extortion:** Encrypting data and demanding payment for decryption, without threatening exposure.
- **Double extortion:** Encrypting AND exfiltrating data, then threatening to publish or leak it unless ransom is paid.
- **Triple extortion:** Layering additional pressure tactics on top of encryption and data leak threats; for example, launching DDos attacks, directly contacting customers, employees, or partners or employing "high-pressure publicity," where data subjects are notified to intensify pressure on the victim organization.
- **Traditional sales:** Selling stolen data on the dark web regardless of whether ransom is paid, particularly identity-related information that enables fraud.

These tactics are not theoretical. In November 2023, the ALPHV/BlackCat ransomware group broke new ground by filing a formal complaint with the U.S. Securities and Exchange Commission (SEC) against its own victim, a publicly traded digital lending company. After exfiltrating data without encrypting any systems, ALPHV grew frustrated by the company's refusal to negotiate and reported it to the SEC for allegedly failing to disclose the breach within four business days under the agency's new cybersecurity incident disclosure rules. The group even published screenshots of the SEC complaint form and the acknowledgment it received. Ironically, the rule ALPHV cited had not yet taken effect. The incident nonetheless signaled a troubling new chapter in ransomware pressure

tactics, and security researchers have since observed a rising trend of gangs leveraging regulatory frameworks, including GDPR in Europe, to coerce victims into paying. This "compliance extortion" adds yet another layer of pressure on organizations already grappling with the fallout of a breach.

Transparent Data Encryption: The primary defense

The key to mitigating data theft lies in understanding how ransomware harvests data. Most ransomware mounts "out-of-band" attacks that circumvent database session controls by directly accessing underlying data files on storage or sniffing network traffic. These attacks bypass application-level security entirely.

Transparent Data Encryption (TDE), part of Oracle Advanced Security, is the primary defense against out-of-band attacks. When encryption keys are stored off server and managed via Oracle Key Vault, attackers who steal encrypted database files obtain effectively useless data they cannot decrypt. This neutralizes double and triple extortion tactics. Attackers have nothing of value to leak.

Implementation considerations

- **Data at rest:** TDE encrypts all data stored in database files using AES-256 encryption. This is the default for Oracle AI Database 26ai and is strongly recommended for all production databases.
- **Data in motion:** Data traveling between clients and database servers should be encrypted using either TLS (Transport Layer Security) or Oracle Native Network Encryption (NNE), both of which are included with the Oracle Database license.

Critical requirement: Off-server key management

Caution: Encryption becomes a liability if attackers can access both encrypted data files AND encryption keys during an attack. Storing keys on the same server as the encrypted data creates a critical vulnerability. Attackers can simply delete or corrupt the keys, permanently locking the organization out of its own encrypted data.

The requirement to store encryption keys separately from the data they protect is well established across major regulatory frameworks. NIST Special Publication 800-57, the foundational key management guidance that most regulations defer to, explicitly requires documented key management plans and separation of keys from encrypted data. PCI DSS is among the most prescriptive, directly mandating that keys be stored separately from the data they encrypt. HIPAA, aligned with NIST guidelines, calls for keys to be stored and managed independently from protected health information. Storing keys off-server is not merely a security best practice; for many organizations, it is a compliance obligation.

Oracle Key Vault (OKV) addresses this requirement directly by moving encryption keys off server and managing the complete lifecycle of TDE master encryption keys. OKV provides:

- **Centralized key lifecycle management:** Manages TDE keys for all Oracle Database instances plus encryption keys for backup infrastructure such as ZDLRA, delivering unified key management across the entire data protection ecosystem
- **Compliance support:** Provides audit trails for key access and automated key rotation policies to satisfy requirements under PCI DSS, HIPAA, and other regulatory frameworks
- **SSH Key Management:** Centralizes storage, management, and rotation of SSH keys used for server access, eliminating unmanaged "orphaned" keys that attackers exploit for lateral movement
- **Recovery clean room support:** In ransomware recovery scenarios, OKV can be restored from a known good backup, or keys can be exported and imported into an isolated recovery environment, ensuring data remains decryptable even if the primary data center is compromised.

Future-proofing: Quantum-safe cryptography

As organizations map out their encryption strategies, they must also reckon with emerging threats from quantum computing. "Harvest now, decrypt later" attacks involve adversaries collecting encrypted data today with the

intention of decrypting it once quantum computers gain sufficient power to break current cryptographic algorithms.

Oracle AI Database 26ai addresses this risk by supporting quantum-resistant cryptographic algorithms for both data at rest and in motion. The release integrates NIST-approved post-quantum algorithms including ML-KEM (for key exchange) and ML-DSA (for digital signing) and enables quantum-safe TLS 1.3 to protect all data traffic between clients and database servers.

For organizations safeguarding highly sensitive or long-lived data such as financial records, healthcare information, and government data, implementing quantum-safe cryptography now forestalls future compromise of today's encrypted backups.

Eliminating data loss through immutable recovery

While encryption neutralizes data theft, organizations still face the threat of data destruction. When ransomware encrypts production database files, only two options remain: pay the ransom and hope the decryption key works, or restore from backup. The second option is viable only if backups exist and have not been destroyed by the ransomware.

The problem: ransomware targets backups

Modern ransomware is highly effective at locating and destroying traditional backups. Ransomware developers understand that eliminating recovery options forces victims to pay, so they actively seek out and corrupt backup files, delete backup catalogs, and compromise backup management systems.

Traditional backup architectures sometimes fail for the following reasons:

- **Reachable through standard protocols:** Traditional backup systems rely on well-known protocols such as CIFS/SMB, NFS, and SSH/SFTP that ransomware is engineered to discover and exploit. Any process running with sufficient privileges can enumerate network shares, locate backup repositories, and delete or corrupt files using the same standard interfaces that legitimate backup software depends on.
- **Backups are writable and deletable:** Standard backup files can be deleted by any account with sufficient privileges, including compromised administrator accounts under attacker control.
- **Inconsistent recovery points:** When multiple interconnected databases are backed up at different times, restoring them produces data inconsistencies where transactions appear in one system but are missing from others.
- **Slow recovery:** Traditional restore processes can stretch across days or weeks, leaving business operations paralyzed throughout.

The solution: immutable, synchronized backup architecture

“Immutable backups” are backup files designed to resist deletion, alteration, or corruption, even by compromised administrator accounts wielding high-level privileges. This architectural requirement has become mandatory for ransomware resilience.

Oracle delivers this capability through specialized recovery infrastructure:

- **Zero Data Loss Recovery Appliance (ZDLRA):** An on-premises appliance providing real-time, synchronized database protection with built-in immutable architecture
- **Oracle Database Zero Data Loss Autonomous Recovery Service (ZRCV):** A cloud-native autonomous recovery service in Oracle Cloud Infrastructure with managed immutability and air gap separation options
- **ZFS Storage Appliance:** High-performance storage with immutable snapshots via retention locks, suitable for snapshot-based recovery strategies.

Critical feature: synchronized recovery point objectives

When ransomware strikes multiple interconnected databases, restoring them to different points in time creates "data inconsistency gaps" where some transactions exist in one system but vanish from related systems. The consequences can be severe:

- Broken referential integrity (orphaned foreign keys)
- Financial discrepancies between orders, invoices, and payments
- Weeks or months of painstaking manual reconciliation to track down and repair missing transactions
- Potential regulatory violations if financial records fail to balance.

ZDLRA and ZRCV solve this problem through real-time synchronization. Every committed transaction is captured as part of the transaction itself, ensuring all databases can be restored to precisely the same point in time. This "zero data loss" capability means committed transactions are captured with minimal or no loss and recovery achieves a consistent point-in-time state across interconnected systems.

Infrastructure requirement: recovery clean rooms

Ransomware recovery should be treated as disaster recovery, not merely database recovery. Organizations need dedicated infrastructure to host recovered systems while production environments undergo malware remediation. Traditional hot, warm, and cold site strategies still apply, but cloud providers now offer enhanced options:

- **Secure Enclaves:** Oracle Cloud Infrastructure provides isolated environments separated from production by network air gaps, preventing ransomware from jumping to recovery infrastructure.
- **Recovery Clean Rooms:** Highly isolated environments purpose-built for data and application recovery, designed to bring up a minimally viable IT environment rapidly after an incident.
- **Continuous Incremental Restore:** Cloud environments can execute continuous incremental restores in standby mode, dramatically compressing Recovery Time Objectives (RTO) from days to hours.

Phase 1: Implementation roadmap

Organizations should prioritize these immediate, high-impact actions:

1. **Assess encryption coverage:** Verify that Transparent Data Encryption (TDE) is enabled for all production databases containing sensitive data and identify any gaps that could leave data exposed or unrecoverable in a ransomware attack.
2. **Implement off-server key management:** Deploy OKV and migrate all TDE master encryption keys off database servers to centralized key management.
3. **Validate backup immutability:** Confirm that ZDLRA, ZRCV, or ZFS Storage Appliance are configured with immutable retention locks that prevent backup deletion or tampering by ransomware.
4. **Review recovery point synchronization:** For multi-database applications, ensure ZDLRA or ZRCV provides synchronized, zero data loss recovery points across all interconnected systems.
5. **Test recovery procedures:** Conduct tabletop exercises and actual recovery tests to validate both technical capabilities and organizational readiness. Ensure recovery tests are conducted against isolated non-production environments to prevent inadvertent data loss.

These Phase 1 measures can typically be implemented in weeks to months (depending on organization size) and immediately neutralize ransomware's ability to destroy data or extort payment through data theft. With these foundations in place, organizations can then embark on the longer-term Zero Trust journey with reduced urgency and risk.

Phase 2: The Zero Trust journey

While Phase 1 encryption and recovery capabilities deliver immediate protection, Phase 2 shifts the focus to comprehensive architectural transformation, reducing the likelihood that ransomware ever reaches database servers in the first place. Zero Trust is an ongoing program of continuous improvement rather than a one-time project.

Zero Trust: The foundation for long-term resilience

Zero Trust architecture is rooted in the principle of "never trust, always verify." Rather than relying on perimeter defenses and implicit trust, Zero Trust verifies every request based on identity, device or workload posture, and context—regardless of where the request originates.

Zero Trust assumes breaches will occur and that any account, credential, or system can be compromised. Organizations reduce reliance on any single point of trust by:

- Enforcing strong, phishing-resistant authentication and least-privilege access
- Continuously verifying identity and session risk, not just at login
- Segmenting networks and applications to contain blast radius
- Granting just-in-time, time-bound access to limit standing privileges
- Monitoring events and enforcing policy in real time.

By removing implicit trust and continuously validating each action, organizations limit lateral movement, prevent privilege abuse, and make ransomware campaigns significantly harder to execute.

Typical Zero Trust implementations

Zero Trust touches virtually every corner of IT infrastructure. The US Cybersecurity and Infrastructure Security Agency (CISA) offers a comprehensive model that illustrates this breadth:

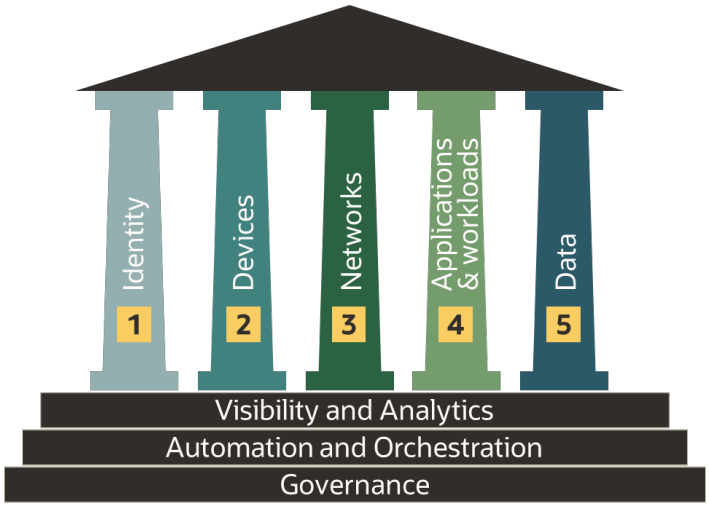

Figure 1-1: CISA Zero Trust Maturity Model Pillars

Common Zero Trust projects that affect database operations include:

- Increased network segmentation enforced by micro-segmentation and more capable firewalls
- Mandates to route administrator connections through bastion hosts or jump servers
- Adoption of Oracle Privileged Account Manager (PAM) for high-privilege operating system accounts like `root` or `oracle` and database accounts like SYS and SYSTEM.

Four core Zero Trust projects for databases

Applying Zero Trust principles to database security can be organized into four major project areas. Each represents an ongoing initiative that organizations continuously refine and strengthen:

Project 1: Configuration assessment and drift monitoring

Zero Trust principle: Never trust that systems remain in their intended secure state; continuously verify configuration compliance.

Databases are complex systems with dozens of parameters that impact security. Misconfigurations rank among the most common entry points for ransomware. Zero Trust demands continuous verification that databases remain properly configured rather than assuming they will stay secure after initial setup.

Implementation approach

1. **Establish security baselines:** Use Oracle Data Safe, Audit Vault and Database Firewall (AVDF), or Database Security Assessment Tool (DBSAT) to conduct initial security assessments and document compliant configurations.
2. **Enable continuous drift detection:** Configure Data Safe or AVDF to automatically flag any deviations from security standards.
3. **Treat changes as potential indicator of compromise:** Investigate every unexpected configuration change as a potential indicator of compromise.

Relevant Oracle utilities, features, services, and products:

- **Data Safe** for security assessment and drift detection
- **AVDF** for security assessment and drift detection
- **Database Security Assessment Tool** for one-time assessment
- Enterprise Manager **Database Lifecycle Management Pack**

Project 2: Attack surface minimization

Zero Trust principle: Assume breach; minimize blast radius through privilege and data reduction.

Most database breaches exploit compromised accounts that attackers simply log in with. Every unnecessary privilege, role, or copy of sensitive data widens the blast radius of a successful compromise.

Implementation approach

1. **Data minimization:**
    - Strip sensitive data from test and development databases using data masking so that breaches of non-production systems yield nothing of value.
    - Implement data subsetting to reduce the volume of data copied to non-production environments.
2. **Privilege minimization:**

- Deploy Database Vault to block even DBAs from accessing application data and enforce Trusted Paths that prevent application accounts from being misused.
- Conduct privilege analysis to identify and remove unused privileges and roles.
- Implement data-driven controls (Virtual Private Database, Real Application Security, Label Security) to restrict what each user can see.

Relevant Oracle utilities, features, services, and products:

- **Data Safe** *Data Masking and User Assessment*
- Enterprise Manager **Data Masking and Subsetting Pack**
- **AVDF** entitlement monitoring/reporting
- Oracle Database ***Privilege Analysis***
- **Database Vault**
- Data-driven controls like ***Virtual Private Database***, ***Real Application Security***, and **Label Security**
- **Database Security Assessment Tool**

Project 3: Authentication strengthening

Zero Trust principle: Never trust passwords or any single authentication factor; verify identity using the strongest available methods.

Authentication is foundational. Every access control ultimately depends on correctly identifying who is making the request. Zero Trust demands a decisive move beyond simple passwords toward multi-factor authentication and strong cryptographic methods.

Implementation approach: Tiered authentication strategy

- **Superuser accounts (e.g., SYSDBA, SYSKM):** Should be protected with PAM and used only when absolutely necessary. SYSDBA is seldom required for routine database administration tasks. Reserve SYSDBA for operations that explicitly require it, such as startup, shutdown and media recovery.
- **Administrator accounts (DBAs, security administrators, application administrators):** Integrate with Active Directory/Entra ID/Oracle IAM and enforce multi-factor authentication if possible. Consider securing these accounts with PAM as well.
- **User accounts (data analysts, developers, testers, business intelligence users):** Require strong authentication (Kerberos, certificates, MFA) for users that connect directly to the database.
- **Application service accounts:** Use the strongest authentication the application supports; implement multi-factor *authorization* via Database Vault or SQL Firewall when strong authentication is not feasible; use Gradual Password Rollover to enable password changes without downtime; monitor logins for unusual patterns.

Note: Starting with Oracle AI Database 26ai and Oracle Database 19c (July 2025 release update), MFA can be enabled for local database accounts using Oracle Mobile Authenticator or Cisco Duo in most configurations, without any client-side changes.

For accounts that continue to rely on passwords, organizations should also audit login activity and watch for indicators of compromise, such as new IP addresses connecting to the database, unfamiliar programs suddenly in use (e.g., AI agents, AI-generated applications), connections at unusual times of day or during non-working hours, or multiple sessions originating from different geographical locations.

Organizations may also want to enforce a trusted path for those password-dependent accounts. This means defining the specific conditions under which they can connect or access sensitive data: restricting access to

approved network paths, client programs, and time windows so that even a compromised password cannot be exploited outside tightly controlled boundaries.

Relevant Oracle utilities, features, services, and products:

- Database ***strong authentication*** (Entra ID OAuth2 tokens, OCI IAM tokens, MFA for local users, Kerberos, certificate, RADIUS)
- Database ***Gradual Password Rollover*** (safely change an application's password without requiring application downtime)
- Database ***Centrally Managed Users*** (Active Directory integration)
- Oracle **RADIUS Adapter** (part of Oracle Access Manager, connects the database to Oracle Access Manager to enable MFA)
- Database ***Unified Audit*** (to audit logins by users authenticated via password)
- **Database Vault** *Trusted Path* (to lockdown accounts with weaker authentication so they can only be used under certain conditions)

Project 4: Comprehensive Database Activity Monitoring

Zero Trust principle: Do not assume preventive controls will catch every malicious action; continuously monitor activity to detect and respond to threats.

Perfect security is unattainable. Some degree of access to data must be permitted. Detective controls identify when someone acts outside the boundaries they should, enabling incident response before damage spreads.

Organizations should deploy a combination of auditing and network-based monitoring to surface anomalies that may signal malicious or unauthorized activity, and to stand ready for incident investigations when they arise. At a minimum, the database's audit trail should capture all data definition and control language activity: if someone creates a new user, grants a role or privilege, replaces a stored procedure, or copies an existing table into a new one, there should be a record. If someone accesses sensitive data from outside an authorized application, there should be a record. And if privileged users are touching data directly, there should most definitely be a record. This visibility is the foundation that makes detective controls actionable rather than theoretical.

Implementation approach

- **Audit security-relevant activities:** Capture all data definition and control language operations (creating users, granting privileges, altering procedures).
- **Monitor sensitive data access:** Log instances when sensitive data is accessed outside normal application flows.
- **Track privileged user activity:** Record all actions by DBAs and other high-privilege accounts.
- **Identify anomalies:** Watch for indicators of compromise—new IP addresses, unusual connection times, unexpected programs (AI agents, AI-generated applications), geographic anomalies.

Relevant Oracle utilities, features, services, and products:

- Database ***Unified Auditing*** (capture security-relevant activity)
- **AVDF's** Database Firewall or SQL Firewall to examine ALL database commands and identify anomalies. SQL Firewall, introduced in Oracle Database 23ai, is natively integrated into Oracle AI Database 26ai.
- **Data Safe** *Activity Auditing* or **AVDF** (audit analysis, reporting, and alerting)

Expanding beyond the core projects

There is always more you can do to secure a system. The four projects above represent essential Zero Trust building blocks, but the work never truly ends. Additional measures worth considering include:

- Implement network micro-segmentation to further isolate database servers
- Implement database blockchain and immutable tables to prevent tampering of custom in-database application logs
- Implement Data Redaction to dynamically mask sensitive fields in query results
- Establish secure application roles that grant privileges only within specific application contexts
- Integrate database security events with enterprise Security Information and Event Management systems.

Keep the scope realistic. Zero Trust is not a quick fix, one-time activity. Most organizations approach it as an ongoing program, continuously iterating and strengthening their security posture over months and years.

Conclusion: A pragmatic path to ransomware resilience

The modern ransomware landscape is evolving rapidly, driven by AI, automation, and increasingly sophisticated criminal tactics. As a result, traditional perimeter-focused security is no longer sufficient to protect critical data, especially in Oracle Database environments that often house an organization's most valuable assets. To meet this reality, organizations need a practical, phased approach that delivers immediate protection while steadily building toward comprehensive resilience. This technical brief outlines a two-phase strategy designed to do exactly that.

Phase 1: Immediate high-impact defense establishes the foundation by neutralizing ransomware's most damaging capabilities:

- **Transparent Data Encryption with Oracle Key Vault** renders stolen data worthless, stripping attackers of leverage from double and triple extortion tactics
- **Immutable recovery infrastructure (ZDLRA/ZRCV)** helps ensure operations can be restored even after catastrophic attacks, with zero data loss and a consistent point-in-time state across interconnected databases.

These capabilities can be deployed in weeks to months and immediately reduce risk. Critically, they empower organizations to follow law enforcement guidance and refuse ransom payments. Attackers gain nothing from destroyed backups or stolen encrypted data.

Phase 2: Zero Trust journey—builds on this foundation with comprehensive security improvements:

- Configuration assessment and continuous drift monitoring
- Attack surface minimization through data masking and privilege reduction
- Authentication strengthening with multi-factor authentication and strong cryptographic methods
- Comprehensive activity monitoring to detect and respond to threats.

Zero Trust projects require sustained organizational commitment and are best approached as ongoing programs of iterative improvement. By implementing Phase 1 first, organizations buy time to execute these transformations while already benefiting from significant protection.

Technology alone is not enough

Effective ransomware resilience demands more than deploying Oracle's security technologies:

- Regular security training for administrators, developers, and end users
- Tested recovery procedures that validate both technical systems and organizational processes
- Incident response plans that define roles, responsibilities, and communication channels

- Ongoing vigilance to adapt to new threats as they emerge

By embracing this phased approach and leveraging the advanced security features of Oracle Database, organizations can achieve measurable risk reduction quickly while building toward comprehensive, long-term resilience. In a threat landscape where breaches should be assumed inevitable, this pragmatic path offers the strongest balance of immediate protection and sustainable security improvement.

Immediate next steps

To equip security and operations teams with practical defensive skills, Oracle provides hands-on resources through Oracle LiveLabs. Of note, take the "Tales from the Dark Side: Hacking the Database" workshop. This practical workshop helps teams understand specific attack vectors that target databases and how Oracle's security features help defend against them.

To begin the ransomware resilience journey, the following immediate actions are recommended:

Phase 1 Quick Wins

- **Audit encryption coverage:** Verify that TDE is enabled for all production databases and that encryption keys are stored in Oracle Key Vault, not on database servers
- **Validate backup immutability:** Confirm that ZDLRA, ZRCV, or ZFS Storage Appliance are configured with retention locks that prevent backup deletion
- **Test recovery procedures:** Conduct actual recovery tests to ensure the team can restore operations under pressure

Begin Phase 2 Planning

- **Establish security baselines:** Deploy Oracle Data Safe to begin configuration assessment and drift monitoring across the database fleet
- **Assess current state:** Use Oracle Data Safe to identify configuration weaknesses and privilege issues that should be addressed in the Zero Trust roadmap.

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