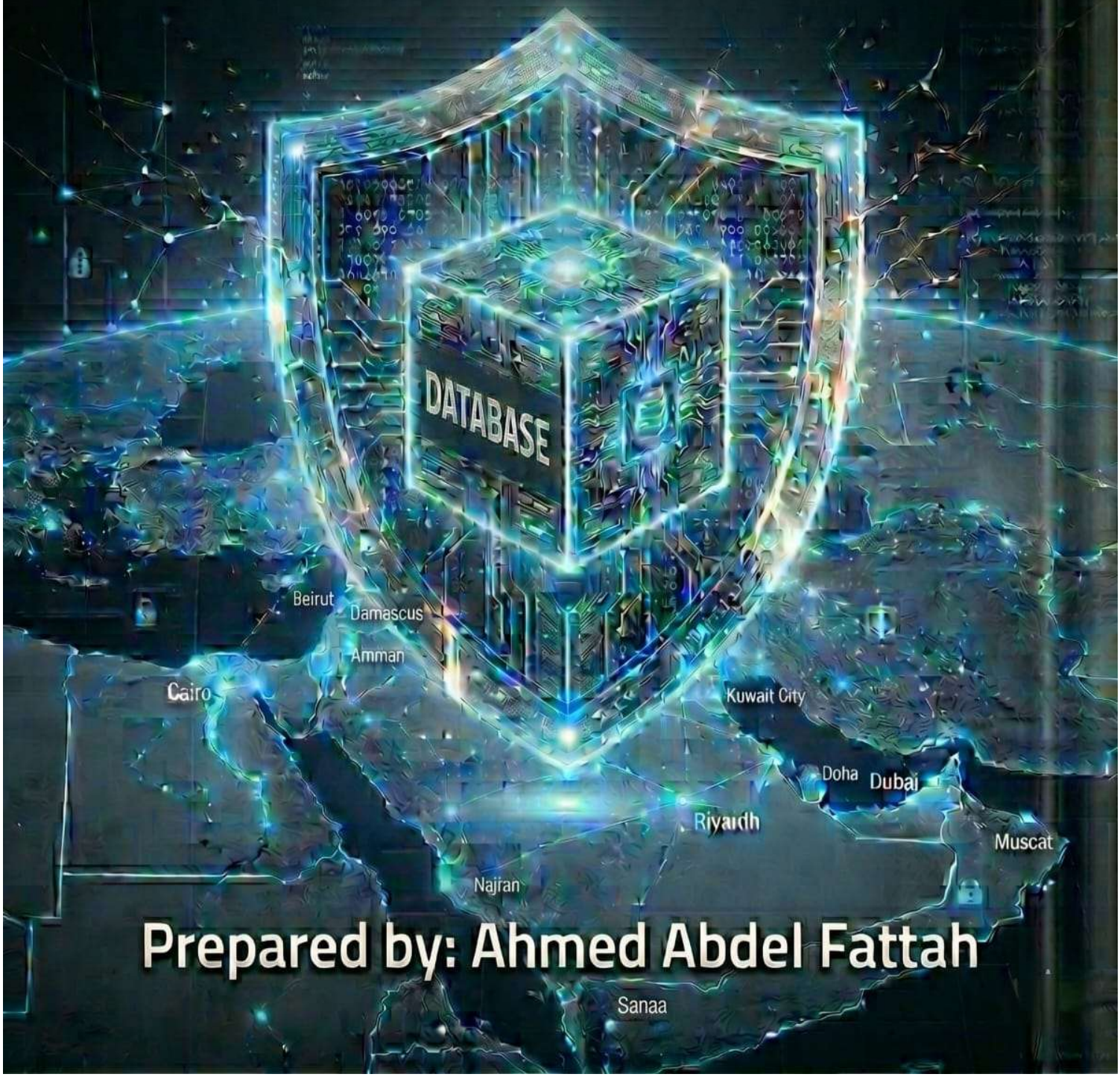
(Oracle Shield)

The Comprehensive Database Security Guide



Prepared by: Ahmed Abdel Fattah

Disclaimer:

The information and scripts contained in this guide are provided 'as is' for educational and guidance purposes. Although every effort has been made to ensure the accuracy of the content, the author accepts no legal liability for any direct or indirect damages that may arise from the use of the scripts in production environments.

It is strongly recommended that all configurations be tested in an isolated test environment before implementation.

Version No.: 1.0

Date: May 2026

For enquiries and consultations **me@ahmedfattah.com**

Official website**https://security.ahmedfattah.com**

Contents

About the Author

Ahmed Abdel Fattah is an Oracle Technology Expert and Oracle ACE, with over 30 years' extensive technical experience across various Oracle products and services. He spent ten years at Oracle, including five years as a Senior Technical Consultant and another five years as Oracle's Technical Consulting and Expert Practice Manager for Egypt and Africa.

Throughout his career, which has spanned the Middle East, Africa and Europe, Ahmed has managed and led numerous complex technical projects. His experience includes implementing cloud environments, migrating databases to Exadata platforms, deploying RAC and Data Guard high-availability solutions, optimizing performance, and designing and implementing data warehouses for major organizations across most countries in the Arab and African regions. He has also worked as an Oracle-certified trainer, delivering certified training courses and bespoke workshops for key clients in the region.

Introduction to the Strategic Guide: Protecting Digital Sovereignty in the Age of Hybrid Cyber Warfare 2026

The complex landscape of cyber threats requires a strategic vision that goes beyond traditional defenses.

We are living in an unprecedented digital reality. Gone are the days when protecting Oracle databases was limited to firewall configurations, routine quarterly updates, and superficial compliance with standards. Amid the accelerating geopolitical shifts in the Middle East and globally, cyberattacks are no longer merely technical possibilities or isolated attempts at self-assertion; they have become strategic weapons targeting the lifeblood of organizations: 'data'.

Oracle Databases serve as the primary repository for the most sensitive data across critical sectors, from banking and energy to defense and government bodies. The latest statistics for 2026 indicate that the average cost of a data breach has reached US$8.64 million, with billions of records exposed to theft or destruction. In this context, relying on default configurations or traditional defenses is akin to leaving the gates of a fortress wide open at the height of a storm.

First: The regional landscape... when data becomes a battlefield

Amid the unprecedented escalation of geopolitical tensions, the rules of the game have changed radically. Networks or endpoints are no longer the ultimate target; rather, it is 'data'. We now live in an environment known as 'Cyber-Kinetic Fusion', where digital attacks are launched in parallel with escalating events on the ground.

When hostile entities and state-sponsored actors declare their intent to target critical infrastructure, they are striking at the "beating heart" of our economies. Oracle databases do not merely run applications; they house financial secrets, government records, and industrial control data for the oil and gas sectors. The fall of a database means the complete paralysis of an organization, and an immediate shift from "business continuity" to "national disaster management".

Today, we are witnessing a terrifying evolution in attack mechanisms; from traditional ransomware to destructive wiper malware. These organized groups are not always seeking a financial ransom; rather, they often aim to completely erase the organization's digital footprint, cleverly targeting the encryption or deletion of data files and backups to cut off any hope of recovery.

Secondly: The gap in official documentation... Why is Oracle's standard documentation insufficient?

One of the most pressing questions that technical leaders might ask is: "Why do we need this specialist guide when Oracle provides thousands of pages of official documentation?"

The new golden rule for 2026 states: "Compliance is the floor, not the ceiling."

The answer lies in the subtle difference between "theoretical lexicon" and "tactical survival plan". Oracle Official Documentation is an excellent encyclopaedical resource, explaining 'how' to run Transparent Data Encryption (TDE) or set up Database Vault, but it suffers from fundamental limitations in real-world environments rife with threats:

1. **Context Neutrality:** Oracle's documentation explains 'how' a feature works, but it does not tell you 'when and why' it should be activated in the face of a cyberattack targeting your technology environment. They assume the presence of a "theoretical attacker" or a curious insider, and do not distinguish between a critical facility facing targeted attacks from hostile actors and a small retail business.

2. **Excessive complexity and distraction:** To fully secure an Oracle environment based on official documentation, your team will need to read and correlate dozens of separate guides (security, network, operating system). This fragmentation creates fatal blind spots during field implementation.

3. **Lack of an integrated systems engineering perspective:** Documentation often focuses on the database as an isolated software entity, ignoring the complex interdependencies in advanced operating environments. Securing the database engine is worthless if the internal network (InfiniBand/RoCE), storage nodes (Cell Nodes) or management systems/network (ILOM) in systems such as Oracle Exadata are compromised

Applying the Zero Trust principle and isolating tasks has become an absolute necessity to protect the 'crown jewels' of organizations.

This is where the true value of this guide lies. It has been designed to **distil** extensive **field experience**, identifying the most critical and impactful measures and translating them into actionable playbooks that are indispensable in times of crisis.

Third: Dissecting Hidden Threats and Weapons of 2026 (Threat Intelligence)

This guide differs radically from any other technical document, as it is fundamentally based on **Threat Intelligence**. We assume that your adversary is an organized group possessing vast resources and advanced technology. By analyzing recent attacks, the guide addresses the following tactics that are not adequately covered by standard documentation:

- **Understanding pre-encryption tactics (Memory Scraping):** The documentation tells you to encrypt data to protect it on disks. But they do not tell you that advanced threat groups have developed malware in modern languages (Rust and Deno)—such as 'RustyWater' and 'Dindoor'—which is injected into live memory to steal data and extract passwords before they reach the encryption stage on the hard drive.
- **Countering Identity Weaponization:** Today's attackers do not breach databases using brute force; instead, they 'log in' as legitimate administrators. We will explain how attempts to break encryption have been abandoned in favour of exploiting zero-day vulnerabilities in identity management systems (such as the critical CVE-2026-21992 vulnerability in Fusion Middleware), and how artificial intelligence is being used to launch MFA Push Bombing attacks to psychologically exhaust users and hack the 'human mind'.

- **Supply Chain and Enterprise Application Breaches:** No database operates in a vacuum. Extortion gangs are now targeting the enterprise application layer. We will demonstrate how vulnerabilities (CVE-2025-61882) in the Oracle E-Business Suite were exploited to lie dormant for weeks and extract terabytes of sensitive data. Worse still, backup devices (such as ZDLRA via the CVE-2026-21977 vulnerability) are being targeted to compromise backup chains and prevent organizations from recovering.

Fourth: What makes this guide different?

This guide is not a theoretical overview, but rather a comprehensive security methodology built on the principles of '**Defense in Depth**' and '**Zero Trust Architecture**'. Its uniqueness and strength are evident in the following areas:

- **A comprehensive approach to complex systems (Full-Stack Security):** We do not merely secure the database engine; we provide a rigorous roadmap for securing the entire infrastructure. The guide offers a rare and exclusive focus on securing engineered systems, through proven strategies for securing storage servers, closing ILOM vulnerabilities, and isolating high-speed interconnect networks.

- **Proactive Compliance:** The recommendations have been formulated to align directly with the requirements of national cybersecurity authorities in the Middle East, as well as the updated CIS standards and DORA guidelines. This saves security teams hundreds of hours of mapping requirements to technical configurations.

- **Secure Migrations:** The most critical periods for security vulnerabilities are during migration and updates. This guide devotes special attention to ensuring that data is not leaked or exposed during complex transfer operations.

- **Bridging the Gap: T**his guide breaks down the barrier between senior management, who speak the language of risk and return on investment (ROI), and technical teams (DBAs & System Admins), who require direct implementation instructions.

Fifth: A Message to Technology Leaders and Data Guardians

To security and executive leaders (CIOs, CISOs):

Investing millions of dollars in advanced Oracle licenses is an investment in performance and reliability, but it loses all its value if these systems become a vulnerability that brings down the organization and inflicts catastrophic losses exceeding millions of dollars, in addition to the legal consequences and risks of compliance fines associated with data breaches. This guide is your 'strategic insurance policy'. It provides you with a clear framework for translating obscure technical discussions into risk-informed decisions, and empowers you to measure your teams' security performance in a tangible and auditable way.

To database administrators and engineers (Senior DBAs & Cloud Architects):

You are the last line of defense. In the event of a real attack, and during the "golden hour" (the first 60 minutes of a breach), randomly searching forums or reading thousands of pages of theory won't help you. You need a tactical tool; a practical guide that puts the right configurations, checklists, and critical, tested hardening scripts at your fingertips.

"Security isn't a product you buy and forget about; it's a continuous, vigilant process that never sleeps. And in the world of Oracle, it's the finer details that make the difference between a resilient organization and one that makes the headlines as the latest victim."

This guide has been created to protect your organization's data and safeguard your career in the darkest of times.

Let's begin the journey to fortify your most valuable digital assets.

Chapter 1: The Strategic Landscape: Geopolitics Meets Data Security (2026)

Understanding the threat is half the battle. Oracle Databases and their associated middleware systems form the vital nerve center of information infrastructure, upon which the energy, finance, government services and defense sectors rely almost entirely for the management of sensitive data and decision-making processes. With the unprecedented military escalation that swept through regions of regional tension in early 2026, cyberspace has become a parallel battlefield no less fierce than operations on the ground. In this chapter, we analyze how geopolitical tensions have impacted the security of technical infrastructure, and how attackers' doctrine has evolved from 'espionage' to 'destruction'.

1.1 Cyber-Kinetic Fusion as a New Reality

In the recent past, regional cyberattacks centered on long-term espionage, isolated sabotage operations, or hacktivism. Today, however, the term **'cyber-kinetic fusion'** has emerged. This concept means that digital attacks are launched in a synchronized and calculated manner to support military and geopolitical objectives on the ground.

In late February and early March 2026, specifically with the launch of large-scale ground military operations, we witnessed a complete integration of kinetic and cyber operations. The intense, reciprocal attacks led to a near-total internet blackout in some targeted areas, with connectivity dropping to just 4% of normal levels. In turn, critical infrastructure in the region faced a massive wave of retaliation unprecedented in its scale and speed.

We are talking today about what is known as **the '0.01% problem'**; when an adversary launches 1.5 million cyberattacks within 72 hours, even defenses operating at 99.99% efficiency will allow breaches capable of destroying entire systems to slip through.

The most dangerous change for database administrators (DBAs) is the shift towards **destructive and wiper malware**. The aim is no longer to hold data for ransom, but to destroy it. Regional Advanced Persistent Threat (APT) groups have used wiper malware variants such as `Shamoon`, `Agonizing` Serpens, `Tickler` and `SHAPESHIFT`. This software targets the Master Boot Record (MBR) and database files for irreversible destruction to cause critical operational paralysis, particularly in the energy (OT/ICS), healthcare and airport sectors. In this scenario, if an Oracle database is compromised, the ultimate goal is to wipe it completely, making over-reliance on network-connected backups a fatal risk.

1.2 The evolution of the threat arsenal: artificial intelligence and secure languages

To understand how to protect Oracle databases, we must first understand the tools used by attackers. Advanced groups have abandoned their traditional tools and carried out large-scale strategic campaigns (such as 'Operation Olalampo'). These groups' tactics have evolved radically and unprecedentedly to bypass the latest generation of antivirus software:

Generative Artificial Intelligence (Offensive GenAI): rather than spending weeks programming and developing bespoke tools, these groups now use large language models (LLMs) to launch precision attacks. Flawless phishing texts are generated, specifically designed to target database administrators, and polymorphic malware is written on the fly to bypass detection systems (Just-in-Time Malware).

To evade detection by endpoint detection and response (EDR) systems, the groups have developed advanced malware (Implants) such as `RustyWater`, written in Rust, and `Dindoor`, built on the Deno environment. The most dangerous feature of this malware is its ability to operate entirely within live memory (Memory

Scraping) and steal data before it reaches the encryption stage, leaving no detectable traces (Fileless) on the hard drive.

Multi-stage backdoors: The use of sophisticated software such as `Fakeset` and `Stagecomp` has been observed; these subsequently download `Darkcomp` malware to lie dormant within the networks of airports, non-profit organizations and banks for extended periods.

C2 Evasion: To exfiltrate data stolen from databases, the groups route malicious traffic through legitimate servers and protocols, such as using the Telegram or relying on complex DNS tunnelling channels, making the data traffic appear entirely normal and making it difficult for firewalls to block it without disrupting operations.

In addition, the role of psychological operations and information warfare has come to the fore, with disruptive groups have hacked into IPTV gateways and media platforms to sway public opinion, and extracted terabytes of sensitive contracts and financial records from leading regional energy companies for the purposes of Doxxing

1.3 The strategy of identity weaponization: breaching the guards rather than the walls

The biggest strategic mistake made by Chief Information Security Officers (CISOs) today is focusing the entire budget on securing the database from the inside through encryption, whilst leaving the 'front door' of identity wide open.

In March 2025, the tech community was shocked by an announcement from a hacker known as 'rose87168' regarding a breach of Oracle Cloud's login servers, granting access to the single sign-on (SSO) systems of a staggering 140,000

tenants. This incident exemplifies the latest and most dangerous tactic: **identity weaponization**.

Today's advanced attacker does not waste time trying to crack Oracle's Transparent Data Encryption (TDE) using brute force, but instead seizes legitimate administrative identities. Once the attacker logs in as a Database Administrator (DBA), all encryption tools become useless, as the database automatically decrypts the data to present it to the user it believes has the necessary authorization. This is achieved through:

MFA Push Bombing / MFA Fatigue: using artificial intelligence algorithms to flood database administrators' phones with continuous authentication requests late at night ( ), to psychologically pressure them—through exhaustion—into approving them, thereby granting the attacker full administrative access.

Exploitation of identity system vulnerabilities: The danger of this tactic lies in the rapid exploitation of critical vulnerabilities, such as the one (CVE-2026-21992) discovered in identity management systems linked to Oracle Identity Manager and Web Services Manager. This vulnerability allows attackers to execute remote code (RCE) without authentication, enabling them to gain complete control over the central identity management system.

1.4 Targeting supply chains and recovery sites as a strategic option

In the context of the hybrid wars of 2026, attackers realize that destroying a database will have no real impact if the organization can restore it from backups within hours. Consequently, the attackers' doctrine has shifted towards **'destruction of the ability to recover'** and compromising **'software supply chains**'.

Compromising major enterprise applications: Advanced threat groups targeted large-scale systems built on Oracle databases, such as the Oracle E-Business Suite, by exploiting a zero-day vulnerability (CVE-2025-61882) through the injection of malicious templates. allowing attackers to lie dormant for weeks and extract vast quantities of financial and procurement records, thereby bypassing the core database engine's security layers.

Backup Annihilation: Direct targeting of sensitive recovery devices, such as (Oracle Zero Data Loss Recovery Appliance – ZDLRA) via vulnerabilities such as (CVE-2026-21977). Through this, attackers aim to access backup data, delete it, or encrypt its keys, to ensure that a subsequent destructive attack (Wiper) will wipe out the organization completely.

1.5 Executive Takeaway

The geopolitics of 2026 have transformed 'corporate data' into critical infrastructure on a par with power stations or desalination plants. For Chief Information Security Officers (CISOs), it is no longer justifiable to view the security of Oracle databases as a purely technical maintenance issue falling under routine IT budgets

The discussion must be elevated immediately to the Board of Directors:

Compliance is **not enough:** failure to secure databases and their environment does not merely mean exposure to non-compliance fines; it means the organization faces irreversible operational and existential paralysis.

Air-gapped backups: Offline backups that cannot be modified or accessed via the normal network must be ensured

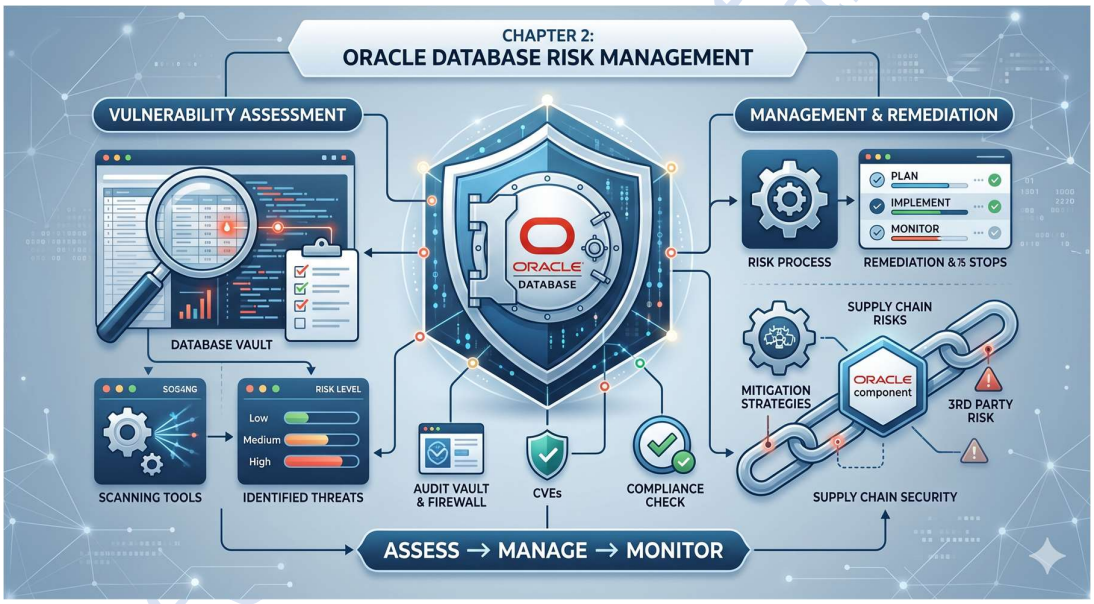
Zero Trust: The mindset that 'our internal network is secure' must be abandoned, and an immediate shift made towards restricting the privileges of system

administrators themselves through technologies such as Oracle Database Vault, and linking this to proactive threat analysis.

This radical shift in security thinking forms the basis upon which the subsequent technical chapters in this guide are built.

Chapter 2: Risk Assessment and Management in an Oracle Environment (Vulnerabilities, Tools, and Supply Chains)

You cannot protect what you do not understand; continuous risk assessment is the first step towards digital sovereignty.



In 2026, vulnerability management is no longer merely a routine task for IT teams to comply with standards; it has become a race against time against advanced persistent threat (APT) groups, which now exploit newly discovered vulnerabilities within just 24 to 48 hours.

In this chapter, we move from theory to a technical dissection of how Oracle databases and applications are targeted, and how to use native Oracle tools to stay one step ahead of attackers.

2.1 Zero-day and critical vulnerabilities: real-world case studies

Advanced threat groups target multiple layers to gain access to Oracle data. Here are the most prominent vulnerabilities currently being exploited and how they work:

First: Identity systems breach (CVE-2026-21992)

Nature of the threat: A critical vulnerability (severity score 9.8) affecting Oracle Identity Manager and Oracle Web Services Manager.

Attack scenario: Here, the attacker does not attempt to break the complex database encryption, but instead targets the 'gatekeeper'. This vulnerability allows the attacker to execute remote code (RCE) over the network without requiring any authentication or a username. Once in control of the identity system, the attacker grants themselves legitimate DBA privileges, rendering all TDE tools useless, as the system will automatically decrypt data for the 'legitimate administrator'.

Second: Infiltration via major enterprise applications – the CL0P and Oracle EBS campaigns

Nature of the threat: Exploitation of zero-day vulnerabilities (such as CVE-2025-61882 and CVE-2025-61884) in the Oracle E-Business Suite (EBS) system.

Attack scenario (how the theft occurred): In August 2025, the attackers began directing malicious requests to a component called `SyncServlet` within EBS servers using the XDO Template Manager feature; they injected malicious templates and then executed them via the "Preview Template" feature. The result? The attackers were able to execute dangerous reconnaissance commands under the privileges of the `` `applmgr` `` application account (such as `` `cat /etc/fstab` `` and opening a reverse connection via `` `/bin/bash -i` ``). The attackers remained in

the system for weeks and extracted terabytes of financial and procurement data without directly compromising the underlying database engine.

Proactive and Immediate Action (Hunting Script):

To verify the integrity of an EBS environment against this type of attack, incident response teams must run periodic queries to search for suspicious templates whose names begin with `TMP` or `DEF`, which are strong indicators of a breach:

```
-- Hunting for potentially malicious templates in the Oracle EBS
environment CL0P campaigns
 -- Warning: Avoid using prohibited aliases and stick to standard names.

SELECT
    t.template_code,
    t.creation_date,
    l.lob_code
FROM
    xdo_templates_b t
JOIN
    xdo_lobs l ON t.template_code = l.lob_code
WHERE
    t.template_code LIKE 'TMP%'
    OR t.template_code LIKE 'DEF%'
ORDER BY
    t.creation_date DESC;
```

Third: Compromising recovery and backup lines (CVE-2026-21977)

Nature of **the threat:** Targeting an Oracle Zero Data Loss Recovery Appliance.

Attack scenario: In wiper attacks, the attacker knows that your backup is your lifeline. The attacker uses the Oracle Net protocol via port 1521 and, by employing social engineering techniques, manages to extract and read the metadata associated with the backups. This reconnaissance paves the way for the destruction of recovery paths before launching the destructive attack.

2.2 Using advanced assessment tools: How do you stay one step ahead of the attacker?

You cannot protect what you do not understand, nor can you patch vulnerabilities you cannot see. Fortunately, Oracle provides two strategic tools that should be part of every DBA and CISO's daily arsenal:

1. **Oracle Security Assessment Tool (DBSAT 4.0): In-depth tactical scan**

   A free and fast tool, consisting of three components (Collector, Reporter and Discoverer). In its latest version (4.0), the tool offers indispensable features:

   CVE Mapping: rather than simply telling you that your updates are out of date, the DBSAT 4.0 report will explicitly state: "Failure to apply this update leaves you vulnerable to CVE-2026-21929", which helps the CISO justify emergency downtime requests to senior management.

   User and Privileged Access Assessment: The tool detects default accounts left with standard passwords (such as the `SCOTT` or (`HR`), for which attackers have ready-made scripts to exploit. It also accurately identifies dormant accounts that have not logged in for a long time (which attackers use as hidden backdoors).

   Data Discovery: The tool scans data dictionaries and tells you precisely: "You have 10 million unencrypted credit card records in table X within schema Y", allowing you to direct your encryption (TDE) budget to the right places.

2. Continuous monitoring using Oracle Data Safe and Drift Detection

A cloud-based tool (also available for on-premises environments), it stands out for its ability to transform assessment from a "one-off snapshot" to "continuous monitoring".

Security Drift feature: Establishes a secure 'baseline' for the database. If a developer grants DBA privileges to a test application account in the middle of the night to make their work easier, Data Safe will trigger an immediate alert for a "security drift", preventing this error from becoming a vulnerability exploited by attackers.

Data Masking: Cloning production databases to development (Dev/Test) environments transfers the full risk. Data Safe provides tools to mask sensitive data with realistic dummy data, so that if the development environment is breached, no real data is leaked.

2.3 Supply Chain & Ecosystem Risks

Advanced threat groups recognize that breaching the firewalls of large enterprises can be costly. Consequently, regional attacks have recently focused intensively on supply chains and service providers with trusted access:

Third-Party Compromise: In a recent extortion campaign (Oracle EBS), hackers used hundreds of compromised accounts belonging to external companies (suppliers and contractors) to send extortion messages to executives at the targeted companies, exploiting the trust placed in these accounts to bypass spam filters

The Fantasy Wiper Case: Advanced groups demonstrated alarming sophistication when they compromised a regional software development

company and used that company's software updates (supply-chain attack) as a Trojan horse to deploy the `Fantasy` wiper—a data-destroying malware—on the developer's clients' systems.

Strategic recommendation: An Oracle database should not trust any connection simply because it originates from a contractor's network or via a technical support VPN. The 'Zero Trust' principle must be applied, multi-factor authentication (MFA) must be enforced, and suppliers' access must be restricted to the 'least privilege' required and only during scheduled maintenance periods.

2.4 Operational Summary for the CISO and DBA

Risk management in 2026 is a race against time.

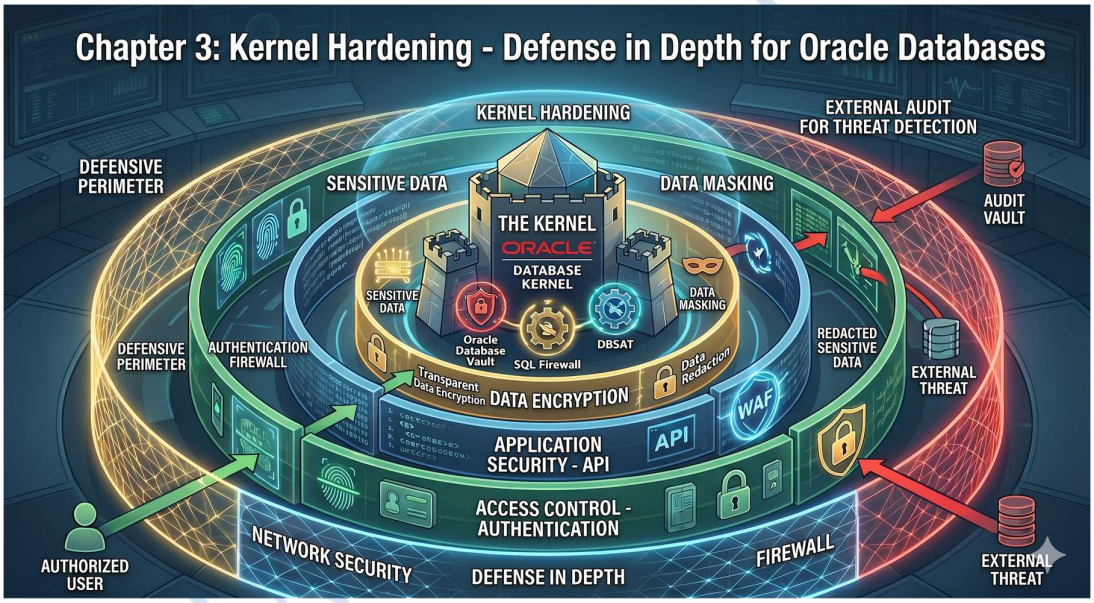
Automate assessments: Data Safe or DBSAT must be run at least monthly. Annual manual reports are a thing of the past.

Emergency Patching: Out-of-cycle security advisories, such as alerts regarding EBS and identity management, require immediate application within hours (SLA), not weeks.

Application Behaviour Monitoring: Attacks via applications (EBS) confirm that securing the database engine must be accompanied by active monitoring of commands coming from friendly applications, which will lead us in the coming chapters to discuss the SQL Firewall feature

Chapter 3: Fortifying the Core – Defense in Depth for Oracle Databases

A sophisticated shield built from AI tools cannot be constructed on fragile foundations; hardening the core is a non-negotiable step.



In light of the advanced threats we are witnessing in 2026, traditional security strategies that rely exclusively on securing the network perimeter have proven to be a resounding failure. Once attackers succeed in breaching the internal network, the database becomes an exposed target.

This chapter sets out a technical and operational roadmap for Chief Information Security Officers (CISOs) and Database Administrators (DBAs) to implement Oracle's Maximum-Security Architecture , transforming the database itself into a fortress capable of defending itself from within even if the external network defenses fall, ranging from encryption and task isolation to the removal of privileged access and the blocking of reconnaissance channels.

3.1 Transparent Data Encryption (TDE) and Data-at-Rest Protection

The first and most important defensive step is to recognize that a breach of the operating system (OS) does not necessarily mean a breach of data. State-sponsored threat groups often exploit OS privileges to copy database files (Datafiles) or backup files and transfer them to their servers.

Intelligence attack scenario: If an attacker manages to gain root access to the operating system, they can simply use basic Linux commands such as `strings` to read the contents of database files with the extension (`.dbf`) in the absence of encryption, passwords, credit card numbers and health data will appear as plain text that can be read and stolen very easily.

Implementation and Mitigation: Transparent Data Encryption (TDE) must be enabled to encrypt the entire tablespaces. When TDE is enabled using advanced encryption algorithms such as AES256, the data within the files is converted into unreadable ciphertext, rendering the stolen files completely worthless to an attacker.

Key management and quantum resistance: Do not store encryption keys on the same server that hosts the database. It is strongly recommended to use external key management solutions such as Oracle Key Vault. Furthermore, to counter 'harvest now, decrypt later' attacks launched by states to store encrypted data pending the development of quantum computers, Oracle has made it possible in the 2026 26ai updates to use quantum-resistant hybrid encryption algorithms such as ML-KEM to secure network communications, adding an indispensable layer of future-proof protection.

3.2 Enable Oracle Database Vault and isolate tasks

The greatest threat to any database is a compromised database administrator (DBA) account. Attackers know that accounts such as `SYS` or `SYSTEM` hold the 'keys to the kingdom', and therefore focus on stealing administrative credentials through phishing or compromising endpoints (Identity Weaponization)

Use of Realms: Database Vault enforces the principle of 'separation of duties'. By creating 'realms', sensitive tables (such as payroll or medical data) can be placed within a secure virtual vault. Even if an account with full administrative privileges (DBA) or SYSDBA is compromised, it will be completely prevented from viewing or modifying sensitive data unless it is explicitly added as an 'Authorized Participant' in that specific realm.

Command Rules to Counter Destruction: The system allows specific commands within the database to be restricted, which is crucial for countering destructive software (Wipers) designed to wipe data. For example, a rule can be created to categorically prevent the execution of `DROP TABLE` or `TRUNCATE` commands at all times, even for authorized users and schema owners, thereby neutralizing the ability of internal or external attackers to destroy the data structure.

3.3 Strict enforcement of the 'least privilege' principle and restriction of general permissions

The most prominent tactic used by attackers today to move laterally within a system relies on exploiting the excessive privileges typically granted to users and applications to facilitate work. The "Principle of Least Privilege" (PoLP) must be strictly applied, so that no user—or even developer—possesses privileges beyond what is strictly necessary to perform their current task.

First: The greatest risk in directly granting system privileges

Many database administrators (DBAs) grant comprehensive privileges such as `DBA`, `SELECT ANY` TABLE, or `GRANT ANY PRIVILEGE` directly to users or application accounts. If this application's credentials fall into the hands of an attacker, they gain complete control of the environment.

All privileges should be managed via dedicated 'roles' rather than being granted directly. In recent versions such as 23c and 26ai, you should make use of **the schema-level privileges** feature Instead of granting a user access to all database tables, a single command allows you to restrict access to the required schema only (e.g. `GRANT SELECT ANY TABLE ON SCHEMA SALES TO SCOTT`), which drastically reduces the attack surface.

Use the following script to immediately detect accounts that possess dangerous system privileges directly (excluding Oracle's default system accounts):

```
-- Detect accounts with direct and excessive administrative privileges
-- Warning: We have adhered to the standard and avoided using
prohibited aliases
SELECT
    sp.grantee AS account_name,
    sp.privilege AS dangerous_privilege,
    sp.admin_option
FROM
    dba_sys_privs sp
JOIN
    dba_users u ON sp.grantee = u.username
WHERE
    u.oracle_maintained = 'N'
    AND sp.privilege IN (
        'DBA',
        'GRANT ANY PRIVILEGE',
        'ALTER ANY SYSTEM',
        'SELECT ANY TABLE',
        'DROP ANY TABLE',
        'CREATE ANY PROCEDURE'
    )
ORDER BY
    sp.grantee;
```

Second: Restricting Public Packages (PUBLIC Grants)

Oracle databases contain powerful built-in packages (such as `UTL_TCP` for network communications, `UTL_FILE` for system files, and `DBMS_CRYPTO` for encryption). Granting EXECUTE privileges on these packages to the PUBLIC group represents a catastrophic vulnerability, as any ordinary user could exploit them to establish reverse connections with attackers' servers (C2) or read sensitive files. These privileges must be immediately revoked from `PUBLIC` and restricted to only those users who require them for actual work.

Third: Important note for developers (DB_DEVELOPER_ROLE)

To avoid granting developers arbitrary privileges, Oracle has recently introduced the `DB_DEVELOPER_ROLE`. Although this is far preferable to granting DBA privileges, caution must be exercised regarding its literal and absolute use in production environments, as it includes privileges that could be exploited for reconnaissance by an advanced attacker. Its use should be restricted exclusively to development and testing (Non-Prod) environments

3.4 Initialization Parameter Hardening

Initialization parameters act as backdoors if not configured correctly, and attackers have repeatedly used them to execute commands at the operating system (OS) level or to bypass audit mechanisms in accordance with CIS Benchmarks

To harden the kernel, the following parameters must be checked and adjusted via: `ALTER SYSTEM`

Prevent unauthorized access to files (UTL_FILE_DIR): This parameter must be left completely blank. Using it allows users (even those without elevated privileges) to read or write files on the server's operating system, which is a classic tactic for planting backdoors.

(In recent versions, this technique has been replaced by the use of strict Directory Objects).

Disable weak remote authentication (REMOTE_OS_AUTHENT):

This must be set to `FALSE`. If set to TRUE, the database will rely entirely on the client's operating system to perform authentication, allowing attackers to easily impersonate administrators simply by spoofing the username on their compromised machines.

Restrict dictionary access (O7_DICTIONARY_ACCESSIBILITY):

This must be set to `FALSE` without compromise. If left set to TRUE, any user with `SELECT ANY TABLE` privileges will be able to read highly sensitive system tables (such as `SYS.USER$`, which contains password hashes), exposing the system to password cracking attacks.

3.5 Securing the network and Oracle Listener

With the evolution of man-in-the-middle (MITM) tactics and memory scraping software, encrypting data in transit has become just as important as encrypting data at rest

Enforce Native Network Encryption (NNE) or TLS 1.3:

No unencrypted (clear-text) connections should be permitted between applications and the database (via the default port 1521). Whether you use NNE via `sqlnet.ora` settings or rely on TLS certificates, encryption must be enforced as 'REQUIRED' rather than 'ACCEPTED'. This thwarts attempts by intelligence groups to intercept credentials passing through the network.

Protection against Listener Poisoning and VNCR

The listener is the first gateway. A skilled attacker will attempt to register a fake service with the listener to divert legitimate traffic to their rogue servers.

To thwart this, Valid Node Checking for Registration (VNCR) must be enabled in the `listener.ora` file. This feature ensures that the listener will reject any request to register a new database service unless it originates from specific, pre-trusted IP addresses (such as legitimate database servers only).

3.6 Eliminating Local Passwords and Integrating Identity (Identity Weaponization Defense)

As advanced attack groups rely heavily on identity weaponization attacks (such as authentication bypass and session hijacking), organizations must immediately cease managing database accounts independently and locally. To fend off automated attacks and MFA fatigue attacks, the following must be implemented:

- **Centrally Managed Users (CMU):**

Oracle databases must be linked to centralized enterprise identity systems such as Microsoft Active Directory or Azure AD. This integration ensures that no 'dormant' accounts in the database after employees leave the company, whilst also enabling the centralized and strict enforcement of phishing-resistant multi-factor authentication (MFA) policies before allowing any connection to access the network or database.

- **User Profiles:**

As a last line of defense in the event that centralized systems fail, database profiles must be configured to respond to attacks:

Strict Limitation of Login Attempts (`FAILED_LOGIN_ATTEMPTS`): Reducing the number of permitted failed attempts (to a maximum of 3 or 5) stops brute-force attacks within seconds.

Password verification functions: Link all profiles to a PL/SQL function that enforces high password complexity and prevents the reuse of passwords listed in global threat lists.

3.7 Operational Summary for the DBA

Hardening the kernel is not a one-off project, but an ongoing 'operational state'.

1. Enable Transparent Data Encryption (TDE) and Database Vault to protect data even in the event of an operating system failure.
2. Immediately revoke direct superuser privileges and replace them with restricted roles, and restrict the `PUBLIC` package
3. Disable obsolete and dangerous configuration parameters.
4. Enforce network-level encryption, restrict the Listener with strict white-lists, and move to centralized identity management.

Once these solid foundations are in place, we can confidently move on to the next chapter to implement 'proactive monitoring and intelligent auditing' to detect the attacker before they strike.