

# Introduction to Secure Databases

## Introduction to Secure Databases

Key concepts, goals, and best-practice building blocks

---

## 1. Why Database Security Matters

| Reason                | Impact if Ignored                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------|
| Confidentiality       | Sensitive data (PII, financials, health records) can be exposed ? legal penalties, loss of trust |
| Integrity             | Unauthorized changes corrupt data ? faulty business decisions, compliance failures               |
| Availability          | Downtime or data loss disrupts operations ? revenue loss, reputational damage                    |
| Regulatory compliance | GDPR, HIPAA, PCI-DSS, etc. require specific safeguards; non-compliance = fines                   |

---

## 2. Core Security Objectives (CIA Triad)

- Confidentiality** – Ensure only authorized subjects can read data.
  - Integrity** – Detect and prevent unauthorized modification.
  - Availability** – Keep data accessible to legitimate users when needed.
- 

## 3. Threat Landscape Overview

| Threat               | Typical Vector                    | Example Mitigation                              |
|----------------------|-----------------------------------|-------------------------------------------------|
| SQL Injection        | Unsanitized input in queries      | Use prepared statements / parameterized queries |
| Privilege Escalation | Over-granted roles                | Principle of least privilege (PoLP)             |
| Insider Abuse        | Legitimate credentials misused    | Activity monitoring, separation of duties       |
| Data Exfiltration    | Unencrypted backups, export tools | Encryption at rest & in transit, DLP controls   |

# Introduction to Secure Databases

| Threat                  | Typical Vector             | Example Mitigation                                   |
|-------------------------|----------------------------|------------------------------------------------------|
| Ransomware              | Compromised admin accounts | Immutable backups, multi-factor authentication (MFA) |
| Denial of Service (DoS) | Flooding DB connections    | Connection throttling, rate limiting, load balancing |

---

## 4. Security Controls – Layered Approach

### 4.1 Physical & Infrastructure

- Secure data center access (badge, biometric)
- Hardened OS, patched firmware
- Network segmentation (DMZ, private subnets)

### 4.2 Network Security

- **Firewalls** – whitelist only required IP/port combos (e.g., 3306 for MySQL)
- **VPN / TLS** – encrypt traffic between client and DB server
- **Zero-Trust networking** – micro-segmentation, mutual TLS

### 4.3 Authentication & Authorization

- **Strong authentication** – MFA, LDAP/AD integration, Kerberos, OAuth
- **Role-Based Access Control (RBAC)** – assign minimal permissions per role
- **Attribute-Based Access Control (ABAC)** – fine-grained policies based on user, data, context
- **Password policies** – length, complexity, rotation, storage with salted hash

### 4.4 Encryption

| Scope           | Technique                                         | When to Apply                 |
|-----------------|---------------------------------------------------|-------------------------------|
| Data in transit | TLS/SSL (e.g., <code>require_ssl</code> in MySQL) | All client-server connections |

# Introduction to Secure Databases

| Scope                    | Technique                                                                                            | When to Apply                                   |
|--------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| <b>Data at rest</b>      | Transparent Data Encryption (TDE), column-level encryption, file/system encryption (LUKS, BitLocker) | Sensitive tables/columns, entire database files |
| <b>Backup encryption</b> | GPG, cloud KMS-managed keys                                                                          | Before storing off-site or in the cloud         |

## 4.5 Auditing & Monitoring

- **Database activity monitoring (DAM)** – capture query logs, privilege changes
- **Immutable audit trails** – write-once storage, signed logs
- **Alerting** – anomalous query patterns, failed logins, privilege escalations
- **Integration** – SIEM (Splunk, Elastic, Azure Sentinel) for correlation