

Database Activity Monitoring (DAM)

Complete Visibility, Continuous Compliance, and Real-Time Threat Detection for Databases



Core Monitoring Capabilities



Security & Compliance



Analytics & Detection



Integration & Deployment

Our **Database Activity Monitoring (DAM)** solution delivers **real-time, tamper-proof visibility** into all database activities across on-premises, cloud, and air-gapped environments. Designed to meet **India-specific regulatory requirements** and global compliance standards, the platform provides deep **SQL inspection, privileged user monitoring, behavioural analytics, and forensic-ready logging** to protect sensitive data such as Aadhaar, PAN, PII, and PCI information.

Get In Touch

To secure your financial ecosystem!

1. Core Monitoring Capabilities

1.1. SQL Activity Monitoring

- Full capture of all SQL operations: **SELECT, INSERT, UPDATE, DELETE**
- Query reconstruction and normalization for accurate analysis
- **Application user + database user correlation**
- Complete session context: **IP address, hostname, session ID, timestamps**
- Automatic detection of sensitive-field access (Aadhaar, PAN, PII, PCI, etc.)
- Deep visibility into **stored procedures, triggers, and functions**

1.2 Real-Time Event Streaming

- **Sub-second** database event capture
- **Real-time rule-based and behaviour-based alerts**
- **Publish / Subscribe** integration for SIEM and SOC platforms

1.3 Privileged User Monitoring

- Detailed tracking of DBA and superuser activities
- Monitoring of sudo, root, and system-level privilege escalations
- Alerts for schema changes, privilege grants, user creation/deletion
- Detection of backdoor or dormant privileged account usage



2. Security & Compliance

2.1 Log Integrity & Protection

- **Immutable, append-only** audit logs
- **Cryptographic digital signing** of logs
- Secure hashing using **SHA-256 / SHA-3**
- **WORM storage** support for regulatory compliance
- Real-time alerts on audit or schema tampering attempts



2.2 Compliance Standards Supported

- UIDAI Aadhaar Data Vault & Security Guidelines
- RBI Cyber Security Framework
- CERT-In log retention and monitoring mandates
- ISO/IEC 27001 – Annex A controls
- PCI DSS (database logging & monitoring requirements)
- SOC 2 Type II alignment

2.3 Forensic-Ready Logging

- Rich, correlation-ready metadata
- Storage of **raw SQL and normalized SQL**
- **Incident replay** for investigations and audits

3. Analytics & Detection

3.1 Behaviour Analytics

- Baseline modelling for users, applications, and query behaviour
- Anomaly detection based on volume, frequency, and time-of-day
- Detection of lateral movement across databases.
- Identification of data exfiltration patterns

3.2 Rule-Based Detection Engine

- Pre-loaded rules for Aadhaar and sensitive-data misuse
- Flexible custom rule builder (AND / OR logic)
- Threshold-based monitoring (row count, query rate, access bursts)
- Alert severity classification: Low, Medium, High, Critical

4. Integration Capabilities

Integration Category	Platforms
SIEM	Splunk, IBM QRadar, ArcSight, LogRhythm, ELK / OpenSearch & Microsoft Sentinel.
HSM	JISA HSM (CryptoBind HSM), Thales Luna, Entrust nShield, SafeNet & any PKCS#11 compliant HSM.
Data Vault & KMS	JISA Aadhaar Vault, Third-party Aadhaar vaults Tokenization engines & Enterprise Key Management Systems (KMS).

5. Architecture & Deployment

5.1 Deployment Models

- On-premises
- Private cloud (VM-based)
- Government cloud
- Air-gapped and offline SOC environments

5.2 Platform Components

- Lightweight database agents
- Centralized DAM server
- Analytics & Correlation engine
- Web-based dashboards & reporting
- Secure log storage with SIEM forwarding

5.3 Supported Databases



6. Dashboards & Reporting

6.1 Dashboard Features

- Real-time database activity stream
- Top users, objects, and tables accessed
- Privileged user activity heatmap
- Aadhaar access tracking dashboard

6.2 Reporting

- UIDAI compliance, DBA activity, and privileged access reports
- Suspicious query and anomaly detection reports
- Schema change and configuration alerts
- Custom report builder with PDF, CSV, and JSON export

7. Security Features

- End-to-end TLS 1.2 / 1.3 encryption
- Role-Based Access Control (RBAC)
- Multi-Factor Authentication (MFA)
- IP whitelisting and zero-trust architecture principles
- API keys with automated rotation
- AES-256 encrypted log storage

8. Maintenance & Management

- Centralized agent lifecycle management
- Continuous health monitoring: CPU, memory, disk, event lag
- Syslog and JSON export
- REST and gRPC APIs for automation and orchestration

9. Optional Add-Ons

- UEBA (User & Entity Behavior Analytics)
- Threat intelligence correlation
- Data masking module
- Cloud-native DAM (roadmap)
- ML-based anomaly scoring

10. Memory Analysis

- Monitoring of memory usage by database engine, query cache, and system tables.
- Detection of suspicious or abnormal memory access patterns.

11. Network Monitoring

- Database-aware packet inspection
- Inbound and outbound traffic analysis
- Source IP visibility and anomaly detection

Key Value Proposition

One platform. Complete database visibility. Continuous compliance. Zero blind spots.

Built for regulated industries, government systems, BFSI, and Aadhaar ecosystems, the DAM solution ensures real-time threat detection, audit readiness, and data protection by design.

Get In Touch

To secure your financial ecosystem!

+91 9619-222-553

connect@jisasoftech.com | sales@jisasoftech.com

A-604, Amar Business Zone, Veerbhadra Nagar, Ganraj Chowk, Baner, Pune,
Maharashtra, 411045, India.



Scan to Save Contact