Database Security & Compliance Transformation for a Regulated Money Exchange Enterprise

IBM Guardium-based database activity monitoring, PCI reporting, vulnerability management and managed support.

Executive Summary

COMnet helped a regulated money exchange enterprise strengthen database security and compliance by deploying IBM Guardium agents for 50 databases, building DC/DR collectors and central management, enabling PCI reporting, vulnerability scans and S1/S2/S3 managed support.

50	3	DC + DR	PCI	24x7
Databases protected	Database platforms	Guardium deployment	Compliance reporting	S2/S3 remote support

IMPACT

Business and Compliance Impact

- Established database activity monitoring across Oracle, PostgreSQL and Microsoft SQL platforms in a regulated money exchange environment.
- Deployed IBM Guardium agents for 50 databases with Central Manager and Collector architecture across DC and DR.
- Improved PCI-aligned compliance evidence through controlled policies, activity trails and reporting workflows.

Security Operations Impact

- Enabled vulnerability manageability for databases through scheduled scans, findings visibility and remediation tracking.
- Created a managed support model with 24x7 remote support for S2/S3 incidents and onsite escalation for S1 severity.

MAJOR ISSUES

Visibility Across Databases

- Database activity was business-critical but required stronger visibility across heterogeneous database platforms.

PCI Reporting Pressure

- Compliance and reporting needed repeatable, evidence-ready controls aligned to PCI obligations and audit cycles.

Database Vulnerability Risk

- Vulnerability manageability for databases required structured scanning, prioritization and remediation governance.

DC/DR Resiliency Need

- The environment needed DC/DR deployment resiliency with centralized administration and consistent security policy enforcement.

Severity-Based Support

- Severity-based support expectations required accountable remote operations and onsite intervention for critical incidents.

HIGHLIGHTS

COMnet converted the original business requirement into a controlled database security program covering agent deployment, centralized Guardium administration, compliance reporting, vulnerability scanning and operational support.

Solution Delivered

- IBM Guardium agent installation for 50 databases covering Oracle, PostgreSQL and Microsoft SQL workloads.
- Deployment of Central Manager and Collector components in DC and DR setup for resilient administration and event collection.

Controls Enabled

- Data security policies configured as per industry standards to monitor privileged access, sensitive activity and policy exceptions.
- Database vulnerability scans executed to identify risk exposure and improve remediation visibility.

Support and Assurance

- Compliance reporting enabled for PCI-driven control evidence and database security governance.
- 24x7 remote support for S2/S3 severity incidents and onsite engineer visits for S1 severity events.

Use Cases Addressed

- Database Activity Monitoring (DAM) for regulated financial data stores.
- PCI compliance reporting, audit support and policy evidence generation.
- Database vulnerability management across Oracle, PostgreSQL and Microsoft SQL.
- Centralized Guardium administration across DC/DR security architecture.
- Severity-based managed support model for database security operations.

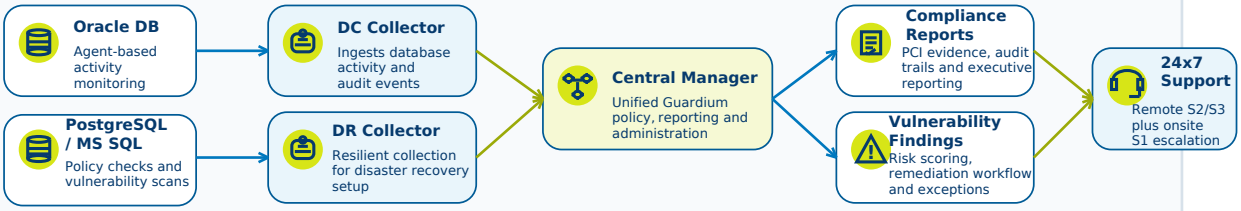
Core Technical Outcomes

- Controlled monitoring for privileged and sensitive database activity.
- Centralized policy and reporting using Guardium Central Manager.
- Vulnerability management inputs for database remediation governance.
- Operational continuity through remote and onsite severity-based support.

ARCHITECTURE AND DEPLOYMENT SCOPE

Reference Architecture - Database Activity Monitoring, Compliance and Vulnerability Management

IBM Guardium agents, collectors and central manager deployed across DC/DR with policy-based monitoring and managed support.



Design principles: DC/DR resilience | Agent-based visibility | PCI reporting | Vulnerability workflow | Managed escalation

Scope Area	Deployment / Technical Scope	Business or Security Outcome
Database Estate	Oracle, PostgreSQL and Microsoft SQL databases monitored through Guardium agents across 50 databases.	Cross-platform visibility for regulated transaction and customer data stores.
Collection Layer	Collectors deployed in DC and DR setup for database activity ingestion and monitoring continuity.	Resilient collection and reduced single-point operational dependency.
Central Management	IBM Guardium Central Manager used for policy administration, reporting and enterprise oversight.	Consistent policy enforcement and centralized governance.
Policy and Reporting	Data security policies configured per industry standards with PCI-aligned reporting outputs.	Audit-ready evidence, exception tracking and improved compliance posture.
Vulnerability Management	Database vulnerability scans executed and findings routed into remediation workflow.	Improved risk visibility, prioritization and remediation accountability.
Managed Support	24x7 remote support for S2/S3 and onsite engineer visits for S1 severity events.	Faster escalation, service continuity and support predictability.

KEY STRATEGIES

The engagement should be positioned as a database security and compliance modernization program, not only a tool deployment. The strategies below make the model suitable for CEOs, CISOs, audit leaders and cybersecurity experts evaluating measurable risk reduction.

Policy-First DAM

- Design activity monitoring policies around privileged users, sensitive objects, anomalous behavior and business-critical database activity.

PCI Evidence Readiness

- Map controls to audit evidence requirements so reporting can be produced consistently during audit and review cycles.

DC/DR Resilience

- Place collectors and central management in a resilient deployment model to sustain monitoring and administration during service events.

Risk-Based Vulnerability Workflow

- Prioritize database vulnerabilities by criticality, exposure, business process dependency and compensating controls.

Agent Rollout Governance

- Plan installation windows, compatibility checks, validation steps and rollback procedures to reduce impact on production databases.

Severity-Based Operations

- Use S1/S2/S3 response model with 24x7 remote support and onsite intervention for critical incident handling.

Centralized Reporting

- Standardize dashboards, reports, exception workflows and stakeholder cadence for IT, audit and security leadership.

Continuous Optimization

- Tune policies, reduce noise, refine scan schedules and update controls as the threat, audit and database landscape changes.

GOVERNANCE AND OPERATING MODEL

Governance Area	Operating Criteria
Control Ownership	Define owners for database policies, reports, scan cadence, exceptions and remediation actions.
SLA / Severity Model	Maintain S1 onsite escalation with 24x7 remote support for S2/S3 events and transparent escalation paths.
Audit Cadence	Run periodic PCI evidence reports, review exceptions and maintain traceability for audit cycles.
Optimization Loop	Tune DAM policies, scan schedules, thresholds and alert volumes to reduce noise and improve detection value.

Technical stack: IBM Guardium Central Manager and Collectors, database agents, Oracle, PostgreSQL, Microsoft SQL, PCI-aligned reports, vulnerability scans, S1/S2/S3 support workflow.

Executive Takeaway
COMnet delivered a database security control layer that improved visibility, compliance evidence, vulnerability manageability and operational support for a regulated money exchange enterprise. The model combines IBM Guardium architecture, PCI-aligned governance and managed severity-based operations.