DATASHEET

ARGUS Database Security

Simplify data compliance and stop breaches

Today's digital economy is driving exponential data growth across financial institutions, government agencies, and enterprises. To protect your data and business, you need compliance and security solutions that take a data-centric approach.

ARGUS Database Security helps organizations unleash the power of their data by reducing the risk of non-compliance or a security breach incident.

A better way to manage data risk

The complexity of achieving compliant and secure data is daunting for large enterprise organizations. Rapid platform change and scarce security resources make it almost impossible to keep up on your own.

ARGUS provides an automated solution to streamline compliance processes and help security staff pinpoint data risk before it becomes a serious event.

ARGUS standardizes audit and security controls across large and complex enterprise database environments, mitigating risks to sensitive data on-premises, in the cloud, and across multiple clouds. Supporting 11 database platforms including Oracle, MySQL, PostgreSQL, SQL Server, MongoDB, and more.

ARGUS ML-powered analytics help limited security staff be more effective at detecting risky or suspicious behavior by eliminating false positives. Our UEBA engine uses LSTM neural networks and Autoencoder models for advanced anomaly detection.

KEY FEATURES AND BENEFITS

- Detect and prioritize data threats using ML, UEBA and behavior analytics
- Pinpoint risky data access activity – for all users including privileged users
- Gain visibility by monitoring and auditing all database activity
- Protect data with real-time alerting or blocking of policy violations
- Uncover hidden risks with data discovery, classification and 5-source vulnerability intelligence
- Reduce the attack surface with 7+ data masking algorithms
- Deploy in 1-2 days vs 3-6 months with competitors
- **Save 60-85% vs IBM Guardium and Imperva**

Gain visibility and fix vulnerabilities

Many organizations don't actually know where all of their sensitive data is and whether it's exposed. Such blind spots create security risks that lead to careless mistakes, or create opportunities that attackers can exploit, often through hidden vulnerabilities or misconfigured databases.

ARGUS Database Security helps organizations reduce non-compliance and breach risk by locating sensitive data and identifying the vulnerabilities that could lead to data compromise.

ARGUS Database Security automatically discovers databases on the network and in the cloud. In the process, it can automatically identify and classify sensitive data, using dictionary and pattern-matching methods for PII, PHI, PCI and financial data.

ARGUS vulnerability assessment capabilities scan your databases using 5-source intelligence: NVD (National Vulnerability Database), CISA KEV (Known Exploited Vulnerabilities), EPSS (Exploit Prediction Scoring), MITRE ATT&CK framework, and Microsoft Security Response Center (MSRC).

Make staff more effective with actionable insights

ARGUS Database Security incorporates advanced Data Risk Analytics that correlate user data access activity over time across all database servers. Our ML-powered UEBA engine builds behavioral baselines and detects anomalies using Isolation Forest, LSTM neural networks, and Autoencoder models.

Figure 1: Real-time security monitoring dashboard with ML-powered threat detection

Protect in real-time

ARGUS Database Security enforces compliance and security policy across heterogeneous data environments. With 296 pre-built policy rules across 21 compliance frameworks including PCI-DSS, SOX, GDPR, HIPAA, ISO 27001, NIST 800-53, Bangladesh Bank ICT Guidelines, and Defense Security requirements.

As a data-centric solution, ARGUS Database Security includes an integrated database firewall that creates a security barrier for the database itself, looking for threats and attacks in SQL instructions. If a threat is detected, it flags it, creates an alert, and if appropriate, blocks the offending data access attempt in real-time.

Continuously monitor

ARGUS Database Security provides continuous monitoring to capture and analyze all database activity from both application and privileged user accounts, providing detailed audit trails. Our agentless architecture means no software installation on database servers is required.

Supported Databases

Database	Versions	Collection Method
Oracle	11g - 21c	Unified Audit Trail, FGA
MySQL	5.7 - 8.x	General Log, Audit Plugin
PostgreSQL	10 - 16	pgAudit, pg_stat
SQL Server	2016 - 2022	SQL Server Audit
MongoDB	4.x - 7.x	Profiler, system.profile
MariaDB	10.x - 11.x	Audit Plugin
Cassandra	4.x+	Full Query Logging
IBM DB2	11.5+	db2audit
Couchbase	7.x+	Audit Logs
Firebird	4.x+	MON$ Tables

Remove risk in development and test

As organizations look to leverage their data, copies of production data are made for non-production environments. Industry analysts estimate that 82% of organizations have more than 10 copies of each production database, significantly increasing breach risk.

ARGUS Data Masking provides proactive control that protects sensitive data from unnecessary exposure without slowing development processes.

7+ Masking Techniques:

- Full Mask – Complete data redaction
- Partial Mask – Preserve first/last characters
- Email Mask – j***@***.com format
- Credit Card Mask – XXXX-XXXX-XXXX-1234
- SSN Mask – XXX-XX-1234 format
- Tokenization – Reversible token replacement
- Format-Preserving Encryption (FPE)

DEPLOYMENT BENEFITS

- 60-85% lower TCO than IBM Guardium and Imperva
- Deploy in 1-2 days vs 3-6 months with competitors
- Database firewall, masking, VA included at no extra cost
- Flexibility to scale as your business grows
- Multi-tenant MSSP-ready with white-label support

Flexible licensing and deployment

ARGUS FlexDeploy offers flexible deployment options. Deploy how and when you need it. You're protected regardless of the number, location, or type of databases – on-premises, in the cloud, air-gapped environments, or hybrid.

Total Cost of Ownership (3-Year Comparison)

Solution	Annual License	3-Year TCO
IBM Guardium	$150K - $300K	$800K - $1.3M
Imperva DAM	$100K - $250K	$600K - $1.05M
ARGUS (Vigilus Labs)	**$25K - $75K**	**$75K - $225K**

Vigilus Labs is a **cybersecurity innovator**
championing the fight to **secure data and applications** wherever they reside.