Kron TECHNOLOGIES

DATASHEET

Database Activity Monitoring (DAM) & Dynamic Data Masking (DDM)

Organizations place a heavy emphasis on data security.

Regardless of the industry—whether financial, insurance, telecom, pharma, and so on—or the type of data, be it product, employee, customer, financial, or medical, organizations recognize the need to secure and effectively monitor their sensitive data.

Data breaches or data loss can negatively impact stakeholders, potentially leading to a decline in stock prices, customer dissatisfaction, and even a financial crisis.

Simply complying with GDPR and similar regulations does not protect companies from data breaches. Thus, organizations should mitigate the effects of breaches by integrating data access or data masking solutions.

Maintain the same user experience

Utilize your preferred client seamlessly with Kron Database Activity Monitoring. No need to modify your current workflows or tools—simply integrate across your favorite database clients

Capture potential data breaches

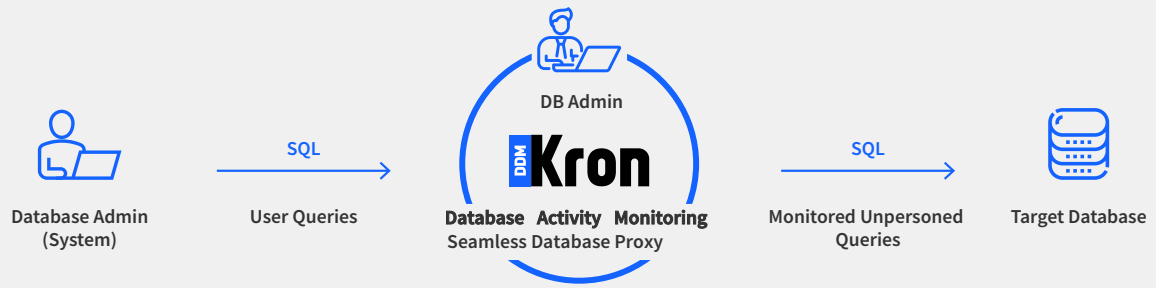
Capture potential data breaches by utilizing its comprehensive logging of all privileged session database connections. Monitor activities closely to prevent data loss, theft, or corruption effectively.

Centralize the security and control of privileged access

Guarantee users access only their assigned data, implement query execution policies, and apply data masking for enhanced control and security. Elevate your database management with Kron.

Create reports for regulatory compliance

Enhance your security and compliance by generating a complete audit trail that details who accessed specific data and when. Utilize the Kron DAM's flexible reporting module to generate insightful reports.



Seamless User Access to Target Database with Kron DAM

Policy and Access Management

Empower your database administrators with robust features to manage user permissions for database access queries.

Using Kron Database Activity Monitoring, administrators can **create rules and policies** that meet strict security specifications.

Through the implementation of policy enforcement and database masking, administrators can **seamlessly control user permissions,** proactively safeguarding against unauthorized execution of SQL commands.

Elevate your database security with our comprehensive central policy and access management system.

Dynamic Data Masking

Sensitive data is a valuable asset for enterprises, as it helps them better understand their customers, develop new products, and generate revenue. However, sensitive data also poses significant risks, as it can be exposed to unauthorized users, compromised by cyberattacks, or violated by regulatory requirements. According to Thales 2023 Cloud Security Study, **75% of businesses reported having sensitive data in the cloud, and 39% experienced breaches in the same year.** Therefore, enterprises need to implement effective data protection strategies to safeguard their sensitive data and maintain their competitive edge.

Kron Dynamic Data Masking is a powerful and user-friendly solution that provides advanced access and masking capabilities for enterprises. Kron DDM manages database access from a single point and provides role-based masking rules to restrict access to sensitive data.

Discover sensitive data across your databases

Scan your databases and identify the location, type, and volume of sensitive data, such as personal information, credit card numbers, health records, etc.

Manage database access from a single point

Use Kron Dynamic Data Masking to control who can access your sensitive data and apply role-based masking rules to restrict unauthorized access.

Provide masked data to privileged users

Protect your sensitive data from data breaches by showing masked or fictional (but realistic) data records to non-privileged users instead of actual data when they access the database.

Ensure data integrity and compliance

Prevent data tampering and manipulation by using Kron DDM, which ensures that data remains unchanged and complies with legal regulations such as GDPR and HIPAA.

Original Data

NAME	PHONE	BIRTH DATE	CREDIT CARD
John Doe	511-336-4455	11.4.1986	1111...3333 4444
Adam Smith	511-472-1314	2.2.1967	5555...7777 8888

Masked Data

NAME	PHONE	BIRTH DATE	CREDIT CARD
John Doe	511-111-1111	1.2.1987	3333 4444 XXXX
Adam Smith	511-123-4567	10.11.1966	7777 8888 XXXX

Kron Dynamic Data Masking (DDM) is a powerful solution that lets you define role-based masking rules that apply to different users and applications.

With Kron DDM, you can access the database without seeing the actual sensitive data, but instead receive masked or fictional data that looks realistic and consistent.

Kron DDM also logs and audits all data access activities, so you can monitor and track any suspicious behavior. Kron DDM supports various masking techniques, such as redaction, shuffling, blurring, tokenization, and substitution, to suit your specific needs and preferences.

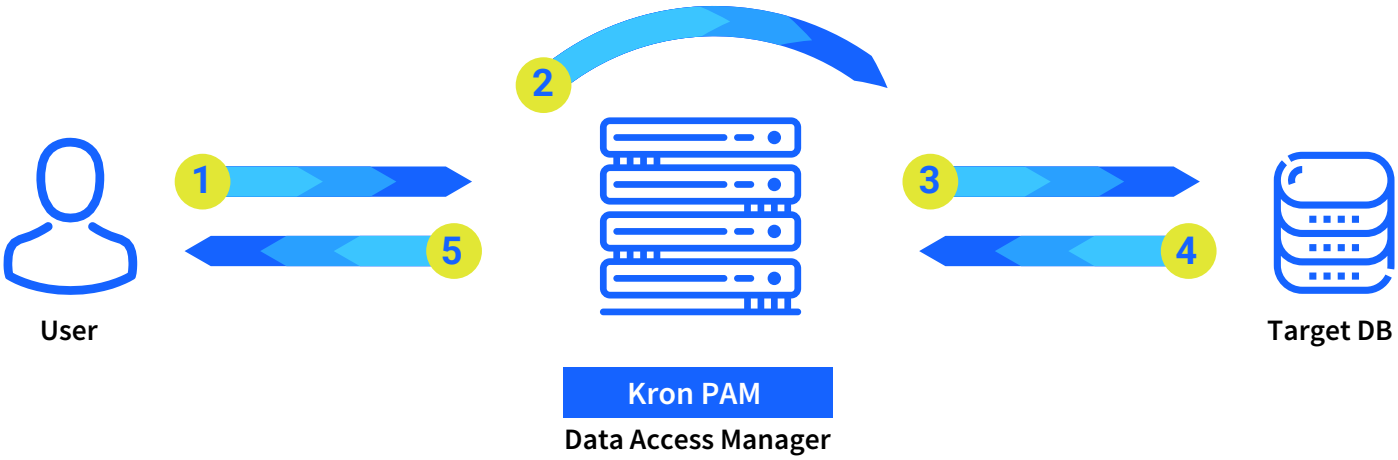
Kron DDM is a flexible and scalable solution that works with any database and any platform. Kron DDM is the ultimate solution for data security and management.

How The DAM & DDM Works?

The Database Activity Monitoring uses a man- in-the-middle proxy to control numerous kinds of databases - e.g. Cassandra, Hive, IBM DB2, Microsoft SQL Server, MySQL, Oracle and Teradata, among others - from a central point. User queries sent to database through SQLProxy.

SQL Proxy capture user queries and apply policies. **The conjunction of Database Activity Monitoring and Dynamic Data Masking ensures data security protection within the data layer itself and provides solid protection for database security.**

- Database activities are monitored by the proxy to permit any action that needs to be done.
- The Database Activity Monitoring seperates out records and shows database query results in accordance with the autorized users and logs all data access sessions.
- Dynamic Data Masking prepares or masks individual pieces of information inside the filtered data set. The DDM engine controls exactlywho should gain access to what, where, when, why and how; down to the level of individual cells in database queries.



Step 1
User runs query.

Step 2
The query is logged and then re-written based on the policy rule. If DDM is activated, (2A) query passes to DDM module and enhanced masking rules are executed. (2B) Masked query is returned to the Database Access Manager.

Step 3
Manipulated query is forwarded to the target DB.

Step 4
Target DB returns the result of query to Kron PAM's Database Activity Monitoring.

Step 5
Kron PAM's Data Access Manager forwards the filtered results to the user

Features & Benefits

Single point of access control management for database layer.

All queries are logged indisputably. Users authenticate with their own credentials even if there is no such DB user, so the real user running a query is known and logged.

Identifies **sensitive data**, such as credit card numbers or personal ID numbers, stored in databases and **Big Data** servers.

Sensitive data can be manipulated and delivered to **applications or users** in a way that renders it non-sensitive, yet remains coherent and usable.

Policies (DB masking rules) can easily and **instantly be assigned** to users, application accounts and/or groups and roles.

Minimizes the **risk of disclosure** for data in progress.

Accounts can be **time-limited** (hours of day, day of the week, etc.).

Has no performance degradation impact on target Databases.

Users are not required to use a proprietary **database** client and can continue using familiar tools (i.e. Toad, etc.). Authorization can be given without any interference.

Eliminates weak and **non-expiry passwords**. Disables inactive accounts.