DataSunrise

DataSunrise Database Security Suite is data-centric database security solution which combines data audit, database firewall and data masking modules.

Benefits

- Data protection in the cloud and on premises across multiple data silos.
- Easy deployment and integration into existing database environments.
- Continuous scanning of traffic between database and client applications in real time
- Seamless integration with most third-party systems such as SIEM
- Compatibility with all popular relational databases.
- Email and SNMP notifications on system events
- Comprehensive web-based GUI
- Achieving and maintaining compliance with database-specific government regulations and industry standards
- Cross-platform (Windows, Linux, UNIX)

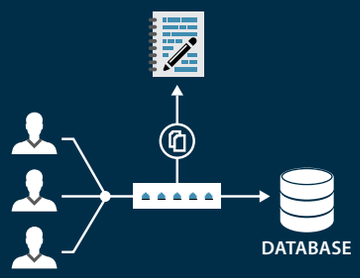
DataSunrise deployment

DataSunrise can be deployed on a separate server or on the database server with minimum impact on database performance. Deployment process doesn't require any changes in database infrastructure.
Depending on scenario, DataSunrise can operate in one of the following modes:

Sniffer mode

This mode used mostly for stealth traffic auditing and self-learning purposes.

Database clients connect the database directly and DataSunrise receives copy of network traffic for analysis from network switch's "mirrored" port. To deploy DataSunrise in this configuration, no tweaking of client applications or the database is required.



Proxy mode

In proxy mode DataSunrise acts as a proxy server, thus database clients query the database through DataSunrise only. Since direct access to the database is disabled, in this mode DataSunrise can block or modify queries before redirecting them to the database. Running DataSunrise in this mode requires additional tweaking of client applications or reconfiguring the database server. Response time is somewhat increased too. DataSunrise can be configured as a reverse proxy as well.

DataSunrise is an innovative software company dedicated to delivering data security products. Our company was founded by a talented team with strong background in database management systems and enterprise security space.

(206) 420-6611 info@datasunrise.com www.datasunrise.com

How it works

DataSunrise Database Security Suite includes three functional modules: Data Audit provides data auditing, Data Security protects the database against unauthorized access and SQL injections, and Data masking is used for dynamic obfuscation of the database output.

Traffic processing control is based on a system of security policies (rules) configured by administrator. Rules define DataSunrise actions (auditing, blocking, masking etc.) and events that trigger these actions. Each functional module has its own system of Rules.

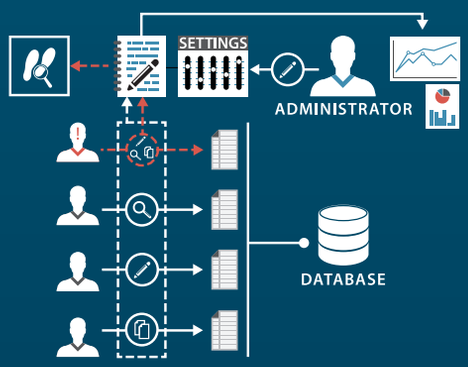
Database traffic intercepted by DataSunrise undergoes two-stage analysis. On the first stage DataSunrise picks out SQL queries, execution results and other information. Queries that match conditions defined by existing security policies undergo detailed investigation: DataSunrise determines names of database elements queries directed to, database output, session details and other valuable information. Then DataSunrise acts according to existing security policies: it audits traffic, blocks SQL-injected queries or obfuscates the output.

Data Audit

DataSunrise logs all user actions, SQL queries and query results. Audit information is saved to firewall-integrated SQLite database or to external database. Auditing results can be exported to third-party system such as SIEM.

Data auditing is most useful for investigating data breach incidents: it enables to reveal occurred data leak, estimate its cost and identify the perpetrator. When paired with SIEM system, data auditing helps to learn a big picture of database activity and detect suspicious behavior before data breach is occurred.

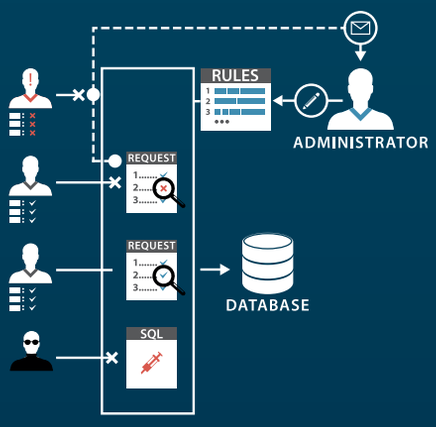
Additionally, DataSunrise delivers self-learning functionality, Learning mode. DataSunrise logs typical database events and creates a white list of queries considered as «safe» in given database environment. The "white list» of queries simplifies configuring of data protection policies and prevents firewall misfiring.



Security

Data Security module is used to prevent unauthorized access attempts and SQL injections on-the-fly. Rule settings enable the firewall administrator to define which queries should be treated as unauthorized based on query source, destination and query code. Prevention of SQL injection attacks is performed due to integrated threat detection algorithms.

If DataSunrise detects unauthorized access attempt or SQL injection attack, it blocks execution of suspicious query or disconnects suspicious user from the database. When the threat is neutralized, DataSunrise notifies the firewall administrator via Email or SNMP.



Dynamic Data Masking

Dynamic masking mostly used to prevent data leak when giving access to live database to third-party IT specialists such as contractors or outsourcers.

DataSunrise intercepts a query, applies masking to it and redirects to the database. Having received modified query, the database alters its output by replacing sensitive data with random values, predefined strings or special symbols.

Along with general-purpose masking methods, DataSunrise provides dedicated algorithms for credit card numbers, Email addresses and date-containing entries.