DataSunrise

Next Generation Data-Centric Security Software

aws partner network
Advanced Technology Partner
Security Competency
Amazon RDS
Amazon Redshift
Amazon Linux 2
Microsoft Workloads

DataSunrise, Inc.
www.datasunrise.com
info@datasunrise.com
+1 206.420.6611

ULTIMATE REAL-TIME DATABASE PROTECTION

- Data Audit, Database Firewall, Dynamic and Static Data Masking, In-Place Masking, Read Native Database Audit Logs, Sensitive Data Discovery – all in one
- Achieving compliance with widespread security standards such as SOX, CCPA, PCI DSS, HIPAA, GDPR, ISO27001
- Continuous database traffic monitoring to/from database servers
- Prevention of SQL injection attacks, Blocking of DDOS and Brute-Force attempts
- Protection in the cloud and on-premises across multiple data silos
- Integration with third-party SIEMs and system management solutions
- Role-based and Location aware policies
- Self-learning rules engine
- Managing DataSunrise configuration as code (Iac)
- Heterogeneous database support with centralized management
- Authentication proxy, High Availability and Autoscale
- Client application user translation, audit and security
- Vulnerability Assessment and Health Check
- Data Encryption on-the-fly and Hide Rows
- Integration with CyberArk, Splunk and RSA

DATABASE ACTIVITY MONITORING

Tracking of all user actions, queries and changes made to databases in real time.

Advanced Audit Compliance Reporting Platform.

Revealing and preventing data leaks.

Application user translation.

DYNAMIC DATA MASKING

Role based and location aware production data protection.

Prevention of accidental data leaks by obfuscating the output from protected databases.

A variety of prebuilt masking algorithms and the possibility to use custom functions for masking.

STATIC DATA MASKING

Enables you to create a fully functional copy of the database with obfuscated data.

Gives you a perfect testing and development environment preventing accidental data leak.

Has no impact on original database.

DATA SECURITY

Analyzing and monitoring of database traffic.

Protection from unauthorized queries and SQL injections in real-time.

Notifications and report generation on detected threats to IT Security and DevOps.

VULNERABILITY ASSESSMENT

Informs about all known CVEs.

Checks databases with the requirements of CIS and DISA with SQL queries.

Provides the information about available database security patches.

Enables you to keep the databases secure and up to date.

SENSITIVE DATA DISCOVERY

Detects where sensitive and confidential data in the company.

Supports a large number of databases both on-premises and in the cloud.

Effectively enforce monitoring and security policies.

Intelligently discovers the relationships between tables when some of them contain sensitive or PII data.

Utilizes multiple patterns to automate the search process.

*All other product names mentioned are used only for identification purposes and may be registered trademarks of their owners

DataSunrise

Next Generation Data-Centric Security Software

aws partner network
Advanced Technology Partner
Security Competency
Amazon RDS
Amazon Redshift
Amazon Linux 2
Microsoft Workloads

DataSunrise, Inc.
www.datasunrise.com
info@datasunrise.com
+1 206.420.6611

USER BEHAVIOR ANALYSIS

Gathers more insights about database activity and detects user's behavior anomaly.

Returns a list of suspicious activities from audited data storage.

Gives notices and alerts on suspicious activity.

Uses your audit database as a training dataset.

SUPPORT FOR UNSTRUCTURED DATA

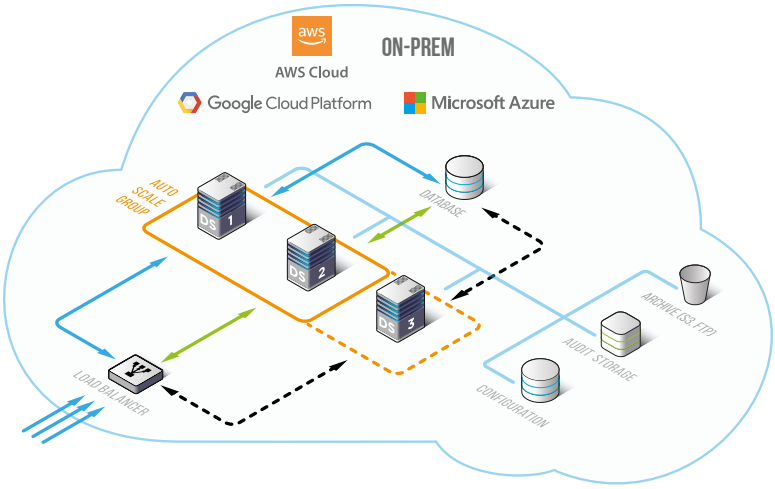
Uses Natural Language Processing (NLP).

Discovery and masks sensitive data in unstructured data (plain text).

Works with text files and binary data types (Word, PDF, etc.).

SUPPORTED DATABASES

Amazon RDS	Amazon DynamoDB	Amazon Redshift	Amazon Aurora
Oracle	Teradata	SAP HANA	Neo4j
PostgreSQL	Hive	Azure SQL	Snowflake
MySQL	Cassandra	Google Cloud SQL	MS SQL Server
IBM DB2	MongoDB	Impala	and more...



HOW IT WORKS

Traffic processing control is based on a system of security policies (Rules) configured by an administrator. The 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. At first 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, query results, session details and other valuable information. Then DataSunrise applies existing security policies: audits the traffic, blocks SQL-injected queries or obfuscates query results.

*All other product names mentioned are used only for identification purposes and may be registered trademarks of their owners

DataSunrise
Next Generation Data-Centric Security Software

aws partner network
Advanced Technology Partner
Security Competency
Amazon RDS
Amazon Redshift
Amazon Linux 2
Microsoft Workloads

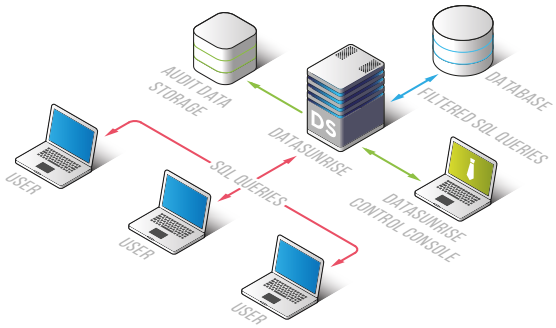
DataSunrise, Inc.
www.datasunrise.com
info@datasunrise.com
+1 206.420.6611

DATASUNRISE DEPLOYMENT

DataSunrise can be deployed in the cloud or on-premises, installed locally on a database server or on a separate machine. Depending on deployment scheme, DataSunrise can operate in Proxy or Sniffer modes:

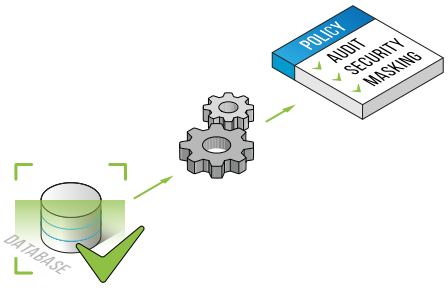
Proxy Mode and Sniffer Mode

Database clients connect to the database through DataSunrise proxy. DataSunrise can block or modify queries before redirecting them to the database. DataSunrise can be configured as a reverse proxy as well.



Compliance Automation

The Compliance Manager feature provides automated data and database security according to national and international regulatory requirements (HIPAA, GDPR, PCI DSS, SOX, CCPA, ISO 27001, KVKK, etc.).



Cloud Watch

DataSunrise can be integrated with Amazon CloudWatch to display DataSunrise-associated metrics and create alarms. Maintaining SaaS Azure SQL inside the Azure cloud is possible as well.

AWS Cloud Formation and Terraform

DataSunrise provides a dedicated script for deployment of HA environment for Amazon cloud service based on AWS CloudFormation and Terraform. All objects are created automatically without user interference.

High Availability And Auto Scaling

When installed in this configuration, all DataSunrise servers use a common Dictionary storage that can be monitored and controlled from any machine. DataSunrise can be paired with a Load Balancer of some kind for Auto Scaling.

Two-Factor Authentication

DataSunrise 2FA tightens control over access to your target database. The basic login procedure is intensified by either email-based authentication or a Google Authenticator verification code.

Application Users

Connects database activity and client application users.

Lets you to mask data or block database access for certain users.

Uses several different techniques to find markers of an application user.

Helps to be compliant with requirements of HIPPA and SOX.

*All other product names mentioned are used only for identification purposes and may be registered trademarks of their owners