DataSunrise

DATABASE & DATA SECURITY & MASKING

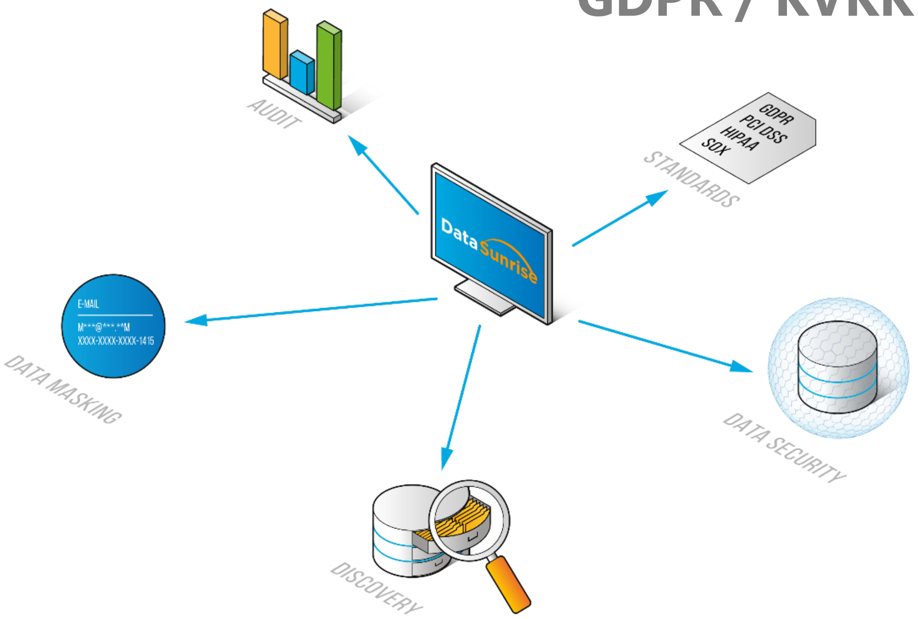
Real Protection and Compliance in Real-Time

DataSunrise Overview

- ✓ DataSunrise secures databases and data in heterogeneous environments in the cloud and on premise.
- ✓ Gives Customers a full and granular control over:
  - security of sensitive data
  - access to data and databases
  - automated compliance policies

- ✓ DataSunrise empowers organizations when moving their databases workload to cloud Database managed services
- ✓ Preserves same level of data security and data auditing

GDPR / KVKK



DataSunrise Benefits

aws partner network

Advanced
Technology Partner

Security Competency
Amazon Redshift
Microsoft Workloads

DataSunrise

- Universal security with Data Auditing, Database Security, Data Masking, Data Discovery and Compliance automation
- Centralized management of security policies & compliance
- Homogeneous database security experience in heterogeneous databases environments
- Monitors database traffic, streamlines compliances in databases
- Supports all popular SQL and NoSQL databases on multiple platforms
- Easy installation, deployment, and integration with cloud providers services

Supported Databases

ORACLE

mongoDB

TERADATA

SAP HANA

MariaDB

IBM DB2

IMPALA

HIVE

VERTICA

Greenplum

PERCONA

NETEZZA an IBM Company

IBM Informix software

cassandra

PostgreSQL

MySQL

SQL Data Warehouse

Microsoft SQL Server

Microsoft SQL Azure

IBM Big SQL

Google Cloud SQL

elasticsearch

Amazon Aurora

Amazon Elasticsearch Service

Amazon S3

Amazon Athena

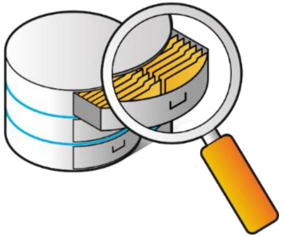
Amazon Redshift

Amazon DynamoDB

Sensitive Data Discovery

DataSunrise

- Data Discovery enables searching through the database for sensitive data to quickly establish protection for sensitive database tables.
- DataSunrise includes built-in search filters for various data types including personal, financial or medical records.



- A user is able to create own filters.
- DataSunrise includes the search filters for the following data types:

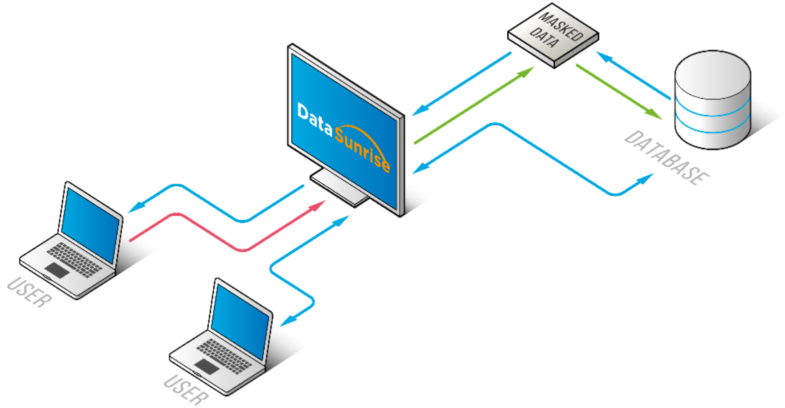
- Personal identifiable information
- Financial data
- Medical data
- Addresses
- Internet related data

Data Masking

- DataSunrise obfuscates the output of sensitive data by replacing it with random or real-looking data.
- Role-based and location aware.
- DataSunrise offers a variety of masking algorithms for any possible scenario.
- DataSunrise includes both **Dynamic** and **Static** Data Masking.

Dynamic Data Masking

- DataSunrise helps to prevent accidental data leaks by obfuscating the database output without changing actual data.
- DataSunrise intercepts a user query, applies masking algorithm to it and redirects it to the database. As a result, the database obfuscates output by replacing sensitive data with random values, predefined strings or special symbols.
- DataSunrise can modify directly the result sets returned by database back to the client application
- DataSunrise can mask not only in sql queries, but also within store procedures and db functions.
- DataSunrise includes a variety of built-in general-purpose algorithms, plus dedicated obfuscation algorithms for credit card numbers, email addresses, date and time entries,..etc.
- DataSunrise includes custom functions and Lua scripts options, format preserving encryption (FPE).

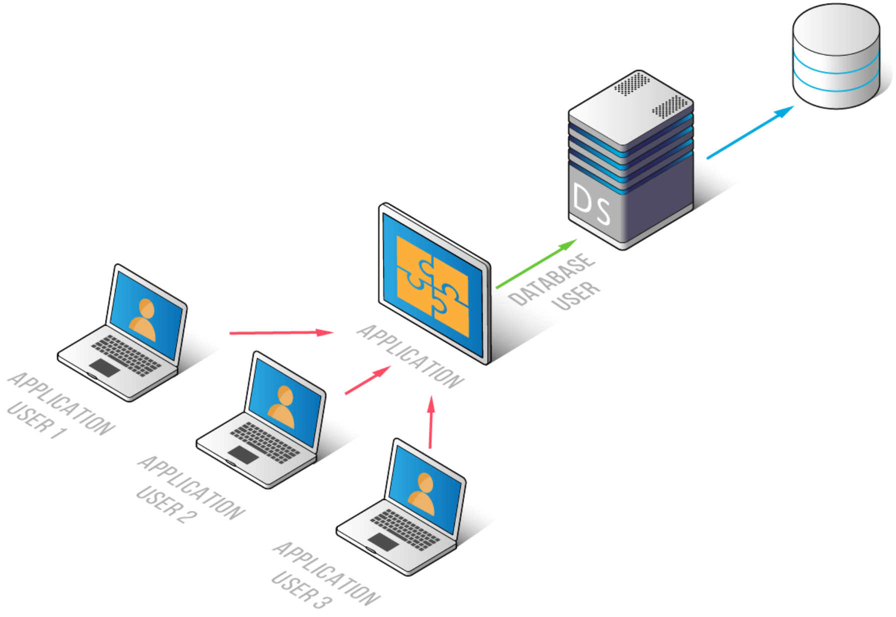


Application User Translation

Application user translation enables to map client application users to database activity and identify end users that connect to the database via an application server.

Monitor database activity or configure security rules in respect to certain application users.

Block unwanted queries, manage access to sensitive data and leverage the dynamic masking functionality by concealing valuable data from unauthorized application users on-the-fly.



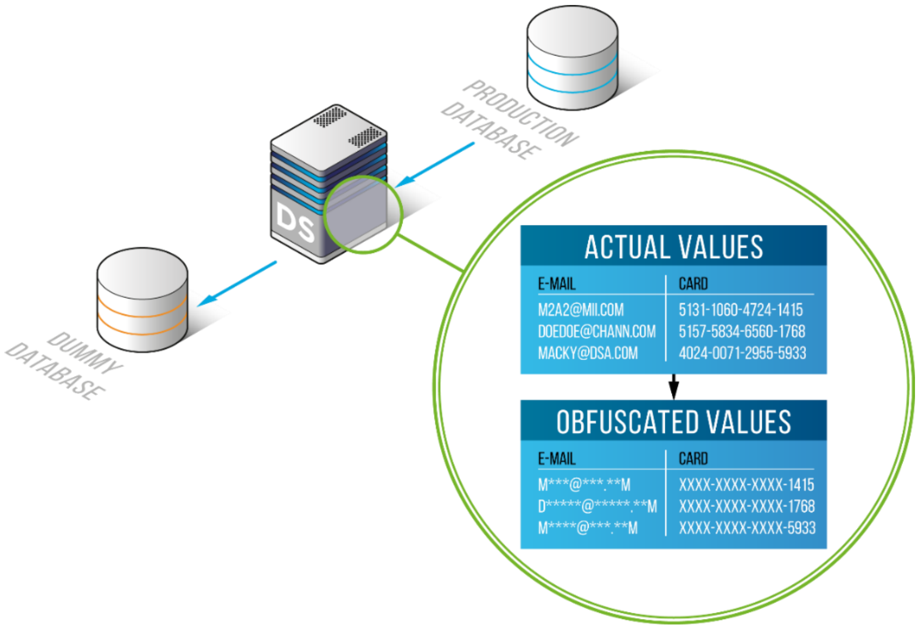
Static Data Masking

- Used when creating a fully functional copy of a production database where original sensitive data is replaced with not-real values.

- Enables building and maintaining a solid testing or development environment while preventing any accidental data leak to third parties or contractors.

- DataSunrise integrated with high-speed native database loaders to speed up the copying.

- Support for custom functions and Lua scripts, database functions, FPE and Tokenization



ACTUAL VALUES

E-MAIL	CARD
M2A2@MII.COM	5131-1060-4724-1415
DOEDOE@CHANN.COM	5157-5834-6560-1768
MACKY@DSA.COM	4024-0071-2955-5933

OBFUSCATED VALUES

E-MAIL	CARD
M***@***.**M	XXXX-XXXX-XXXX-1415
D*****@*****.**M	XXXX-XXXX-XXXX-1768
M****@***.**M	XXXX-XXXX-XXXX-5933

Database Activity Monitoring

- DataSunrise enables real-time tracking of all user actions and all changes made to the database.
- DataSunrise Auditing assists in revealing any potential data breaches, quickly finds its culprit and assesses the impact & cost.
- Audit Compliance Reporting Platform.

Database Audit

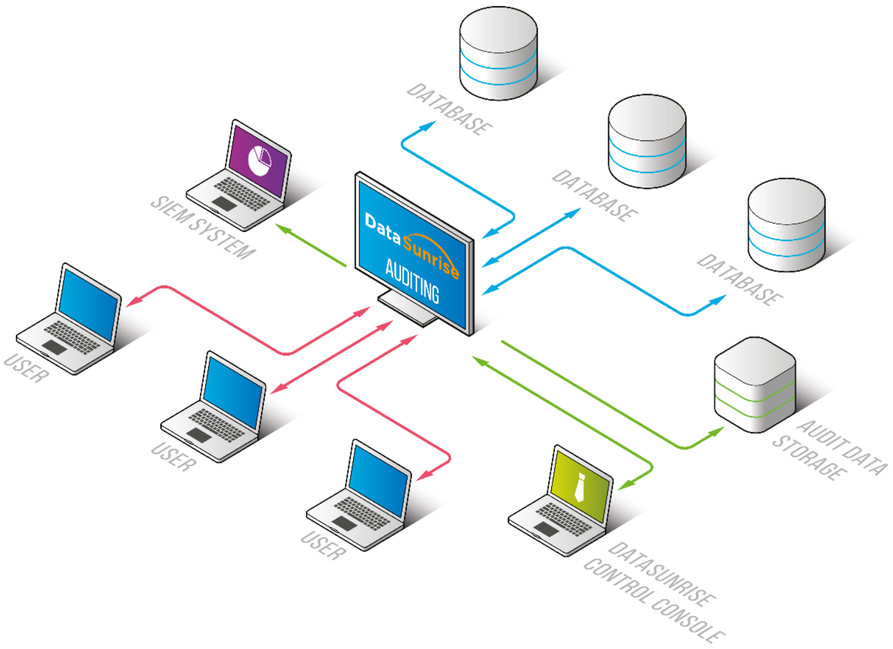
- DataSunrise logs all user actions, SQL queries and query results, including auditing store procedures

- Data Audit saves information on database users, user sessions, query code, etc.

- Audit results are stored into an integrated database or into an external database or S3.

- Exported to 3rd party data management systems, such as SIEM. When paired with SIEM system, Data Audit helps to get a big picture of database user activity.

- Advanced reporting based on security policies.



Database Firewall

- DataSunrise DBF analyzes database traffic, detects and prevents execution of unauthorized queries and SQL injections in real time.
- Alerts and reports on detected threats are delivered to network administrators via an email, SNMP or instant messengers.
- Blocking of DDOS and Brute-Force attempts
- Role-based and location aware.

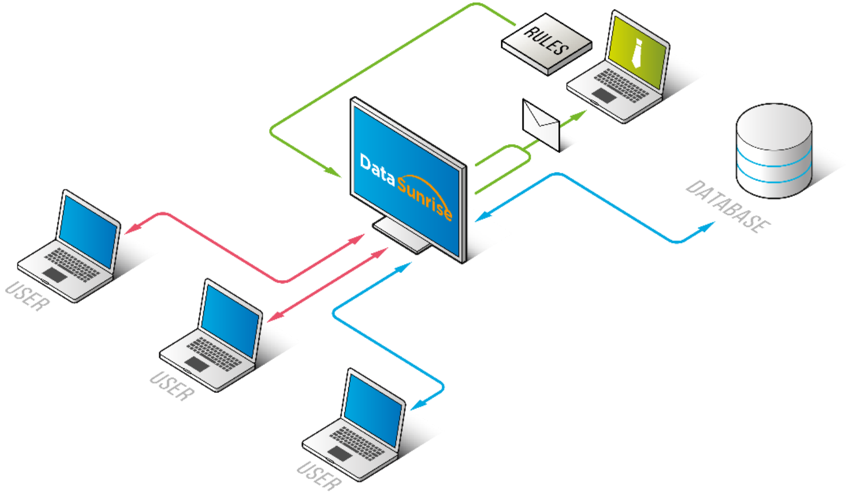
Database Active Security

DataSunrise DAF prevents unauthorized access attempts and SQL injections on-the-fly.

With DAF Security Policies administrator defines the queries to be treated as unauthorized based on query source, destination and SQL statements used.

Automatic blocking of SQL injection attacks with integrated threat detection algorithms in DB Firewall.

When DataSunrise detects an unauthorized access attempt or SQL injection attack, it blocks a suspicious query in the form of a database error, or disconnects a suspicious user from the database.



Once the threat is neutralized, DataSunrise notifies the firewall administrator via an email, SNMP or instant messengers.

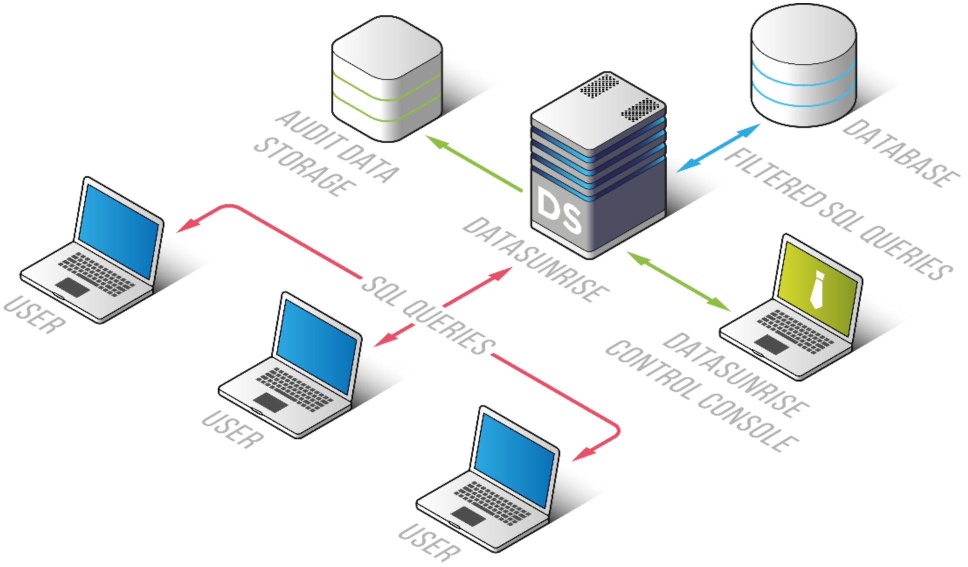
Built-in behavioral analysis (learning engine).

Operating Modes

Proxy Mode

DataSunrise is placed between database clients and the database server to disable direct access to the database.
The clients can connect and access the database through the DataSunrise firewall only.

In this configuration DataSunrise can perform data protection as well as data masking and auditing.



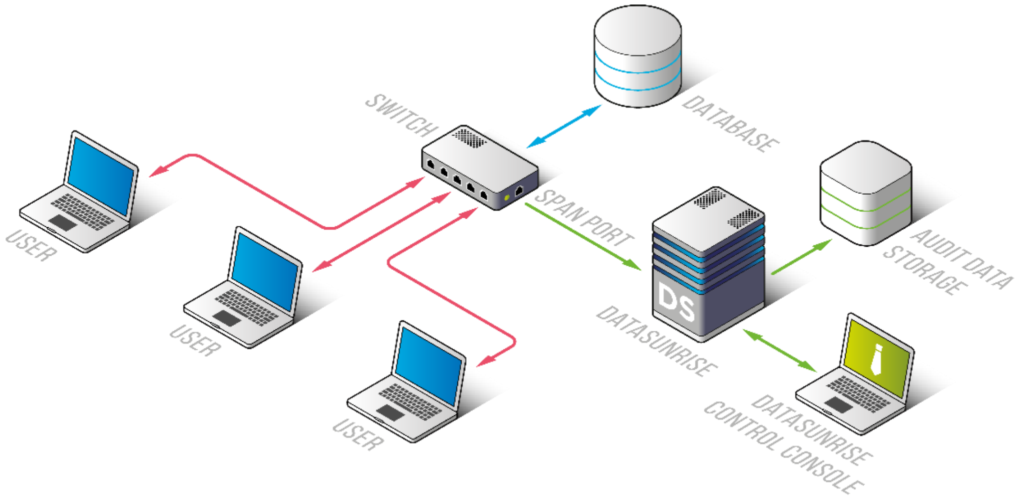
Operating Modes

DataSunrise

Sniffer Mode

DataSunrise works as a “sniffer”: it gets mirrored traffic from a network switch and performs stealth auditing.

In this configuration only data auditing is available. No database server reconfiguration is required.

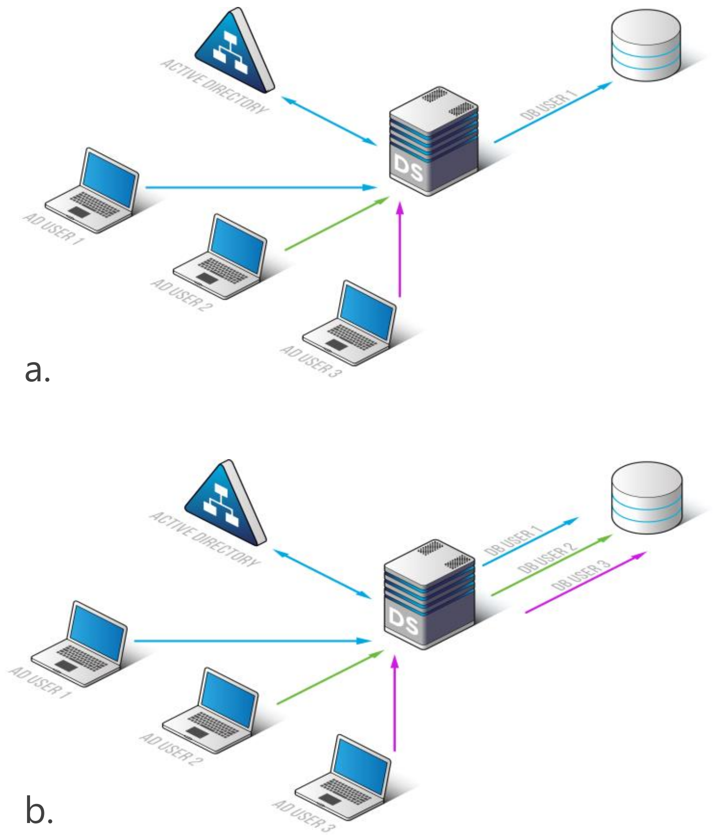


Authentication Proxy

- DataSunrise Authentication Proxy provides Active Directory (AD) authentication support to maintain organizational authentication policies.

- Authentication Proxy provides mapping of each AD user to a separate DB user (Figure 1.a) or mapping multiple AD users to one DB user (Figure 1.b).

- It ensures secure connection to cloud and on-premises databases with AD user credentials when the protected database itself doesn't support integration with AD.



a.

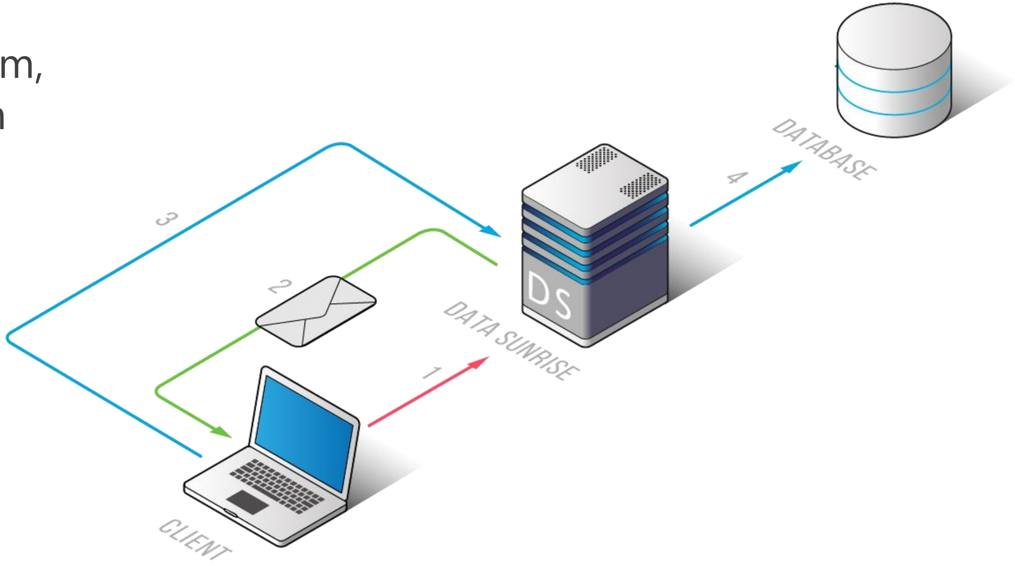
b.

Two-Factor Authentication

DataSunrise

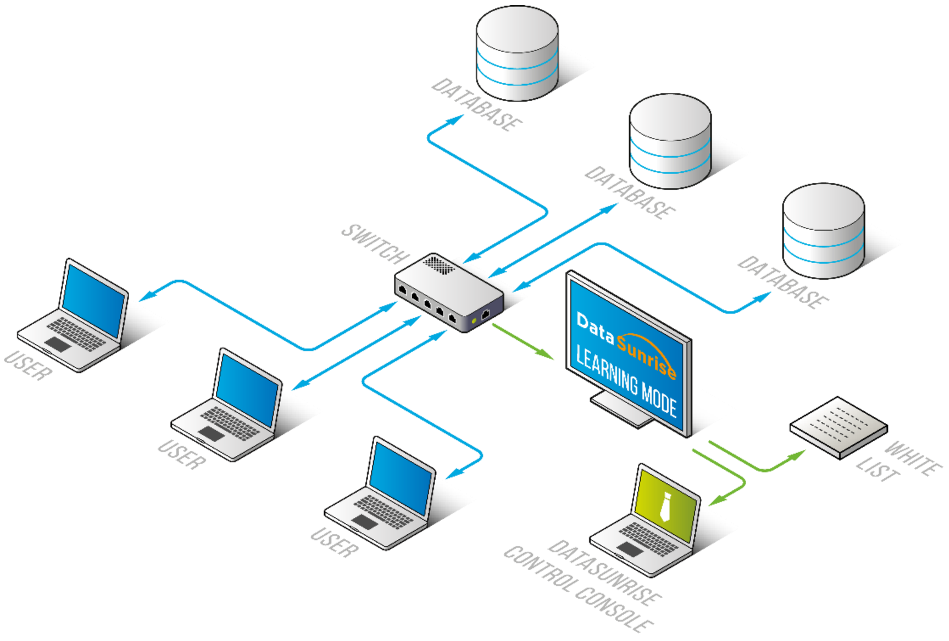
- DataSunrise provides two-factor authentication to the target database as an extra layer of database security.

- Before obtaining access to the restricted system, users are authenticated with two identification methods
  - username and password combination
  - email authentication.



Intelligent Learning Mode

- DataSunrise features self-learning capability, the Learning Mode.
- DataSunrise creates a list of queries acceptable in a given database environment.
- DataSunrise creates a list of database objects routinely addressed and a list of database users authorized to access these objects.
- “White lists” help to speed up configuring of data security policies and to prevent firewall “misfiring”.



THANK YOU!

DataSunrise

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