DataSunrise

DATABASE SECURITY SOLUTION

WHITE PAPER

CONTENTS

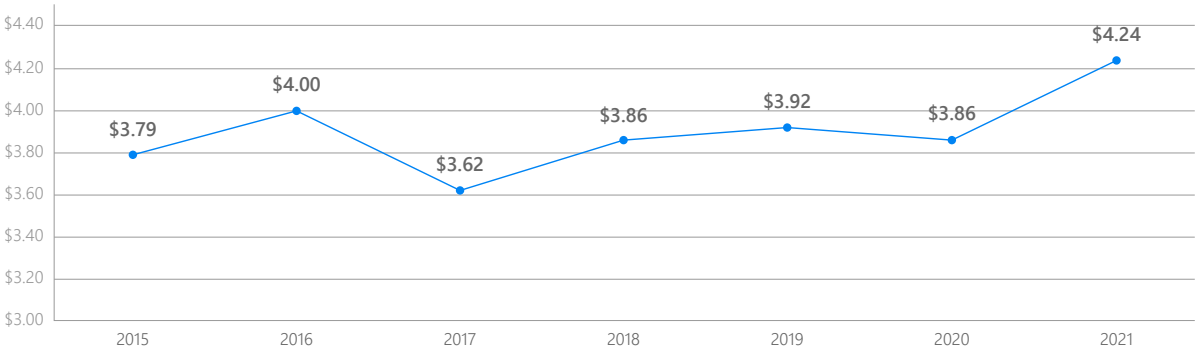
INTRODUCTION

We observe the situation with data breaches every year. As we see in the latest report from IBM and Ponemon Institute, the number and cost of data breaches rise with every year passed. And the prognosis does not give us time for taking a breath.

According to the report from IBM Security, the average cost of data breach is on the rise. Since 2020, the cost of breaches has increased by 9.8% and now it has reached $4.24 M!

In 2020, the cost of data breach was $3.86 M, and in 2019 it was $3.92 M.

Average total cost of a data breach
Measured in US$ millions



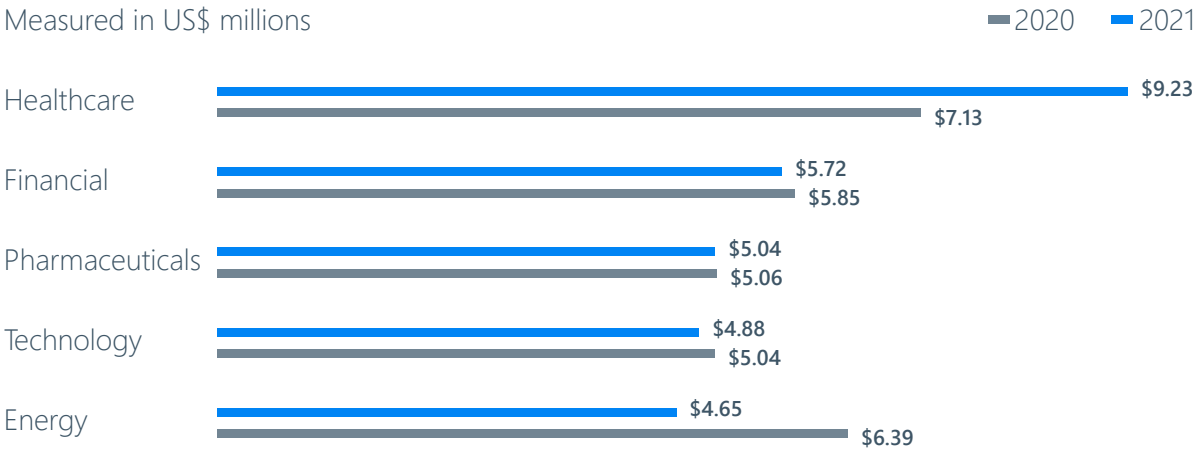
The most vulnerable spheres where sensitive data is under huge risk are:

- Healthcare;
- Financial;
- Pharmaceuticals;
- Technology;
- Energy.

During the last 11 years, the healthcare industry has been the most vulnerable, and in 2021 the cost of data breach made up $9.23 M. In comparison with the previous year, there is a 29.5% increase.

Average total cost of a data breach by industry

Measured in US$ millions



The most common type of compromised records was customer PII (Personal Identifiable Information). It was involved in 44% of all breaches. The cost per lost or stolen PII record in 2021 was $180 on average.

As the cost of data breach rises, the amount of time required to identify and contain a breach also increases. The lifecycle of a data breach in 2021 took 287 days. In comparison, in 2020 it took less, 280 days for identifying and containing a data breach.

A serious problem for all businesses is to stay in compliance with different regulations and laws. Compliance failures adversely affect companies and the cost of a data breach. In 2021, the cost made up $5.65 M.

The most common initial attack vector in 2021 was compromised credentials (20%). But the costliest ones were phishing and malicious insiders (second and third places accordingly).

Cloud breaches are another headache for companies all around the world. The average price of a cloud-based breach in a public cloud is $4.8 M and $4.55 M for a private cloud.

The situation with the pandemic also does not work in businesses' favor. The impact of remote work is vital. In the situations when the remote work is a factor, the cost of the breach reaches $4.96 M. Otherwise, the cost is $3.89 M. The difference between them is 24.2%.

Every business is susceptible to data breaches, no matter its size. Small businesses pay on average $2.98 M this year. There is a 26.8% increase compared with the previous year. And this amount of money may be critical for small businesses.

Curiously, middle-sized companies (500-1000 employees) have the smallest average cost. It consists of only $2.63 M.

And of course, the highest average cost of a data breach takes businesses with 10000-25000 employees. The cost is $5.52 M.

WHAT YOU NEED TO KNOW ABOUT DATABASE SECURITY

As a rule, employee and client data, commercially-sensitive and other important information are stored in corporate databases and that is why database security is critical to a company's operations.

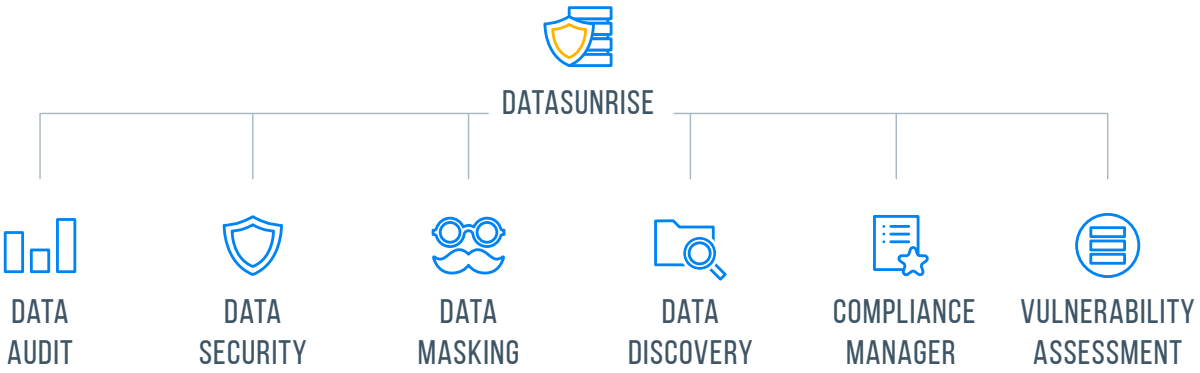
Despite numerous data breach incidents, not so many organizations pay proper attention to data security. For instance, they use DBMS-integrated solutions for data protection and auditing purposes. But experience shows that such integrated tools' capabilities are very limited so they can not counter modern threats. Besides that, integrated solutions are prone to inflict load on the database servers they're installed on. All these drawbacks often make database administrators disable built-in auditing and protection.

One of the basic ways of protection against insider threats is strict user rights differentiation, but in practice employees often get excessive access rights. Such situations increase the potential risk of user privileges misuse and make the security system more vulnerable. For instance, a malicious actor can seize control of a database user account and increase its access rights level so it can lead to a data breach. DBMS-built-in security systems often ignore such incidents because they see nothing suspicious in a sudden increase of user access rights and are not able to identify a potential threat to database security.

It means that DBMS-integrated solutions in most cases are not able to maintain a sufficient level of security. Besides that, efficient security tool development requires data-security-specific knowledge and experience, which DBMS developers often lack (they are database experts, not security experts). That is why if the high level of database security is of importance, it is better to use dedicated software like DataSunrise Database Security Solution.

WHAT IS DATASUNRISE?

DataSunrise Database Security is a data-centric security solution purpose-built for the protection of relational and NoSQL database contents against external and internal threats. DataSunrise Suite includes the following functional modules: Data Audit, Data Security and Data Masking, Sensitive Data Discovery, Compliance Manager, and Vulnerability Assessment.



Data Audit

DataSunrise enables real-time database activity monitoring. Database Audit logs all incoming user queries and query results and collects extensive information on all database users trying to access the protected database. It logs the query's code, user information (IP address, username, client application name, etc.), session information, etc. For maximum efficiency, Data Audit can be paired with a SIEM system to analyze the audit results.

The Data Audit component features a **Self-learning Capability**, the Learning mode. When running in Learning mode, DataSunrise creates an "allow list" of queries acceptable in a given database. This list simplifies the creation of security policies and prevents the database firewall from "misfiring". It can also create a list of "safe" queries used to access the lists of database objects, and a list of database users who are authorized to access these objects.

Data Security

An integrated database firewall prevents hacker-driven data breaches and insider-caused data leaks. DataSunrise utilizes smart traffic filtering algorithms to detect SQL injection attacks, DDOS attacks, Brute-Force attempts, and unauthorized queries in real-time.

DataSunrise's flexible system of security policies enables the firewall administrator to restrict access to certain database objects based on database usernames, IP addresses, client applications, and queries used.

Data Masking

DataSunrise includes Dynamic, Static, and In-place Data Masking.

The **Dynamic Data Masking** capability enables DataSunrise to limit exposure of sensitive database contents to unauthorized users by obfuscating the query results. DataSunrise intercepts unauthorized user queries, modifies them according to existing masking policies, and redirects to the database. Having received the modified query, the database provides the original user with an obfuscated response.

In most cases, data masking is used to prevent insider-driven data leaks during database development and testing procedures. Masking conceals only the query results without affecting the actual database contents.

DataSunrise **Static Data Masking** protects sensitive data from exposure in non-production environments such as development, devops, or testing environments; completely eliminates the possibility to reverse engineer the masked data or access the original sensitive records. The Static Masking engine creates a copy of a live database where actual data is replaced with a fake. At the same time, a "dummy" database remains fully operational and can be used for analytical, development, or statistical purposes.

Both Format-Preserving Encryption (FPE) and Format-Preserving Tokenization (FPT) are included in the Static Masking component. FPE and NLP (Natural Language Processing) masking (masking of unstructured data) are included in Dynamic Masking.

DataSunrise supports the **In-place Data Masking** capability as well. In-place masking obfuscates sensitive database columns by filling them with fake data in the same, "source" database ("In-place"). Hence, you can replace your sensitive data in the database with the obfuscated one and use such a database for your purposes without the need of creating and maintaining another "dummy" database. The obfuscated data in such a database will still be usable and fully operational. Also, in-place masking replaces the sensitive data permanently and irreversibly.

Format-Preserving Encryption and Tokenization

FPE and FPT enable you to obfuscate sensitive data, preserving the format of this data at the same time. For encryption, DataSunrise uses the AES (Advanced Encryption Standard) algorithm. Thanks to FPE and FPT, you can keep the structure of databases and applications while securing sensitive data by replacing it with masked one.

Moreover, FPE is very useful for primary and foreign keys obfuscation. Using FPE enables you to keep referential integrity so every time your data will be returned complete, and there will be no loss of valuable information.

Natural Language Processing

Natural Language Processing (NLP) enables you to mask sensitive data contained in database columns in the format of plain text. DataSunrise parses the columns' contents and replaces sensitive data with asterisks (*).

The NLP masking engine supports the following file formats: DOC, DOCX, RTF, ODT, OTT, HTML, TXT, PDF, and others.

Sensitive Data Discovery

Data Discovery enables companies to detect where sensitive and confidential data resides across their databases. In DataSunrise, you can configure a periodical search of sensitive data according to your schedule.

Data Discovery by DataSunrise has different engines to detect sensitive data in almost every possible format. With NLP, you are able to search through sensitive data in plain text (unstructured data) in such formats as PDF, Word, TXT, etc. With the OCR functionality, you are able to search for sensitive data through Amazon S3 buckets in the following image file formats: JPG, PNG, GIF, etc. In Amazon S3 you can also search for parquet files, unstructured text files, and common CSV, XML, and JSON.

Of course, you can discover data using regular expressions and built-in dictionaries. If these are not enough, we support Lua script for uncommon formats of data.

Table Relations

The Table Relations enables DataSunrise to analyze database traffic and create associations between database columns. "Associated columns" means that these columns can be linked by integrity constraints or by JOIN and WHERE clauses in queries.

Associations can be used when configuring Dynamic and Static data masking. DataSunrise suggests possible associations when selecting the columns to be masked. Moreover, DataSunrise displays associated columns that were discovered by the Data Discovery component to avoid the loss of unprotected sensitive data.

Compliances

DataSunrise's Compliance Manager enables you to search for sensitive data according to international and national security standards and regulations. Having found sensitive data, you can quickly and easily apply masking, audit, and reporting to it. Also, here you can arrange users into 4 groups and configure access to your sensitive data according with the Principle of Least Privilege (POLP).

DSAR

The Data Subject Access Request (DSAR) component enables you to detect where sensitive and confidential data resides across your databases to ensure compliance with the corresponding laws and regulations and effectively enforce monitoring and security policies.

DataSunrise uses its Data Discovery engine that works periodically on schedule for DSAR purposes. Besides that, easily configurable reports on data of interest are available.

Reporting

Data collected by DataSunrise's components can be used for creating custom PDF or CSV reports. Auditing results can be transferred to an external SIEM application through Syslog.

Vulnerability Assessment

Thanks to Vulnerability Assessment by DataSunrise you are able to identify and get rid of security vulnerabilities in your databases. To fulfil the task, CIS Benchmark and DISA STIGS recommendations are used.

Using Vulnerability Assessment, your database administrators can get the latest information about available database security patches and apply them to increase database and data security across your company.

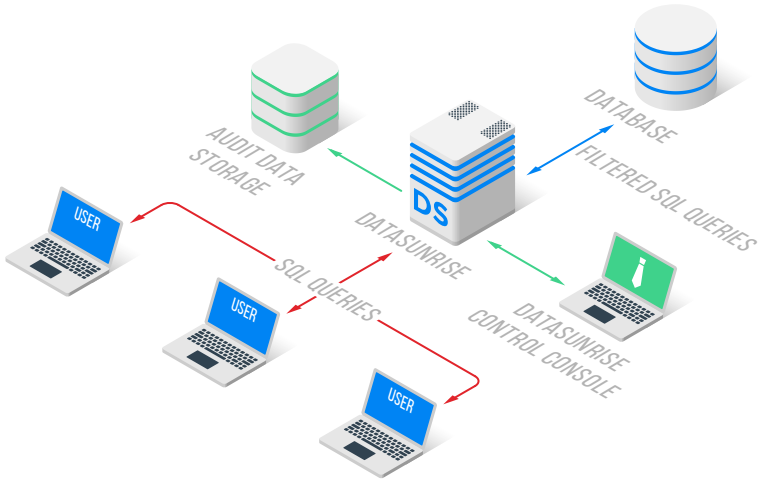
User Behavior

User Behavior enables you to reveal unsuspected database user behavior. This self-learning analyzer considers regular database user behavior as right and secure. If any anomalies are detected, User Behavior provides you with notices and alerts about suspicious activity.

DATASUNRISE DEPLOYMENT TOPOLOGIES

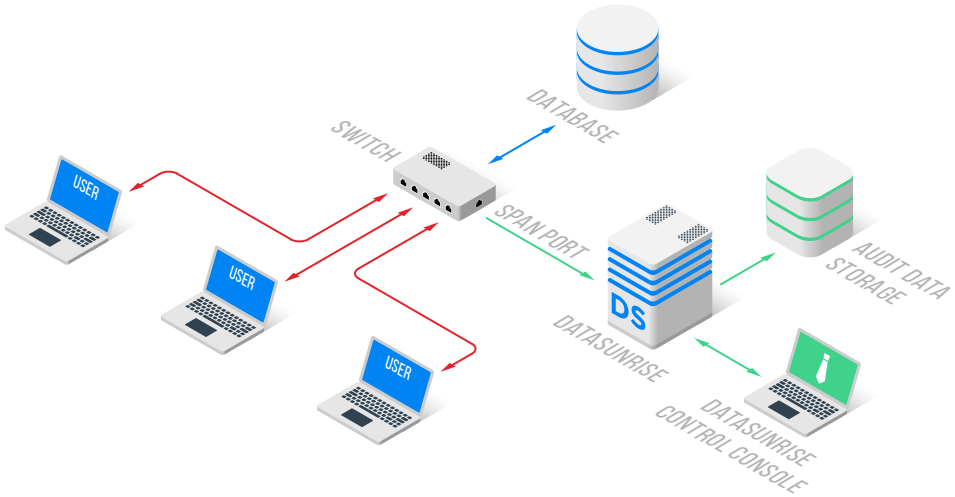
Based on a scenario, DataSunrise can be deployed in Proxy (active) mode, Sniffer (passive) mode, or in Trailing mode (passive) configuration.

Proxy Mode



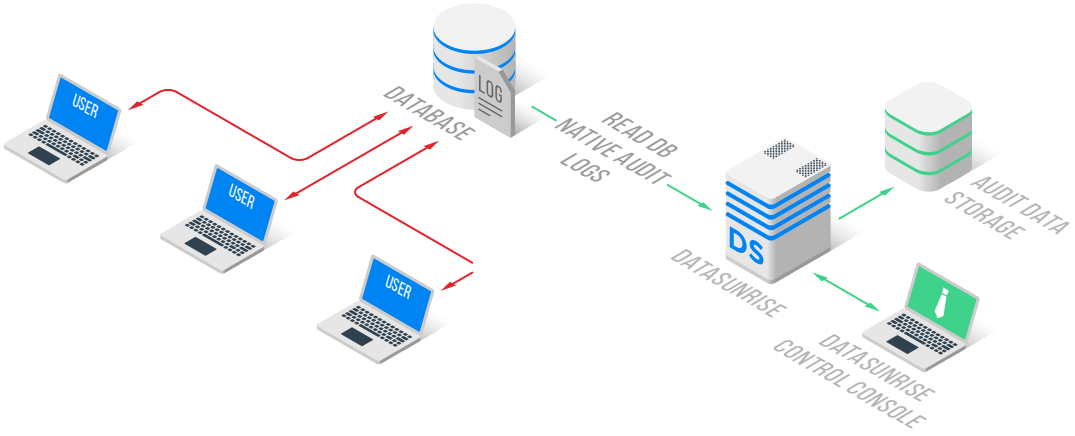
DataSunrise is deployed as a proxy between database clients and database server to disable direct client access to a database. Thus, clients can query database through the proxy only. In this configuration, DataSunrise can perform data protection as well as data masking and auditing, but database response speed is somewhat decreased (not more than 10-15%).

Sniffer Mode



DataSunrise works as a sniffer: it gets mirrored traffic from a SPAN port of a network switch and performs stealth auditing. In this configuration database audit only is available. No database server reconfiguring is required.

Trailing DB Audit Logs



This deployment scheme can be used to perform auditing of Oracle, Snowflake, Neo4J, PostgreSQL-like, AWS S3, MS SQL Server, and MySQL-like databases by the means of native auditing tools.

DataSunrise establishes a connection with the database, downloads the audit data from the database, and passes it to DataSunrise's Audit Storage for further analysis.

BENEFITS

Easy deployment and configuring both with comprehensive Web Console and optional CLI

A broad spectrum of supported platforms in-the-cloud and on-premises

Database audit, database firewall, static, in-place, and dynamic data masking in one suite

Continuous monitoring of all activity in databases and real-time reports via Email or instant messengers

Integration with third-party systems such as SIEM

Prevention of SQL injection attacks, DDOS attacks, and Brute-Force attempts in real-time

Firewall management based on a flexible system of security policies and rules

Intelligent self-learning capability

WHO WE ARE

DataSunrise, Inc. is a private corporation with headquarters in Seattle, Washington. It was founded by a talented team with a strong background in enterprise security, data protection, and database management systems.

Our mission is to deliver first-class software to secure sensitive data around the world. DataSunrise solves the compliance problem for organizations that fight against privacy and security incidents. We are convinced that the best data security software has to be user-friendly and easy-to-use. At the same time, DataSunrise software provides you with the reliable protection of customer data.

DataSunrise team is passionate about our customers' data security, whether it's a large enterprise or a small business. DataSunrise solution protects databases both against external and internal threats, providing real-time traffic and event monitoring, data masking functionality, and deep SQL query analysis. Combine this with easy implementation, intuitive user interface, and extreme performance and you will see why the entire team is proud of the results we deliver.