DataSunrise

DATABASE SECURITY SUITE

WHITE PAPER

CONTENTS

INTRODUCTION

2017 was a monumental year for data breaches, but in 2018-2019 the situation is not getting any better. A big number both of commercial companies and government bodies became victims of hacker attacks.

- 1.1 billion people. Aadhar, the Indian government portal for storing information of its residents and biometric information experienced a leak that gave anyone the access to obtain information from the Aadhar website.

- 340 million people. Exactis, a data broker. A security expert found a vulnerability in the publicly accessed server that exposed detailed information of many US citizens. The information compromised included phone numbers, addresses, and personal preferences of the members.

- 150 million people. MyFitnessPal, a smartphone app and website that tracks diet and exercise. Hackers gained access to user-data through illegitimate ways and got hold of confidential account information including addresses and passwords.

- 100 million people. Quora, a question-and-answer website. A 'malicious' third party gained access to the Quora's system and retrieved account information of user accounts.

- 87 million people. Cambridge Analytica, a British political consulting firm. A Facebook app "This is your digital life" mishandled users information and provided access to third parties including the Cambridge Analytica, a data analytics firm that assisted President Trump in creating targeted ads during his presidential campaign.

- 52.5 million people. GooglePlus, a social network from Google. Wall Street Journal reported that a software glitch caused Google to expose data of over 500,000 users. The company experienced another security breach in November 2018 that compromised data of approximately 52.5 million users. After the recurrent hacking incidents, Google announced that it would shut down Google+ for good by April 2019.

- 40 million people. Chegg, an education technology company. Unauthorized access was gained on the company's database that compromised data of consumers including their name, addresses, and login credentials.

- 29 million people. Facebook, a social networking website. The hackers made use of the vulnerabilities in the Facebook's code and gained full access to user's data that included sensitive information such as user's location, relationship status, devices used and recent searches

- 27 million people. Ticketfly, a ticket distibution service. IsHaKdz, the hacker accessed the website and gained access to information about the clients and promoters that utilized Ticketfly's services.

- 25 million people. AMCA, the American Medical Collection Agency. An 8-K filing with the Securities and Exchange Commission revealed billing services vendor American Medical Collection Agency was hacked for eight months.

These are only some of the most remarkable data breach incidents of 2018 and the first half of 2019.

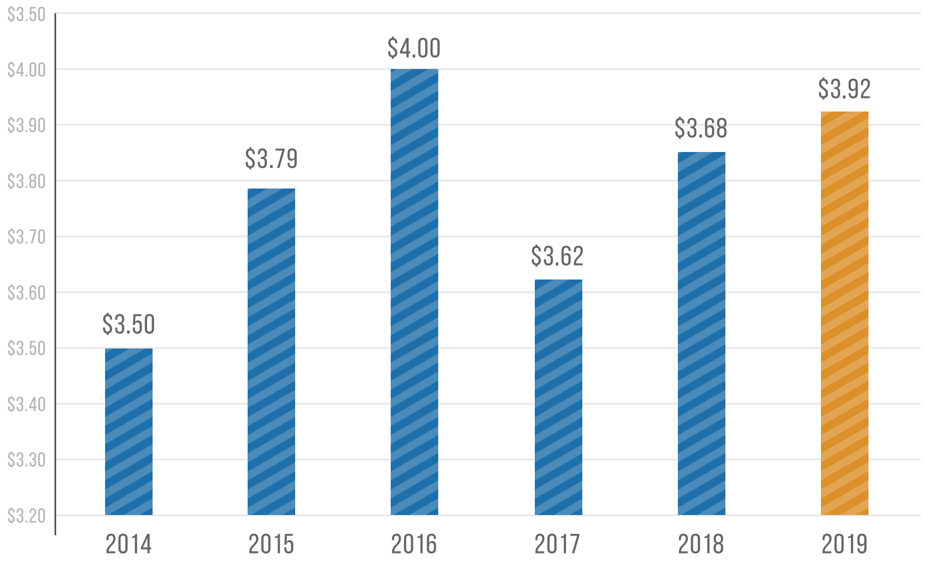
The IBM company reports in its annual study examining the financial impact of data breaches on organizations that the cost of a data breach has risen 12% over the past 5 years and now costs $3.92 million on average. These rising expenses are representative of the multiyear financial impact of breaches, increased regulation and the complex process of resolving criminal attacks.

The financial consequences of a data breach can be particularly acute for small and midsize businesses. In the study, companies with less than 500 employees suffered losses of more than $2.5 million on average – a potentially crippling amount for small businesses, which typically earn $50 million or less in annual revenue.

For the first time this year, the report also examined the longtail financial impact of a data breach, finding that the effects of a data breach are felt for years. While an average of 67% of data breach costs were realized within the first year after a breach, 22% accrued in the second year and another 11% accumulated more than two years after a breach. The longtail costs were higher in the second and third years for organizations in highly-regulated environments, such as healthcare, financial services, energy and pharmaceuticals.

Global average total cost of a data breach

Measured in US$ millions



WHAT YOU NEED TO KNOW ABOUT DATABASE SECURITY

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

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

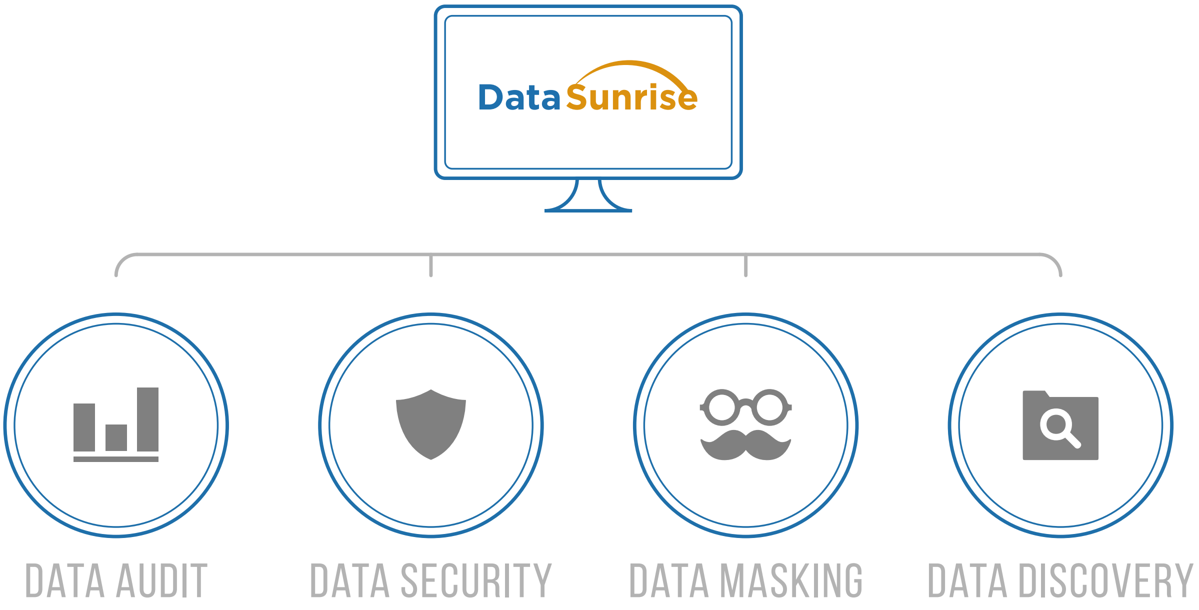
According to statistics, insiders such as employees, contractors and partners are another serious source of data leaks along with hacker attacks. Basically, a sufficient number of data leaks were caused by insiders whether with criminal intentions or just negligent ones. According to breachlevelindex.com web site, 55.42% data breaches of 2018 were caused by hackers, 5.25% breaches — by malicious insiders and 33.62% of incidents were related with accidental loss of information. In 2017, hackers were responsible for 72.63% of data breaches, 8.77% incidents were caused by malicious insiders and 18.25% — related to accidental data loss. In 2018, number of hacker-caused breaches totaled 67.26%, and insider-caused data leaks rate was 9.01% due to criminal-minded insiders and 19.99% due to accidental data loss.

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 potential risk of user privileges misuse and make security system more vulnerable. For instance, hacker can seize control of database user account and increase its access rights level to perform data breach. DBMS-built-in security systems often ignore such incidents because they see nothing suspicious in sudden increase of user access rights and are not able to identify potential threat to database security.

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

WHAT IS DATASUNRISE?

DataSunrise Database Security Suite is data-centric security solution purpose-built for protection of relational database contents against external and insider threats. DataSunrise Suite includes four functional modules: Data Audit, Data Security and Data Masking, Data Discovery.



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 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.

Self-learning

Data Audit component features self-learning capability, the Learning mode. When running in the Learning mode, DataSunrise creates an allow list of queries acceptable in a given database. This list simplifies creation of security policies and prevents the database firewall «misfiring». Except “safe” queries it creates lists of database objects these queries accessed, and database users au-thorized to access these objects.

Data Security

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

DataSunrise 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 both Dynamic and Static Data Masking features.

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 query, modifies it according to existing masking policies and redirects to the database. Having received the modified query, the database provides the original user with obfuscated response.

In most cases data masking is used to prevent insider-driven data leaks during database development and testing procedures. Masking obfuscates 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. Static Masking engine creates a copy of a live database with actual data replaced with fake. At the same time such 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 masking (masking of unstructured data) are included in Dynamic Masking.

In-place masking

In some cases, when you create a copy of your production database to be used by testers or outsourcers but you are not allowed to give access to the actual data the database contains, you could use the In-place masking feature to mask data in the database without creating a copy of this database as Static Masking does. In-place masking utilizes DataSunrise's Static Masking engine. The peculiarity of it is that the database/schema/table to be masked is the target and source at the same time, thus In-place masking replaces the sensitive data with obfuscated values permanently and irreversibly.

Sensitive Data Discovery

This feature enables companies to detect where sensitive and confidential data resides across production databases to ensure on-going compliance and effectively enforce monitoring and security policies.

DataSunrise also includes the Periodic Data Discovery feature which enables administrators to perform sensitive data search automatically on schedule. Data Discovery includes a variety of built-in search filters for almost all kinds of sensitive data types existing.

DSAR

The DSAR feature enables you to search across your databases and get the personal data of interest in compliance with the GDPR and CCPA security standards. This data can be downloaded from the database and displayed as a report.

Compliances

DataSunrise's Compliances feature enables you to search for sensitive data according to international and national security standards and regulations such as HIPAA, PCI DSS, GDPR, SOX, KVKK, CCPA and ISO27001 and to enforce protective means for your production databases according to the aforementioned standards.

Reporting

Data collected by DataSunrise's components can be used for creating custom reports based on PDF or CSV files. Besides that, auditing results can be transferred to external SIEM applications through Syslog.

Vulnerability Assessment

This feature enables you to view all known vulnerabilities for the databases included in your DataSunrise's configuration. The list of vulnerabilities can be downloaded from the DataSunrise web site in the form of a SQLite database file.

User Behavior

This feature enables you to reveal unsuspected database user behavior. The User Behavior Periodic Task uses existing audit data to create an allow list of user activity in the target database.

Table Relations

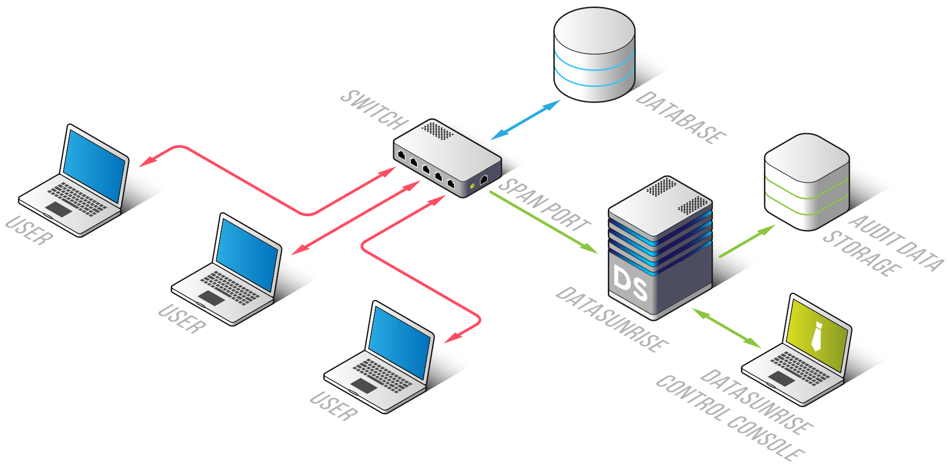
The Table Relations feature enables DataSunrise to analyze database traffic and create associations between database columns. "Associated columns" means that columns can be linked by integrity constraints or by JOIN and WHERE clauses in queries.

Associations can be used when configuring Dynamic and Static Data masking, suggestions on possible associations may be given when selecting the columns to mask. Columns associated with the columns retrieved by Data Discovery tool will be shown too.

DATASUNRISE DEPLOYMENT TOPOLOGIES

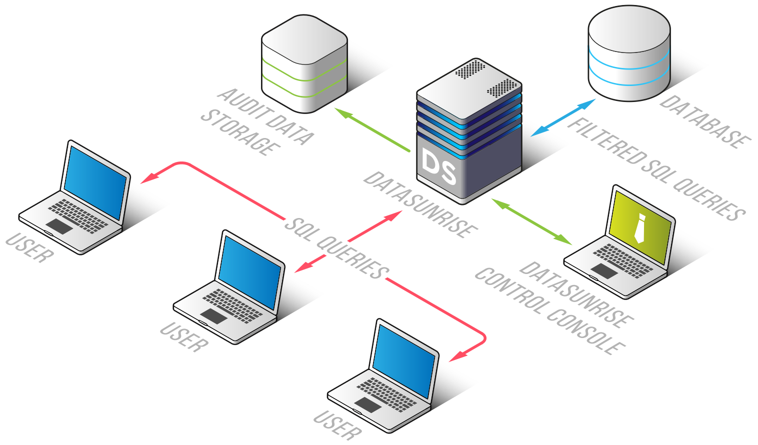
Based on a scenario, DataSunrise can be deployed in Sniffer (passive) mode or in Proxy (active) configuration.

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.

Proxy mode



DataSunrise is deployed as a proxy between database clients and database server to disable direct client access to database. Thus, clients can query database through the firewall 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%).

BENEFITS

- Database audit, database firewall and dynamic data masking in one suite
- Continuous monitoring of all activity in your databases and data warehouses
- Broad spectrum of supported platforms in the cloud and on-premises
- Easy deployment and configuring
- Integration with third-party systems such as SIEM
- Prevention of SQL injection attacks, DDOS attacks and Brute-Force attempts in real time
- Intelligent self-learning capability
- Dynamic data masking on-the-fly across multiple data silos
- Comprehensive Web Console and optional Command Line Interface useful for scripting
- Firewall management based on a flexible system of security policies and Rules
- Real-time reports via Email or instant messengers
- You can create custom Data Masking and Data Discovery scenarios using Lua Script

WHO WE ARE

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

Our mission is to deliver the 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 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 with real-time traffic and event monitoring, data masking functionality and deep SQL query analysis. Couple 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.