DataSunrise

DATABASE SECURITY SUITE

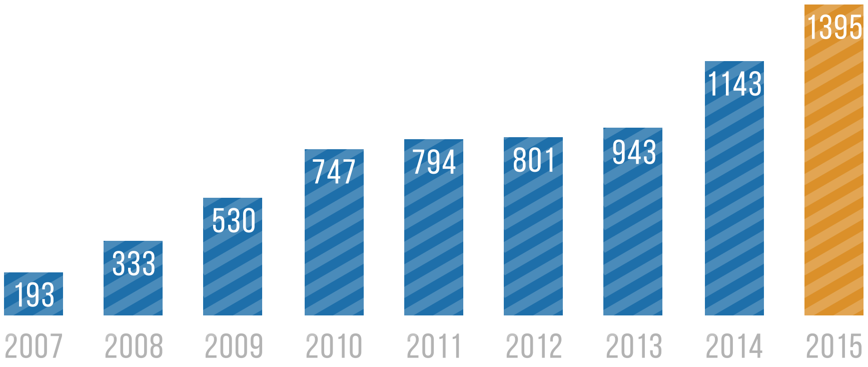
WHITE PAPER

CONTENTS

INTRODUCTION

Many experts characterized 2014 as a Year of the data breach, but in 2015-2016 the situation is not getting any better. A big number both of commercial companies and government bodies became victims of hacker attacks.

- Health insurance company "Anthem" was hit by unknown hackers accessed 80 million clients' records.
- The database of "Ashley Madison" online dating portal was stolen by Impact Team group that published the sensitive data online. Some time later another breach was performed that resulted in 11 million users' credentials stolen.
- Unknown hackers infiltrated hundreds of banks in multiple countries, having stolen around $1 billion. At least 100 banks in 30 countries including Russia, Germany, China and Ukraine were affected by the operation.
- An American hacker hacked personal email of John Brennan, the CIA director, with some sensitive information within.
- Hackers gained access to the database of the Office of Personnel Management and captured personal data of about 22 million federal workers.
- Health-care Centene corporation lost six hard drives that included client's personal health information. It was announced that 950.000 members are potentially impacted by the breach.
- Hackers stole personal information of about 30.000 workers of FBI and Department of Homeland Security.
- A hacker attempted to sell data on the dark web on 167 million Linkedin accounts and 360 million emails and passwords of MySpace users.
- Verizon Enterprise servicers announced that it has become a victim of a hacker attack that affected about 1.5 million of its enterprise customers.



These are only some of the most remarkable data breach incidents of 2015 and first half of 2016.

Researches, conducted by Ponemon Institute, show that data breach cost continues to rise. The average total cost of data breach increased from 3.52 to $3.79 million in 2015 and to 4 $million in 2016. It means 29% increase in total cost since 2013.

Experience shows that the most pricy aspects of data breach are the ones related to client trust regain and new customers acquiring. In the past many companies almost ignored data security means, but today there is growing concern about potential damage to business reputation, class action lawsuits and costly downtime that motivates corporate executives to pay greater attention to their organizations' data security.

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.

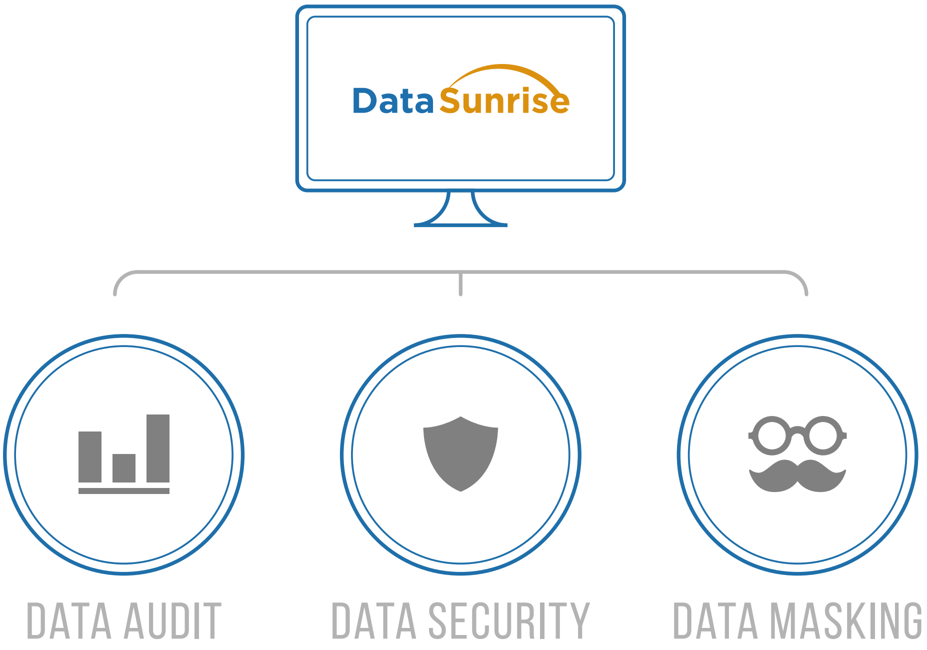
According to statistics, insiders such as employees, contractors and partners are another serious source of data leaks along with hacker attacks. Basically, a sufficient number of data leaks were caused by insiders whether with criminal intentions or just negligent ones. According to breachlevelindex.com web site, 55.15% data breaches of 2013 were caused by hackers, 16.26% breaches — by malicious insiders and 25.28% of incidents were related with accidental loss of information. In 2014, hackers were responsible for 55.04% of data breaches, 16.4% incidents were caused by malicious insiders and 23.93% — related to accidental data loss. In 2015, number of hacker-caused breaches increased (59.19%), but insider-caused data leaks rate somewhat dropped (13.95% due to criminal-minded insiders and 22.81 accidents respectively). First half of 2016 statistics show 69% of malicious outsider attacks, 9% breaches caused by insiders and 18% of accidents related to accidental loss of data.

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 three functional modules: Data Audit, Data Security and Data Masking.



Data Audit (DAM)

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, user name, client application name), session information etc. For maximum efficiency, DataAudit can be paired with a SIEM system to analyze the audit results.

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 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 user names, IP addresses, client applications and queries used.

Data Masking

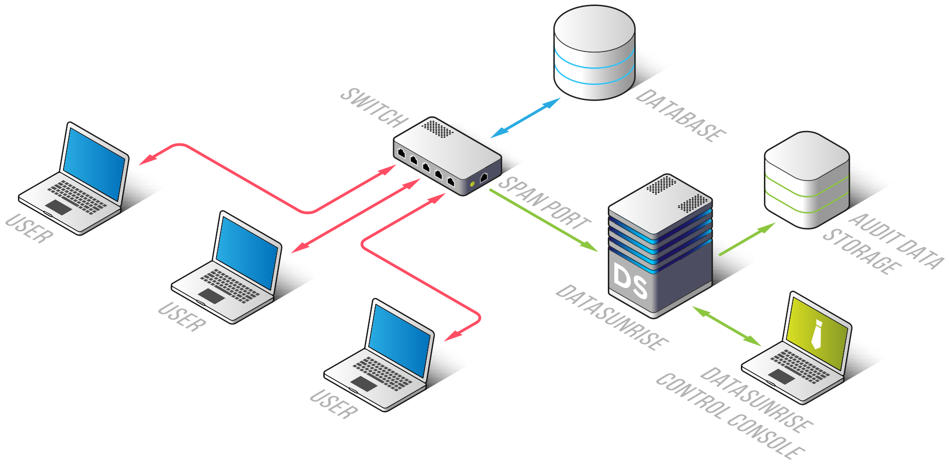
Dynamic Data masking capability enables DataSunrise to limit exposure of sensitive database contents to unauthorized users by obfuscating the query results. DataSunrise intercepts unauthorized user query, modifies it according to existing masking policies and redirects to the database. Having received 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 DEPLOYMENT TOPOLOGIES

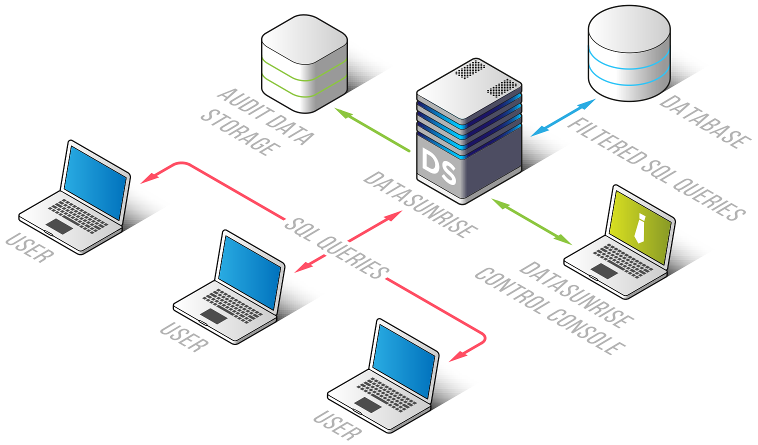
Based on a scenario, DataSunrise can be deployed in Sniffer (passive) mode or in Proxy (active) configuration.

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 databases and data warehouses

Intelligent self-learning capability

Prevention of SQL injection attacks in real time

Dynamic data masking on-the-fly across multiple data silos

Firewall management based on a flexible system of security policies.

Broad spectrum of supported platforms in the cloud and on-premises

Integration with third-party systems such as SIEM

Easy deployment and configuring

Comprehensive web-based GUI

Real-time reports via Email or instant messengers

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 the sensitive data across 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 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 against both external and internal threats, providing with real-time traffic and event monitoring, data masking functionality and deep SQL queries 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.