Data Security

Database Firewalls, Encryption and SIEM Systems

ABSTRACT

Securing your data against unauthorized access and the certainty of data integrity are paramount in dealing with databases and file servers. This whitepaper shows how easy it is to achieve traceability through logging, alerting and blocking of connections. Improper access to files and databases can be prevented by an effective encryption system.

In addition, a SIEM system may combine the logging information from various sources, correlate them and provide a greater view onto threat scenarios.

CONTACT

SPHINX IT CONSULTING GMBH | ASPERNBRÜCKENGASSE 2 | 1020 WIEN

TEL: +43 1 599 31 - 0 | office@sphinx.at

sphinx
MASTERING THE GAP

How to ensure Data Security?

Data security must be viewed at different technical levels:
- Access protection (logical / physical)
- Data integrity
- Availability, in the sense of High Availability and Disaster Recovery

This White Paper focuses on data integrity and the protection of data against unauthorized access. Availability is not covered here.

Various security mechanisms, from SQL / Filesystem Access Security through to Network and Application Security, form a multi-layer implementation, which protects against different threats and types of access. Furthermore, it is also important to implement organizational procedures, including awareness raising and training for end-users.

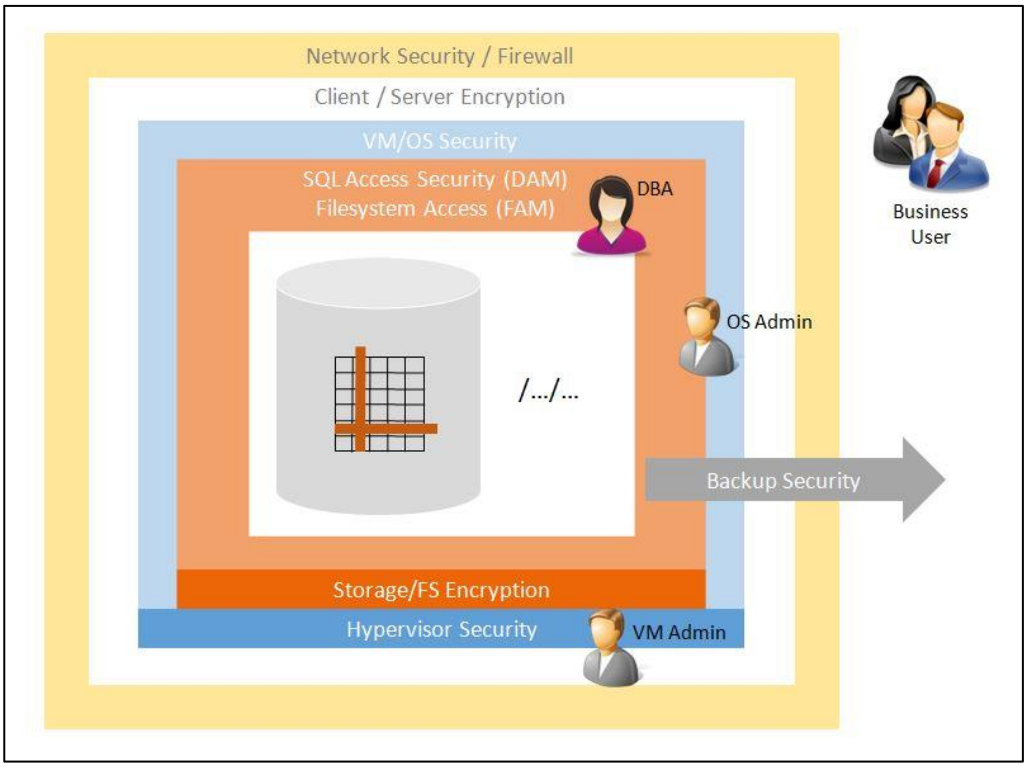

Figure 1: Security layers

In principle, access rights should be tight and data should be moved as infrequently as possible. The closer the data gets to the user, the smaller the data volume should be. This is achieved by using the functionality applicable at each level (database, network, application server, application program, etc.).

The result is a multi-layered filter, which increasingly reduces the data stream. The user only sees what he really needs. Copying all data to the client and then applying filters is problematic and is no longer state of the art.

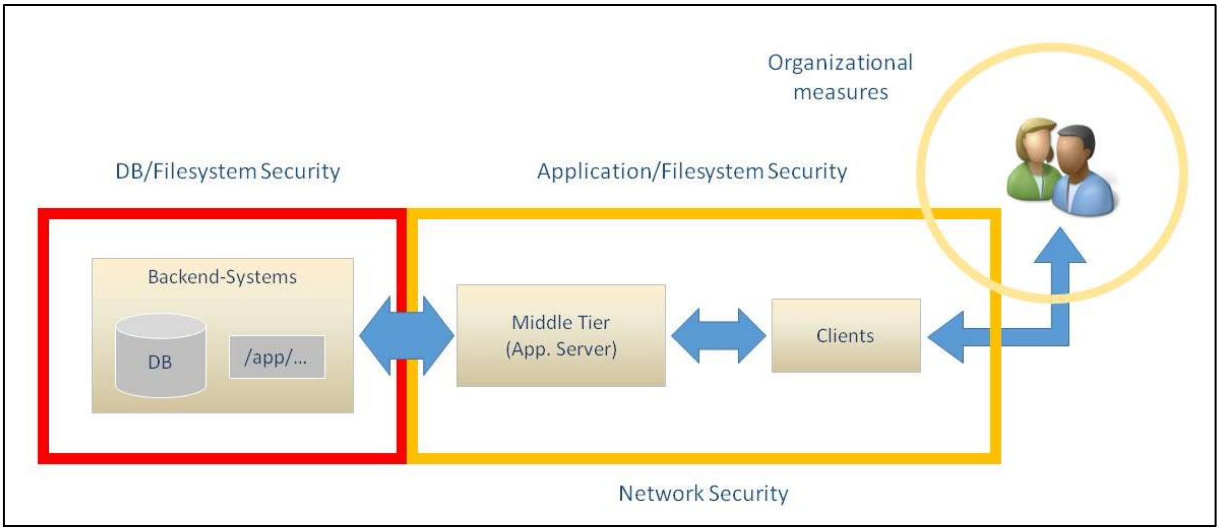

Figure 2: Data stream reduction

Security in databases:
For databases, there are two levels that must be considered:
- Protection against access via the SQL interface
- protection against access to the physical files, i.e. via the file system, avoiding the database mechanisms

In order to achieve traceability, the logging of access to data is imperative. Alerting and blocking are also enabled at this level.

Each database system has its own resources to ensure access protection and logging. These often have certain limitations:

- Dealing with super-users (both internal DB and operating system, such as "root"-user
- Logging performance ("Auditing")
- Immutability of the logging data ("Audit Trails")
- Separation of duties, including logging

To overcome these limitations this paper presents two cross-platform tools, which are described in more detail below:
IBM Security Guardium Database and File Activity Monitor (DAM/FAM)
IBM Security Guardium Data Encryption (GDE)

A SIEM (Security Information & Event Management) system like **IBM QRadar** is recommended to support a holistic view. It combines logging data from various sources, including IBM Guardium DAM/FAM and GDE, and others. It therefore provides a central point for further correlations, forensics, alerting and vulnerability assessments.

IBM Security Guardium Database and File Activity Monitor

Database access via SQL commands and file system I/O can be logged using the IBM Security Guardium Database and File Activity Monitor (short: Guardium DAM / FAM). It is manufacturer-independent and provides fine-grained control. For certain type of access there is the possibility to define real-time alerts that are generated and sent immediately. Alerts can also be generated if, for example, "normal" statements suddenly occur at abnormal frequency.
Finally, access to database and file systems can be blocked, if necessary.

Guardium DAM/FAM protects against internal and external threats, and automates compliance control. It reacts dynamically and in real-time to a broad range of situations. Logging can be selectively deactivated depending upon user/user-groups, environment variables, SQL-statements, target systems and other criteria. Furthermore, it is possible to set various granularity-levels, create alerts immediately or blocks connections. Users can even be sent into quarantine-mode to temporarily prohibit log-ins.

The rules controlling all these actions are defined and stored on a central server using a Web-GUI. The S-TAP agents execute the rules on those systems which are to be monitored. The architecture supports a single Guardium server as well as highly available, multi-level configurations.

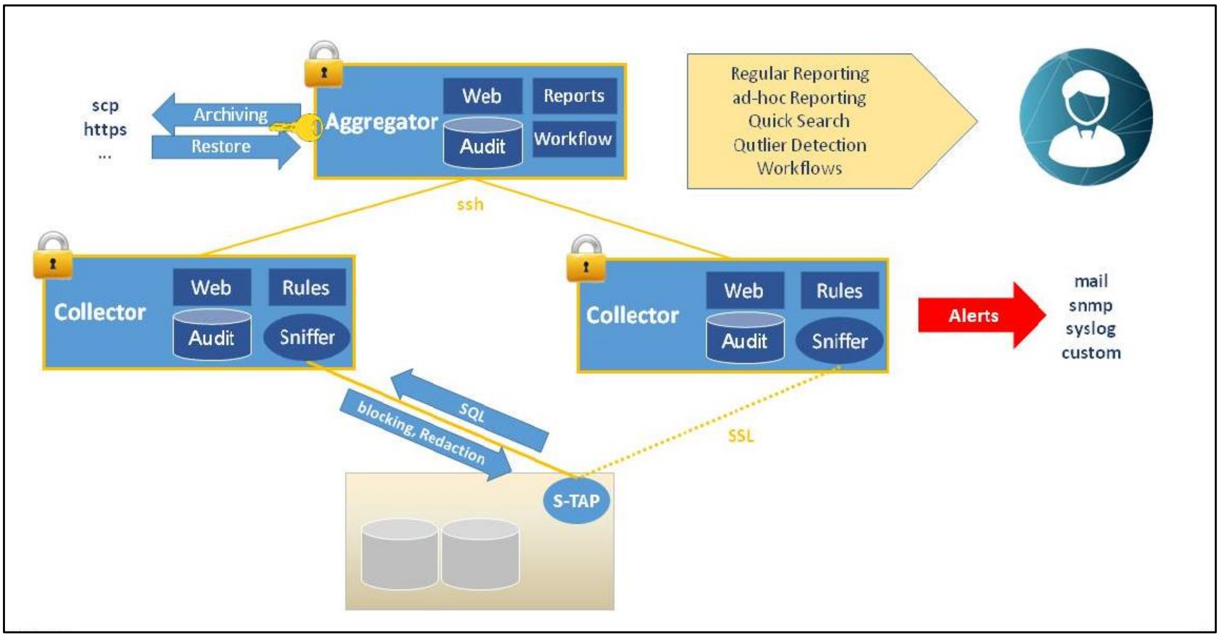

Figure 3: Guardium components

Comprehensive reporting is available to analyze logging data. An unusual accumulation of otherwise harmless events over a certain timeframe can easily be detected. First-time log-ins can be singled out and handed over to an approval process which adds them to white- or black-lists. For one-time reports, which are not preconfigured, a Quick-Search function allows ad-hoc viewing of log files.

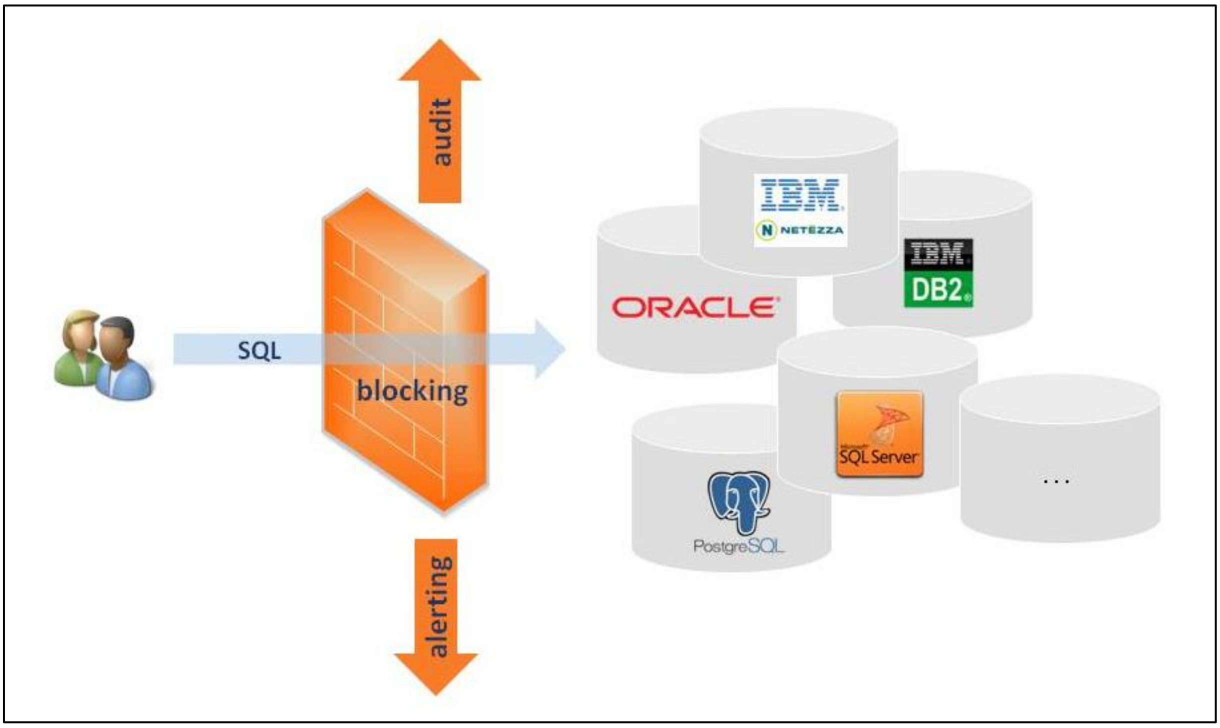

Figure 4: Database firewall

Super-users are also included in these mechanisms without any restrictions. The existing access rights in the database and / or filesystem are supplemented by the rights defined in Guardium DAM / FAM.

By implementing an agent as a kernel module ("S-TAP"), bypassing these mechanisms is almost impossible. It is impossible even for super-users (root, or database administrators such as SYS, DB2INST1, Administrator, etc.). Nothing remains undetected.

All logging information is stored inside a secured database to ensure immutability, and can be forwarded to other systems. IBM QRadar SIEM is the natural companion to use in such a case.
IBM Guardium DAM / FAM provides for a separation of responsibilities, with two administrator levels, as well as the ability to assign individual roles.

IBM Security Guardium Data Encryption

Data encryption has to meet the criteria of transparency, operational efficiency and universality. Day-to-day operation must be performance-optimized, and key management must be easy to handle. IBM Security Guardium Data Encryption (abbreviation: IBM GDE) fulfills these criteria.

IBM GDE implements a 2-tier approach to key management. A "Data Encryption Key" (DEK) encrypts the data and is itself encrypted by the "Key Encryption Key" (KEK), and therefore protected (in the picture below, the "eDEK"). This allows simple key rotation and cryptographic deletion by destroying the key encryption key. In operation the Data Encryption Key is also hidden from the administrator.

During normal operation the host, e.g. a database machine, stores the key in (kernel) memory. Only when the machine is started is the key queried by the IBM GDE server. A connection between the IBM GDE server and encrypted hosts is therefore only necessary when starting the host, or when a key refresh occurs.

The IBM GDE server has a fail-safe configuration, which implements the same functionality in all instances of the GDE server. Administrative changes can only be performed on the primary GDE server. These changes are then immediately replicated to the secondary servers. Each server can individually be defined as a "primary contact" for encrypted hosts.

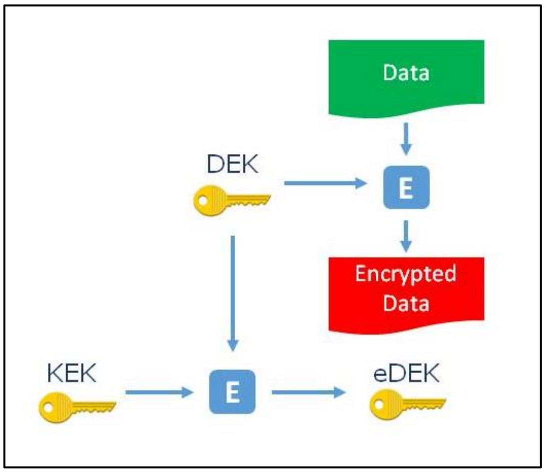

Figure 5: GDE Key Management

In GDE encryption is performed by an agent, which is implemented as a kernel module in the file system driver. This provides complete transparency for the application programs, e.g. databases. Due to the efficient implementation, there is practically no performance degradation due to encryption.

The permissions defined in IBM GDE are, once again, applied in addition to the existing permissions in the file system. Even the root user can be blocked from certain areas. The granularity is very finely adjustable, starting at individual files. This also includes directories, directory trees, or even the entire file system. Authorizations can be assigned to users, processes, time-periods, or combinations thereof.

A separation of responsibilities is, of course, also implemented. There are three levels of administrator. If it becomes necessary to import a configuration, or a key, a separate key is necessary. This key can be split into fractions ("Key Shares"), more than one of which is needed to decrypt a backup. Example: 10 people are assigned a "key share", at least three key shares are needed to “open” the backup.

IBM Security QRadar SIEM

QRadar SIEM offers multiple modules to combine and correlate information from various sources. Log data from devices and programs are read, stored and normalized. In addition, network packets are also analyzed. Combined, these are used to show events, which may be classified as attacks based on defined rules. These attacks are correlated with assets, which are a part of the network, therefore highlighting any risks. This analysis helps to circumvent future attacks and their associated risks.

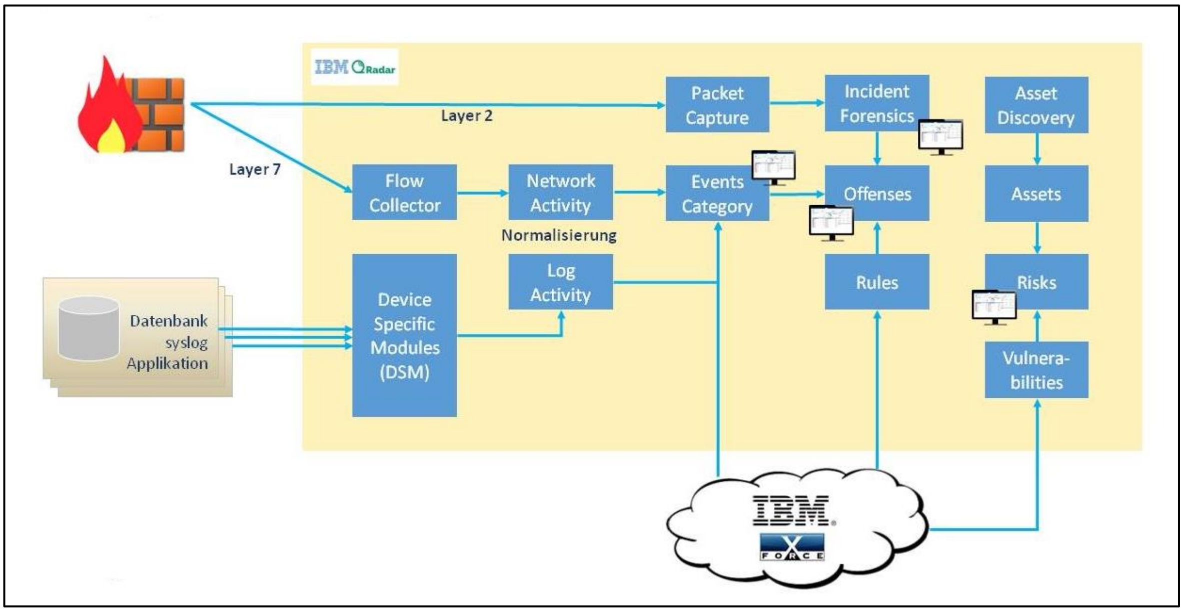

Figure 6: QRadar architecture

Log Management: Various sources of log data (syslog, LEEF, device specific, …) are received, stored and normalized. Information from different sources can therefore be combined and correlated.

Security Intelligence: IBM X-Force data is used to regularly update a local QRadar installation, keeping it up-to-date and enabling it to always recognize the latest threats.

Network Activity Monitoring: Using a network switch's mirror port the complete network traffic is captured, stored and normalized, similar to the logging data.

Risk Management: Based on the captured network traffic, and the information about network devices, an automatic risk assessment can be carried out.

Vulnerability Management: QRadar supports IT-Security officers with their vulnerability management. It combines information about devices, therefore minimizing risks.

Network Forensics: Pattern recognition and protocol abnormalities are searched for. Impending attacks can therefore be identified.

Event Correlation: Events that are recorded through various information channels (log data, network traffic) can be correlated to find threats which may compromise network integrity.

Alert Management: Alerts are created based upon rules which analyze log data and network traffic. These rules are either predefined or customized to best reflect the customer's environment.

The complete Architecture

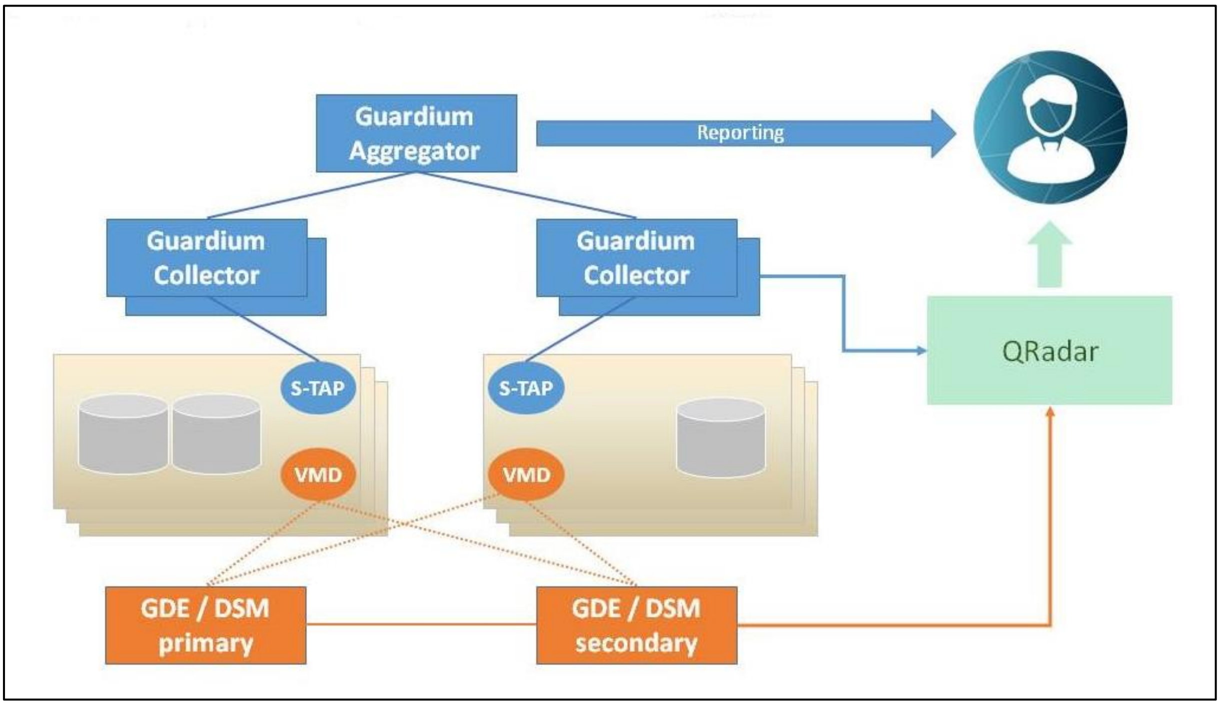

Figure 7: Overall architecture

IBM Security Guardium Database and File Activity Monitor (blue items), IBM Security Guardium Data Encryption (orange items) and IBM Security QRadar SIEM (green item) provide excellent security for your data.

Conclusion

Securing your data against unauthorized access, and the certainty of data integrity, are paramount in dealing with databases and file servers. IBM Security Guardium Database and File Activity Monitoring allows traceability based upon its logging capabilities. Comprehensive reporting helps to identify threats. Alerts may automatically cause log-in blocking.

IBM Security Guardium Data Encryption helps to prevent unauthorized access to data. Its slim implementation ensures minimal overhead.

Both tools are managed via a simple, yet comprehensive, Web-GUI, which is used to define the rules which control access permissions.

Additionally, a SIEM system combines the logging information from various sources, correlates them, and provides a clearer view of threat scenarios. IBM QRadar SIEM combines analysis of network flows from various log sources, of which Guardium may be one. Potential vulnerabilities or threats can therefore be identified and remedies are proposed accordingly.