DATA SHEET

McAfee Data Center Security Suite for Databases

Defend your most valuable data assets

PRODUCT OVERVIEW

McAfee® Database Security is an easy-to-deploy and highly scalable software solution that monitors the Database Management System (DBMS) and protects it from internal and external threats and even intra database exploits.

McAfee Database Security Suite for database includes the following products:

- **McAfee® Database Activity Monitoring (McAfee DAM)** — Protects data from all threats by monitoring activity locally on each database server and by alerting or terminating malicious behavior in real time, even when running in virtualized or cloud computing environments.
- **McAfee® Virtual Patching** — Detects missing patches, applies vulnerability-specific countermeasures and fixes misconfigurations (via McAfee Database Security virtual patching technology) found by vulnerability scans to improve the security posture of databases immediately, without requiring any downtime.
- **McAfee® Vulnerability Manager for Databases** — Automatically discovers databases on the network, determines if the latest patches have been applied, and tests for vulnerabilities, such as weak passwords, default accounts, and other common threats. In addition, it allows for detailed data discovery scans, including PII, PCI-DSS, SOX, and HIPPA.

Note: Product features depend on the product version. When a function is unavailable in the version you are using, the User Interface informs you that a different license is required to enable the feature.

Key features

McAfee Database Security provides full visibility into DBMS user activity and can issue alerts or terminate suspicious activities based on predefined vPatch rules and custom rules.

In line with the layered defense strategy employed by leading enterprises, McAfee Database Security complements other security measures, such as encryption, network security, and other tools, by providing a hardened security layer surrounding the DBMS itself.

The key advantages of McAfee Database Security include:

- Monitoring of all DBMS activities, including the activities of authorized and privileged users
- Prevention of intrusion, data theft, and other attacks on the DBMS
- Real SQL Injection Protection
- Rule-based policies for users, queries, and DBMS objects
- Quarantine rogue users
- Enterprise level vulnerability assessment for DBMSs
- Quick and easy deployment and configuration

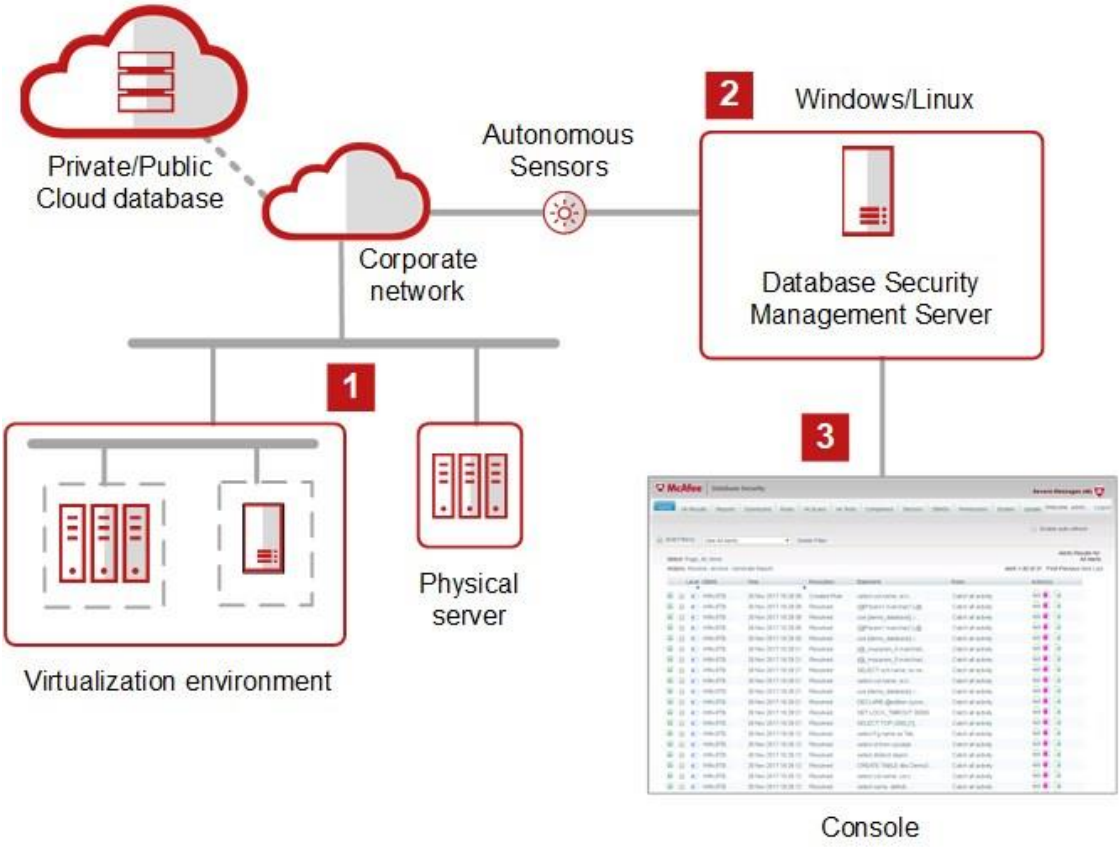
How it works

McAfee Database Security Suite for databases offers real-time protection for databases from all types of threats, external, internal, and even intra database exploits.

McAfee Database Security is ideal for servers operating in a physical or virtualized environment, on premises, or in the cloud.

1. The McAfee Database Security sensor enables the monitoring of local and network access to DBMSs in real time. The sensor operates safely in operating system (OS) user-space, and can either run on the machine hosting the DBMS or on a separate dedicated system, depending on the selected configuration.
2. The McAfee Database Security server is a J2EE server that communicates with all the installed sensors. It can run on a dedicated physical machine or a dedicated virtual machine.
3. The web console is the interface in which the administrator can monitor and manage all Database Security products.

The McAfee Database Security sensor monitors access to the DBMS and sends transaction data to the McAfee Database Security server. Based on the policies defined using the McAfee Database Security Web Console, the server logs the transaction, issues an alert, and prevents access to the DBMS.


Private/Public
Cloud database
Autonomous
Sensors
2
Windows/Linux
Corporate
network
Database Security
Management Server
1
3
Physical
server
Virtualization environment
Console

Feature	Advantage	Customer Benefits
Software Solution (no appliance required)	McAfee Database Security eliminates the need for expensive appliances.	• Allows customers to quickly and easily deploy the solution without the need for an additional, and often expensive, appliance
Superior Technology – SC Magazine Award for 2 years in a row	Advanced memory analysis for deep insight into transactions together with network sniffing and other methods Autonomous Agents enforce policies even when there is no connection to the server	• Gives customers greater insight into their database activities through unique memory analysis
Cloud Ready	Due to its client server architecture, McAfee Database Security is cloud ready.	• Allows customers to be more flexible on where their database infrastructure is located (local datacenter, private cloud or public cloud)
No Downtime	Non-intrusive during installation; no restart of the database or the database server is required	• Increases operational availability for mission critical databases where downtime is undesirable and can lead to revenue loss
Large Deployment Support	Simple policy management and assignment	• Drastically reduces planning and deployment times, required manpower and hardware. Lowers total cost of ownership and offers faster readiness
Vulnerability Assessment	McAfee Database Security Vulnerability Manager has over 6000 vulnerability tests which is by far the largest set in the industry.	• Being able to scan for vulnerabilities, misconfigured databases, sensitive data and much more right from the get go, helps customers harden their databases and secure their sensitive data much faster and more efficiently
Database Activity Monitoring (DAM)	McAfee Database Activity Monitoring uses unique memory monitoring together with network traffic monitoring to provide a 360 view of database activity.	• Offers full visibility into database activity, including network, local and internal activity, without any black spots. Customers can even see obfuscated statements as well as accessed objects and execution plan

The Database Activity Monitoring Sensor can be installed on the following operating systems;

Platform	Operating system version support (as per internal validation)
Windows	Microsoft Windows 2003 Microsoft Windows 2008 Microsoft Windows 2008 R2 Microsoft Windows 2012 Microsoft Windows 2012 R2 Microsoft Windows 2016 Microsoft Windows 2019
Linux	CentOS 5.5 and greater, 6.x, 7.x RedHat 5.5 and greater, 6.x, 7.x RedHat 8.x (4.8.4 and greater for pre-selected Postgres versions only) SUSE Linux 10, 11, 12, 15 Debian 10
Solaris Intel	Sun OS 5.10 Sun OS 5.11
Solaris Sparc	Sun OS 5.10 Sun OS 5.11
AIX	AIX 7.1 AIX 7.2 only for: • Sensor 4.8.3 and newer for Oracle • Sensor 4.8.4 and newer for DB2 11.5.4.0 and newer
HPUX	HPUX 11.31

Supported DBMS

- Microsoft SQL Server
- Oracle
- Sybase
- DB2
- SAP HANA
- MongoDB
- MySQL
- MariaDB
- Percona
- PostgreSQL
- Teradata

Minimum system requirements

McAfee Database Security Suite system requirements

Data repository

Acceptable data repositories for McAfee DBS include:
Microsoft SQL Server 2016 up to 2017 64-bit Standard Editions or higher

Memory

24 -128 GB (24 GB+ recommended)

Processor

x64 Processor 2.0 GHz+
8+ cores (Standard)

Disk Space

Standard: 500+ GB for temp/output/data repository

Operating Systems

Windows Server 2016 or Windows Server 2019
64-bit Standard Editions or higher

Browser

Firefox v53 and later
Chrome v56 and later
Microsoft Internet Explorer 11.0 and later

Account Rights and Privileges

A Local or Domain Administrative account is required for installation

Port considerations

McAfee DBS components communicate on the network ports listed below;
Console Port 8443 TCP
Sensor Port 1996 TCP