WHITE PAPER

McAfee
Together is power.

Protecting McAfee ePolicy Orchestrator Database with McAfee Database Security

Protecting McAfee ePolicy Orchestrator Database with McAfee Database Security

Authors

This white paper was written by:

- Markus Strauss, McAfee, Inc.
- Raj Dhesi, McAfee LLC

In today's enterprises, databases house some of the most sensitive, tightly regulated and valuable data—the very data that is sought after by malicious insiders and external attackers. Any database that stores sensitive information (customer, intellectual property, infrastructure, and security data) requires protection. The database of McAfee ePO software (Microsoft SQL Server or Microsoft SQL Server Express) is no exception.

This white paper is for security administrators and database administrators responsible for managing McAfee® ePolicy Orchestrator® (McAfee ePO™) software. The paper covers current threats, reasons why having specific security for McAfee ePO software is important and how McAfee Database Security addresses these points. The white paper also provides an overview of McAfee Database Security Activity Monitoring and highlights specific policy requirements to secure McAfee ePO software.

McAfee ePolicy Orchestrator Database and Sensitive Data

McAfee ePO software is a centralized management console used for McAfee security solutions. It is a powerful infrastructure that allows the customer to manage large and complex networks, deploy software and software updates, define policies, and meet reporting requirements. This is only possible if McAfee ePO software can access sensitive information about the infrastructure, policies, and other settings and store these in its own database.

Why Is Protecting the McAfee ePolicy Orchestrator Database So Important?

Let's assume for a moment that an attacker succeeds in accessing the McAfee ePO software database. The attacker could find out the user name and even the password of an existing McAfee ePO database user. The use of any of the freely available database management tools would then give the attacker access to the database, with no challenges from any of the conventional security measures in place.

Now that the attacker has access, modifying the security settings is easy. For example, the following activities are all possible:

- Disabling the antivirus policy for a workstation
- Uninstalling the McAfee agent on one or more systems
- Retrieving sensitive information based on events
- Modifying an email address to get copies of mails sent out by McAfee ePO software
- Creating a new McAfee ePO software user with administrative privileges

At this point, McAfee ePO software has no knowledge of the changes and no entries or evidence will appear in McAfee ePO software user logs. If the attacker is careful and the changes are consistent with the data model, no one would notice the changes.

Securing the McAfee ePolicy Orchestrator Database

McAfee Database Activity Monitoring is the best way to keep attackers out of the McAfee ePO database and to protect the sensitive information in the database.

With McAfee Database Activity Monitoring, an additional agent (the sensor) is installed on the McAfee ePO server or the database server, where the McAfee ePO database resides. This sensor is managed by McAfee ePO software and monitors access to the database. As part of this monitoring, all SQL statements are checked against assigned monitoring policies prior to execution on the database. When access is attempted (via a SQL statement, for example), McAfee Database Activity Monitoring uses its unique in-memory scanning to match conditions defined within the policy.

Actions and alerts can be created based on these policies.

For example:

- A notification is sent by McAfee ePO software
- An alert is generated
- The database session is terminated (optional)

How McAfee Database Activity Monitoring Works

The idea behind McAfee Database Activity Monitoring is to not only have a valid audit log to capture any access to the database, but to also differentiate between **good** access and **bad** access. Being able to differentiate between the two is extremely important because this is what enables powerful policies and access control.

Example: A SQL statement is good when:

- It comes from the correct application (McAfee ePO software).
- It comes from the correct IP address.
- It is issued by the correct database user.
- It is issued by the correct operating systems (OS) user.
- It comes from the correct database host.

Any other access to the database is considered bad access. This pushes the integrity of the McAfee ePO database to the highest possible level.

Implementing McAfee Database Activity Monitoring in McAfee ePolicy Orchestrator

To implement McAfee Database Activity Monitoring in McAfee ePO software, search for the Database Security extension in the McAfee ePO software manager. Check in, and install the extension. A 30-day free trial is available.

- Deploy the sensor on the server where the McAfee ePO database is running. Once detected, the McAfee ePO database instance will be added to the system tree.
- Download and import the McAfee ePO Database Protection policy, and follow the instructions in the package.
- Customize the McAfee ePO Database Protection policy as needed.

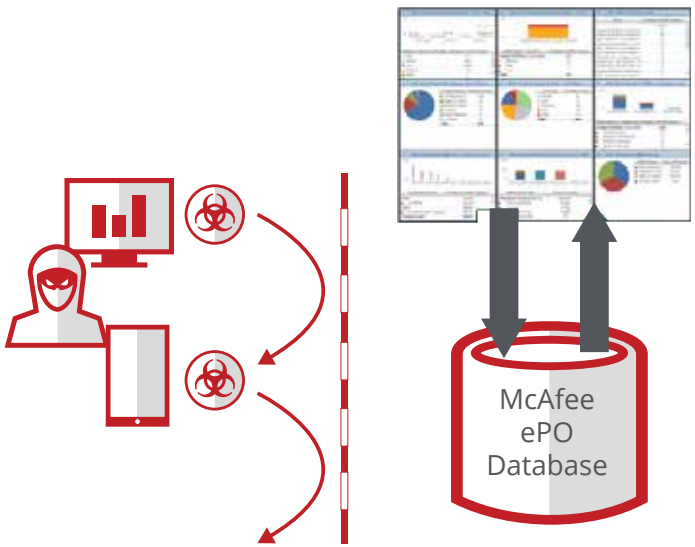

Figure 1. Attack on McAfee ePO software is successfully prevented.

Figure 2. The McAfee ePO policy package on the McAfee download page.

All packages (including McAfee ePO software-specific policies) can also be downloaded via the official McAfee download page: **McAfee Download Page**.

Have Questions? Looking for more information on how McAfee Database Security works? Visit the **McAfee Database Security page** and the **McAfee Community page**.

More Information: McAfee Database Security on McAfee ePO

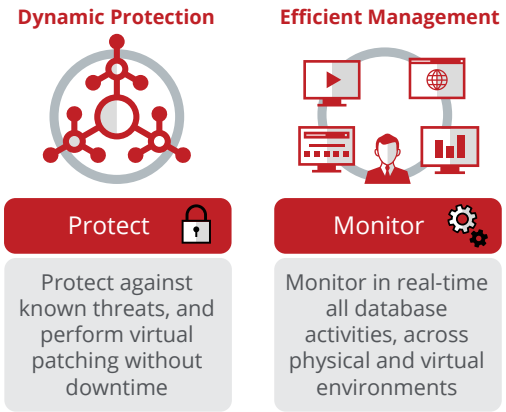

Figure 3. McAfee Database Activity Monitoring and McAfee Virtual Patching for Databases.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring automatically finds databases on the network, protects them with a set of preconfigured defenses, and helps build a custom security policy for the database environment—making it easier to demonstrate compliance to auditors and improve critical asset data protection. McAfee Database Activity Monitoring cost effectively 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.

Key Features

- Provides protection against all database threat vectors to meet compliance requirements
- Identifies threats as they occur and intervenes to stop attacks—reducing risk and liability
- Provides flexible reporting, including preconfigured templates for PCI DSS, SOX, and HIPAA—all viewable within McAfee ePO software
- Deploys quickly and nonintrusively, with minimal resources
  - Protects databases running on today's modern IT infrastructure, including virtualized and cloud environments
  - Provides security in an easy-to-use form factor—downloadable software (not an appliance)

McAfee Virtual Patching for Databases

McAfee Virtual Patching for Databases shields databases from risks presented by unpatched vulnerabilities by detecting and preventing attacks and intrusions in real time without requiring database downtime or application testing. McAfee Virtual Patching for Databases helps organizations effectively meet compliance requirements that call for critical databases to be protected and kept at required patch levels while allowing production to continue uninterrupted.

- **Patch protection during crucial periods:** Guard databases during the window of risk that covers the time between the issuance of a vendor's critical patch update and when the patch is actually installed.
- **Seamless update design:** Continuous flow of automatic updates keeps the security status of systems current and permits organizations to focus on production considerations.
- **Coverage that helps meet compliance requirements:** Meets standards such as HIPAA, PCI DSS, SOX, and internal corporate governance policies through patching protection.

Key Features

- Provides real-time protection for databases that do not have vendor patch updates installed but have known vulnerabilities that can be exploited by hackers
- Deploys easily and does not require customization or specific database management system (DBMS) knowledge
- Covers a broad array of DBMSs and protects versions no longer supported by the vendor
- Provides security in an easy-to-use form factor: downloadable software

Did You Know?

McAfee Virtual Patching for Databases (vPatch) is an integral part of McAfee Database Activity Monitoring and is included when installing the McAfee Database Security extension in McAfee ePO software. No additional license is required.

Glossary

Good database access	For this document, any authorized, non-malicious connection
Bad database access	For this document, any unauthorized and/or malicious connection
Health Insurance Portability and Accountability Act (HIPAA)	Healthcare regulation—more information is available at: http://www.onlinetech.com/resources/references/what-is-hipaa-compliance
Payment Card Industry Data Security Standard (PCI DSS)	Payment Card Industry regulation—more information is available at: https://www.pcicomplianceguide.org/pci-faqs-2/#1
Sarbanes–Oxley (SOX)	Sarbanes Oxley compliance—more information is available at: https://digitalguardian.com/blog/what-sox-compliance

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com