

McAfee Enterccept Database Edition

Intrusion Prevention for Database Servers

The Challenge

The number of new vulnerabilities and the speed and sophistication of attacks seeking to exploit those vulnerabilities increase every year, intensifying the risks to enterprise security. The evolution of new hybrid attacks that use multiple vectors to breach the security infrastructure means that enterprises must defend themselves against a constantly shifting threat.

Database servers present unique security challenges—real-time access to the information that resides on database servers helps improve business performance for enterprise customers, employees, and partners. However, increased access also means increased risk of compromise.

Unfortunately, traditional host IDS tools are reactive and always one step behind an attack. To ensure comprehensive, proactive security, enterprises need to adopt a layered approach to security that delivers overlapping and complementary technologies that protect networks and systems from the edge to the core. McAfee® Intrusion Prevention delivers the most comprehensive, accurate, and scalable threat protection solutions available, helping enterprises mitigate risk, ensure business availability, and reduce total cost of ownership.

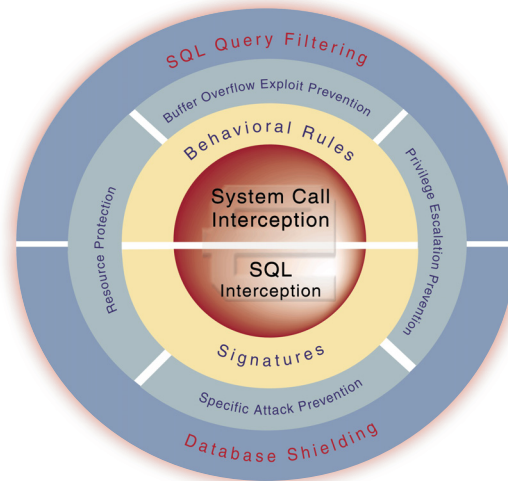
The McAfee Enterccept Solution

McAfee Enterccept® Database Edition gives enterprises running Microsoft® SQL Server 2000, a proven, easy-to-deploy method to protect assets and preserve database integrity. Building upon the patented protection of Enterccept Standard Edition, the Database Edition offers broader defense against database-specific threats, including very popular SQL Injection attacks. Enterccept is the only intrusion prevention solution to create application-specific content interception engines and rules. Each Database Edition agent evaluates SQL requests before being processed. It applies a powerful combination of behavioral rules and signatures to detect and block both known and *zero-day* attacks before they can succeed.

Benefits

Comprehensive

- IPS, plus firewall protection, ensures availability of mission-critical applications by blocking known and unknown attacks
- Reduces criticality of patch deployment for new vulnerabilities and exploits
- Protects integrity and privacy of confidential data by preventing database compromise



SQL query filtering and database shielding, combined with OS protection, defends databases from both known and unknown attacks.

Accurate

- Unique combination of behavioral rules and signatures protects against *zero-day* attacks like buffer overflow exploits
- Process firewall enforces policies with granular packet filter and application layer firewall
- Preconfigured, customizable rules and signatures reduce false positives thus freeing up valuable security staff

Scalable

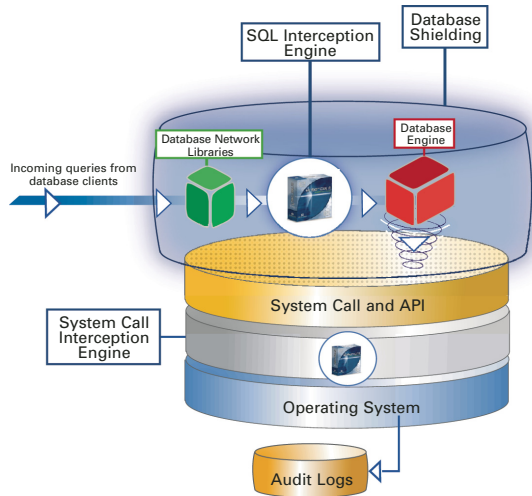
- Configure and manage thousands of agents with a single management server
- Silent install/update with no reboot required
- Optional agent deployment and monitoring via McAfee ePolicy Orchestrator® 3.5 (Q3 2004)
- Customizable levels of protection, from logging to blocking

How Enterccept Database Edition Works

Each centrally managed Database Edition agent ships with fully configured default policy templates for protection out of the box. The agent also contains powerful customization features, which allow organizations to create custom policies and tune them for their unique environments to further reduce false positives. Agents automatically retrieve encrypted and authenticated updates from the management system.

The SQL Interception engine analyzes all incoming database queries for buffer overflow conditions, SQL injection attempts, and abnormal manipulation of the database.

The Database Edition agent matches calls against the appropriate behavioral rules and known attack signatures and blocks any queries that attempt malicious behavior or match any specific attack signatures.



McAfee Enterecept's unique SQL Interception Engine integrates directly into the database application and intercepts malicious behavior, thus preventing intrusions.

Features

SQL Injection Protection—Attackers can gain access to restricted data such as credit card numbers or patient records, alter data, and even attack other computers on the network by entering malicious SQL statements into a vulnerable application's data fields. Database Edition agents prevents SQL injection attacks by validating SQL queries before the database engine processes the query. Enterecept rejects malicious SQL injection attempts and preserves the database's integrity.

Database Shielding—Shielding ensures that no process other than the database itself will be able to access the database's execution environment, data, and settings. Database shielding provides a protective envelope of operation that prevents both outside penetration and malicious use of the database server. As a result, it prevents both known and unknown attacks in real time, before they reach the database server and cause harm. Intruders cannot access or modify operational parameters—even if they manage to gain privileged access to the server.

All Features of Enterecept Standard Edition—Including known and unknown attack prevention, buffer overflow exploit prevention, resource protection, and prevention of privilege escalation.

Process Firewall—The Database Edition agent blocks network traffic to and from the system through a highly granular packet filter and application layer firewall. It analyzes over 120 IP protocols and can block network attacks like WinNuke and reconnaissance techniques like port scanning.

Fast Path to Prevention Policies Out of the Box—Enterecept easily shifts critical systems into a high level of protection quickly through an intuitive and systematic GUI, which builds policies through exceptions. Organizations can switch agents through increasing levels of sensitivity, allowing them to change their security posture incrementally. The result is near-zero false positives and minimal long-term tuning.

McAfee ePO™ 3.5 Deployment and Monitoring—Options for installing, updating, and monitoring agents.

Event Aggregation—The Enterecept Management System aggregates similar events and displays as a single line for ease of analysis.

Integrated HIPS and NIPS Event Monitoring—IntruShield 2.1 Manager imports and correlates Enterecept agent alerts with IntruShield sensor alerts for a consolidated, system-wide view of security status.

Installation Requirements

Windows® Database Server

- 200MHz Pentium III or better
- 128MB RAM minimum
- Microsoft SQL Server 2000
- Windows 2000 Server, Windows 2000 Advanced Server, or Windows 2003 Server
- Windows NT 4 Server or Enterprise Server, Service Pack 6a or later

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, Enterecept, ePolicy Orchestrator, ePO, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-ent-dbe-004-0704