

# McAfee Enterccept Database Edition

## Intrusion Prevention für Datenbankserver

### Die Herausforderung

Die Anzahl neuer Sicherheitslücken und die Geschwindigkeit und Raffinesse, mit der diese Sicherheitslücken angegriffen und ausgenutzt werden, wächst jedes Jahr und erhöht die Risiken für die Sicherheit von Unternehmen. Durch die Entwicklung neuer komplexer Angriffe, die mithilfe zahlreicher Vektoren in die Sicherheitsinfrastruktur eindringen, sind Unternehmen gezwungen, eine sich ständig ändernde Gefahr zu bekämpfen.

Datenbankserver abzusichern, ist eine schwierige Aufgabe — der Echtzeitzugriff auf die Daten eines Datenbankservers ermöglicht es Unternehmenskunden, Mitarbeitern und Partnern, ihre Unternehmens-Performance zu optimieren. Der erweiterte Zugriff vergrößert jedoch auch das Sicherheitsrisiko.

Leider arbeiten herkömmliche IDS-Tools reaktiv, die Angreifer sind also immer einen Schritt voraus. Zur Gewährleistung umfassender, proaktiver Sicherheit benötigen Unternehmen ein mehrstufiges Sicherheitskonzept mit ineinandergreifenden und sich ergänzenden Technologien, die Netzwerke und Systeme von der Peripherie bis zum Kern schützen. McAfee® Intrusion Prevention ist eine der umfassendsten, genauesten und skalierbarsten Angriffsabwehrlösungen auf dem Markt. Sie hilft Unternehmen, das Angriffsrisiko zu verringern, die Verfügbarkeit aufrechtzuerhalten und die Gesamtbetriebskosten zu reduzieren.

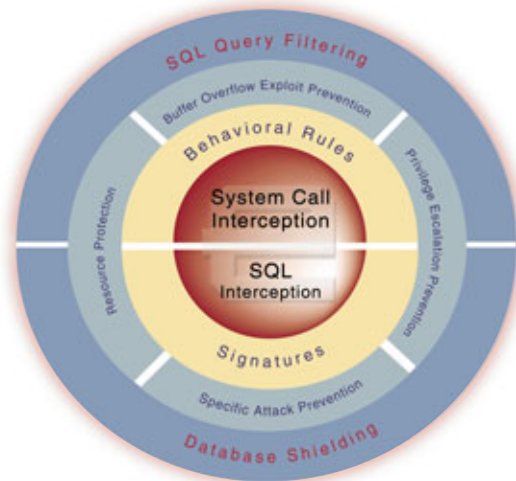
### Die McAfee Enterccept-Lösung

Die McAfee Enterccept® Database Edition ist ein bewährtes, einfach zu implementierendes Tool. Unternehmen, die Microsoft® SQL Server 2000 einsetzen, können damit ihre Daten und Ressourcen schützen und die Integrität der Datenbank sicherstellen. Die Enterccept Database Edition, die auf der patentierten Technologie der Enterccept Standard Edition basiert, gewährleistet einen noch umfassenderen Schutz vor datenbankspezifischen Angriffen, z. B. den weit verbreiteten „SQL Injection“-Angriffen. Enterccept ist die einzige Intrusion Prevention-Lösung, die anwendungsspezifische Programme und Regeln zur Inhaltsüberwachung erstellt. Jeder Database Edition-Agent evaluiert SQL-Abfragen, bevor sie verarbeitet werden. Er kombiniert Verhaltensregeln mit Signaturen, um bekannte und unbekannte Angriffe mit höchster Genauigkeit zu erkennen und zu blockieren, bevor diese Schaden anrichten können.

### Vorteile

#### Umfassend

- IPS und Firewall-Schutz gewährleisten die Verfügbarkeit geschäftskritischer Anwendungen durch Blockieren bekannter und unbekannter Angriffe
- Reduziert bei neuen Sicherheitslücken und Gefahren die Dringlichkeit der Patch-Implementierung



*Durch die Kombination aus SQL-Abfragefilterung, umfassender Datenbankabschirmung und Betriebssystemabsicherung schützt die Database Edition Datenbanken vor bekannten und unbekanntem Angriffen.*

- Gewährleistet die Sicherheit des Servers und stellt dadurch die Integrität und den Schutz vertraulicher Daten sicher

#### Genau

- Verhaltensregeln in Verbindung mit Signaturen bieten einen sicheren Schutz vor sogenannten *Zero-Day* Angriffen (Angriffe auf eine neue, bisher unbekannte Sicherheitslücke) wie z. B. Angriffe, die einen Buffer Overflow erzeugen
- Prozess-Firewall setzt Richtlinien über granulare Paketfilter und Firewall auf der Anwendungsebene durch
- Vorkonfigurierte, individuell anpassbare Regeln und Signaturen verringern die falschen Einstufungen. Sicherheitsspezialisten können sich wieder auf ihre eigentlichen Aufgaben konzentrieren

#### Skalierbar

- Konfigurieren und Verwalten von mehreren Tausend Agenten mit einem einzigen Management-Server
- Installation bzw. Update im Hintergrund, kein Neustart erforderlich
- Optionale Implementierung und Überwachung von Agenten mit dem McAfee ePolicy Orchestrator® 3.5 (ab 3. Quartal 2004 verfügbar)
- Individuell anpassbare Schutzebenen, von Protokollierung bis Blockierung

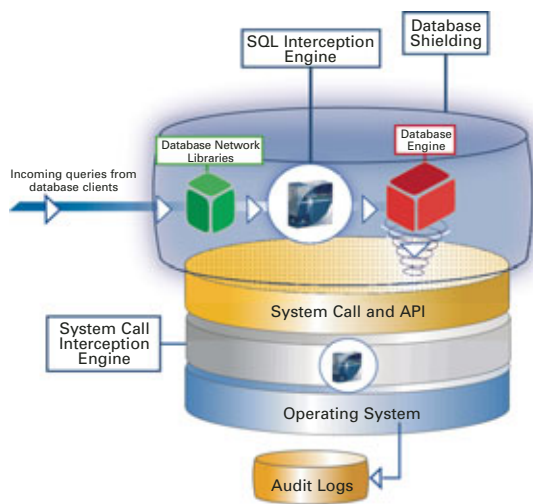
### Funktionsweise der Enterccept Database Edition

Jeder zentral verwaltete Database Edition-Agent wird mit einer vollständig konfigurierten Standard-Sicherheitsrichtlinien geliefert, die als Vorlage dienen und ohne weitere Konfigurationseinstellungen verwendet werden können.

Der Agent stellt zudem leistungsfähige Anpassungsfunktionen zur Erstellung eigener Sicherheitsrichtlinien bereit, die ganz auf die spezifischen Anforderungen einer Umgebung zugeschnitten werden können. Auf diese Weise lassen sich falsche Einstufungen weiter verringern. Agenten rufen darüber hinaus automatisch verschlüsselte und authentifizierte Updates aus dem Management-System ab.

Die SQL Interception-Engine überprüft jede eingehende Datenbankabfrage auf Überlaufbedingungen und kontrolliert, ob versucht wird, SQL-Code einzuschleusen oder die Datenbank zu manipulieren.

Der Database Edition-Agent gleicht Aufrufe mit den entsprechenden Verhaltensregeln und bekannten Angriffssignaturen ab und blockiert alle Anfragen, die schädigendes Verhalten auslösen oder mit einer Angriffssignatur übereinstimmen.



**Die einzigartige SQL-Interception Engine von McAfee Enterecept wird direkt in die Datenbankanwendung eingebunden und verhindert so schädigendes Verhalten und wehrt somit Angriffe ab.**

## Features

**Schutz vor SQL Injection-Angriffen** — Durch die Eingabe bössartiger SQL-Anweisungen in die Datenfelder einer anfälligen Anwendung kann der Angreifer auf geheime Daten wie z. B. Kreditkartennummern oder Patientendaten zugreifen, Daten ändern und sogar andere Rechner im Netzwerk des Datenbankservers angreifen. Die Database Edition-Agenten verhindern SQL Injection-Angriffe, indem sie die eingehenden SQL-Abfragen auswerten, bevor die Datenbank-Engine diese verarbeitet. Enterecept wehrt Versuche ab, bössartigen SQL-Code einzuschleusen, und stellt so die Integrität der Datenbank sicher.

**Abschirmung der Datenbank** — Die Abschirmung der Datenbank gewährleistet, dass nur die Datenbank selbst auf die Ausführungsumgebung, die Daten oder die Einstellungen

zugreifen kann. Diese Datenbankabschirmung schafft so ein Schutzschild, das ein Eindringen von außen und den Missbrauch des Datenbankservers unmöglich macht. Folglich werden bekannte und unbekannte Angriffe in Echtzeit abgewehrt, bevor sie den Datenbankserver erreichen und Schaden anrichten können. Eindringlinge können nicht auf Betriebsparameter zugreifen oder diese ändern, selbst wenn sie sich bereits widerrechtlich Zugang zum Server verschafft haben.

**Die Enterecept Database Edition umfasst alle Funktionen der Enterecept Standard Edition** — Wie z. B. Abwehr bekannter und unbekannter Angriffe, Schutz vor Buffer Overflows, Ressourcen-Schutz und Verhinderung einer Berechtigungseskalation.

**Prozess-Firewall** — Der Database Edition-Agent blockiert Netzwerkverkehr zum und vom System über einen hochgranularen Paketfilter und eine Firewall auf der Anwendungsebene. Er analysiert mehr als 120 IP-Protokolle und kann Netzwerkangriffe wie z. B. WinNuke und Ausspähungstechniken wie z. B. Port-Scanning blockieren.

**Schneller Pfad zu Abwehrrichtlinien ohne weitere Anpassung** — Über eine intuitive und systematische grafische Benutzeroberfläche (GUI) können Richtlinien durch Ausnahmen erstellt und geschäftskritische Systeme problemlos auf eine höhere Sicherheitsstufe gehoben werden. Unternehmen können so für Agenten immer höhere Sensitivitätsstufen festlegen, um ihr Schutz- und Abwehrverhalten schrittweise zu ändern. Auf diese Weise lassen sich Fehlalarme nahezu eliminieren und langfristige Anpassungen auf ein Minimum beschränken.

**Implementierung und Überwachung mit dem McAfee ePO™ 3.5** — Optionen zur Installation, Aktualisierung und Überwachung von Agenten.

**Ereignisaggregation** — Das Enterecept Management-System fasst ähnliche Ereignisse zu einem einzigen Eintrag zusammen, um die Analyse zu vereinfachen.

**Ereignisüberwachung durch Integration von HIPS und NIPS** — Der IntruShield® 2.1 Manager importiert und korreliert die Alarme der Enterecept-Agenten mit den Alarmen der IntruShield-Sensoren, um die Anzeige des Sicherheitsstatus für das gesamte System zu vereinheitlichen.

## Installationsvoraussetzungen

### Windows® Datenbankserver

- 200MHz Pentium III oder höher
- Mindestens 128MB RAM
- Microsoft SQL Server 2000
- Windows 2000 Server, Windows 2000 Advanced Server oder Windows 2003 Server
- Windows NT 4 Server oder Enterprise Server, Service Pack 6a oder höher

**McAfee GmbH** Ohmstraße 1, 85716 Unterschleißheim, Telefon: 089 – 37 07 0 | Luisenweg 40, 20537 Hamburg, Telefon: 040 – 25 31 0  
Regus Center – Twin Tower, Wienerbergstraße 11/12 A, A-1100 Wien, Telefon: +43-(0)1-994 60 6202 | [www.mcafee.de](http://www.mcafee.de)

Die Produkte von McAfee® zeichnen sich durch jahrelange Erfahrung und Engagement im Bereich Kundenzufriedenheit aus. Das PrimeSupport®-Team besteht aus hoch qualifizierten Support-Technikern, die Ihnen mit maßgeschneiderten Lösungen und detaillierter technischer Unterstützung bei der Verwaltung geschäftskritischer Projekte zum Erfolg verhelfen. Der Service-Level wird dabei jeweils an die Bedürfnisse des einzelnen Unternehmens angepasst. McAfee Research, marktführend in der Informationssysteme- und Sicherheitsforschung, führt die bahnbrechenden Innovationen bei der Entwicklung und Verbesserung unserer Technologien fort.

McAfee, Enterecept, ePolicy Orchestrator, ePO, IntruShield, und PrimeSupport sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Niederlassungen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit steht unverkennbar für alle McAfee® Markenprodukte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind Eigentum ihrer jeweiligen Besitzer. © 2004 Networks Associates Technology, Inc. Alle Rechte vorbehalten. 1-sps-ent-dbe-gr-002-0704