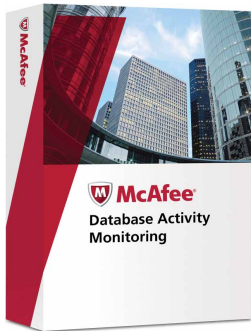


# McAfee Database Activity Monitoring

Kosteneffektiver Schutz von Datenbanken zur Erfüllung Ihrer Compliance-Anforderungen



Unternehmen legen ihre wertvollsten und vertraulichsten Informationen in einer Datenbank ab, doch der Perimeterschutz und die grundlegenden Sicherheitsfunktionen dieser Datenbank schützen Sie nicht vor raffinierten Hackern oder potenziellen Bedrohungen durch nicht autorisierte Insider. Eine Studie<sup>1</sup> belegt, dass über 92 Prozent der ausspionierten Daten auf einer Datenbank gespeichert waren und mehr als 87 Prozent Angriffe darstellen, die eine große technische Kompetenz erfordern. McAfee® Database Activity Monitoring erkennt die Datenbanken in Ihrem Netzwerk automatisch, schützt sie mit vorkonfigurierten Verteidigungsmechanismen und hilft Ihnen dabei, individuelle Sicherheitsrichtlinien für Ihre Umgebung zu erstellen — so dass es einfacher wird, die Einhaltung gesetzlicher Richtlinien zu belegen und kritische Daten besser zu schützen.

## Hauptvorteile

- Maximiert die Transparenz und den Schutz vor den unterschiedlichsten Angriffen
- Überwacht externe Bedrohungen, privilegierte Insider und komplexe Bedrohungen aus der Datenbank
- Minimiert das Risiko und die Haftungsansprüche, indem Angriffe gestoppt werden, bevor sie Schaden anrichten können
- Spart Zeit und Geld mit einer schnelleren Bereitstellung sowie einer effizienteren Architektur
- Gibt Ihnen die Flexibilität, problemlos die IT-Infrastruktur Ihrer Wahl zu nutzen
- In die Kernprodukte von McAfee, wie beispielsweise McAfee ePolicy Orchestrator® (McAfee ePO™) Management-Plattform und McAfee Vulnerability Manager for Databases, integrierbar

Mit McAfee Database Activity Monitoring erhalten Unternehmen Transparenz für alle Datenbankaktivitäten, darunter auch lokale privilegierte Zugänge und komplexe Bedrohungen aus der Datenbank. McAfee Database Activity Monitoring hilft Unternehmen, ihre wertvollsten und vertraulichsten Daten vor externen Bedrohungen und böswilligen Insidern zu schützen. McAfee Database Activity Monitoring liefert nicht nur ein zuverlässiges Audit-Protokoll, sondern verhindert auch unbefugte Eingriffe, indem es Sitzungen beendet, die die Sicherheitsrichtlinien verletzen.

Mit McAfee Database Activity Monitoring können Unternehmen:

- Umgehend individuelle Sicherheitsrichtlinien aufsetzen, um branchenspezifische Vorschriften oder interne IT-Standards zu erfüllen
- Den Zugriff auf vertrauliche Informationen für Auditzwecke protokollieren, darunter auch die vollständigen Transaktionsdaten
- Sitzungen, die die Richtlinien verletzen, beenden und verdächtige Anwender isolieren, so dass keine Daten ausspioniert werden können
- Die Abgrenzung der Verantwortungsbereiche beibehalten, so wie sie von vielen Vorschriften gefordert wird

McAfee Database Activity Monitoring schützt Ihre Daten effektiv vor allen Bedrohungen, indem die Aktivitäten lokal auf jedem Datenbank-Server überwacht werden und böswilliges Verhalten selbst bei virtuellen Umgebungen oder Cloud Computing in Echtzeit angezeigt oder beendet wird.

## Schutz vor allen Bedrohungsvektoren für Datenbanken

Angriffe auf wertvolle Informationen, die in Datenbanken abgelegt sind, können von überall aus dem Netzwerk kommen: von lokalen Anwendern, die auf dem Server eingeloggt sind, und sogar direkt aus der Datenbank über gespeicherte Abläufe oder Auslöser. McAfee Database Activity Monitoring nutzt speicherbasierte Sensoren, um alle drei Arten von Bedrohungen mit einer einzigen, nichtintrusiven Lösung zu erfassen. Diese Informationen können dann genutzt werden, um die Richtlinieneinhaltung anlässlich von Audits zu belegen und die Sicherheit für die wertvollsten Daten eines Unternehmens insgesamt zu steigern.

## Bedrohungen unmittelbar erkennen, Risiken und Haftungsansprüche reduzieren

Im Gegensatz zu Audit- oder Protokollanalysen, die Ihnen nur sagen, was bereits passiert ist, können die Funktionen zur Echtzeit-Überwachung und Intrusion Prevention Verstöße stoppen, bevor sie Schaden anrichten. Alarmmeldungen werden direkt an das Überwachungs-Dashboard gesendet. Dabei werden sämtliche Daten zur Richtlinienverletzung zwecks Behebung gleich mitgeliefert. Hochgefährliche Verletzungen können so konfiguriert werden, dass sie verdächtige Sitzungen automatisch beenden und böswillige Anwender isolieren. Das Sicherheitsteam hat Zeit, den Eingriff zu prüfen.

### Virtuelles Patching schützt vor bekannten Angriffen und vielen Zero-Day-Bedrohungen

Nicht immer ist es möglich, die Patches der Hersteller sofort zu installieren. Oft bedingen diese den Test von Applikationen und eine Ausfallzeit, um das Update vorzunehmen. Es gibt auch Anwendungen, die ältere Versionen der Datenbanken nutzen. Für diese Versionen werden keine Patches mehr geliefert. McAfee Database Activity Monitoring erkennt Angriffe, die bekannte Schwachstellen ausnutzen wollen sowie die üblichen Bedrohungsvektoren. Es kann so konfiguriert werden, dass es eine Alarmmeldung ausgibt oder die Sitzung in Echtzeit beendet. Es werden regelmäßig Updates zum virtuellen Patching für neu erkannte Schwachstellen geliefert, die ohne Ausfallzeiten der Datenbank implementiert werden können und vertrauliche Informationen schützen, bis ein Patch vom Hersteller der Datenbank veröffentlicht wurde und eingesetzt werden kann.

### Schnelle und nichtintrusive Bereitstellung mit minimalen Ressourcen

Als reine Software-Lösung kann McAfee Database Activity Monitoring in weniger als einer Stunde implementiert werden und Datenbanken schützen. Es sind keine spezielle Hardware oder zusätzliche Server erforderlich. McAfee Database Activity Monitoring macht die Implementierung noch schneller, scannt das Netzwerk nach Datenbanken und nutzt mit einem Assistenten ausgestattete Templates für unterschiedliche regulatorische Umgebungen, um dem Anwender dabei zu helfen, umgehend individuelle Sicherheitsrichtlinien zu erstellen und so die Anforderungen von Audits zu erfüllen. McAfee Database Activity Monitoring verteilt die Aufgabe der Implementierung von Sicherheitsrichtlinien auf autonome Sensoren, die auf jedem Datenbank-Server laufen, und bietet so auch den größten Unternehmen eine kosteneffiziente, skalierbare Lösung.

### Unterstützt die moderne IT-Infrastruktur von heute, einschließlich Virtualisierung und Cloud Computing

Andere Systeme zur Datenbanküberwachung verlassen sich auf eine Analyse des Netzwerk-Datenverkehrs, um Richtlinienverletzungen zu erkennen. Das ist aber bei den hochdynamischen und verteilten Architekturen, die für die Virtualisierung von Rechenzentren und Cloud Computing genutzt werden, nicht effizient oder sogar gänzlich unmöglich. Die Sensoren von McAfee können dagegen so konfiguriert werden, dass sie sich automatisch um jede neue Datenbank kümmern, die Sicherheitsrichtlinien anhand der Daten darauf abfragen und dann alle Alarmmeldungen an den Management-Server senden. Selbst wenn die Netzwerkverbindung unterbrochen wird, sind die Daten immer noch geschützt, da der Sensor die Sicherheitsrichtlinien lokal implementiert und die Warnmeldungen in eine Warteschlange kommen und zugestellt werden, sobald der Management-Server wieder erreichbar ist.

### Die nächsten Schritte

Weitere Informationen erhalten Sie unter [www.mcafee.com/dbactivitymonitoring](http://www.mcafee.com/dbactivitymonitoring) oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten.

### Über McAfee Risiko- und Compliance-Produkte

Die McAfee Risiko- und Compliance-Produkte helfen Ihnen, Risiken einzudämmen, für automatische Einhaltung zu sorgen und die Sicherheit zu optimieren. Unsere Lösungen führen eine Diagnose Ihrer Umgebung durch, um Ihnen Echtzeit-Einblicke in Ihre Schwachstellen und Richtlinien zu geben. So können Sie ihre wichtigsten Ressourcen schützen, indem Sie Ihre Sicherheitsinvestitionen auf die ausschlaggebenden Punkte konzentrieren. Weitere Informationen erhalten Sie unter: [www.mcafee.com/riskandcompliance](http://www.mcafee.com/riskandcompliance).

