McAfee Database Activity Monitoring

Kosteneffizienter Datenbankschutz zur Erfüllung Ihrer Compliance-Anforderungen

Unternehmen speichern ihre wertvollsten und sensibelsten Daten in Datenbanken. Doch der Peripherie-Schutz und die grundlegenden Sicherheitsmaßnahmen, die zum Lieferumfang der Datenbanken gehören, schützen nicht vor raffinierten Hackern oder potenziellen Bedrohungen durch böswillige Insider. Studien[1] zeigen, dass mehr als 96 Prozent aller Datenkompromittierungen über eine Datenbank erfolgen und Einbrüche in 66 Prozent aller Fälle monatelang unbemerkt bleiben. McAfee® Database Activity Monitoring findet automatisch Datenbanken in Ihrem Netzwerk, schützt sie mit einem Satz vorkonfigurierter Verteidigungsmittel und unterstützt Sie beim Aufbau von Sicherheitsrichtlinien, die auf Ihre Umgebung zugeschnitten sind. Dadurch können Sie gegenüber Audit-Prüfern leichter Ihre Compliance nachweisen und den Schutz wichtiger Datenressourcen verbessern.

Hauptvorteile

- Maximiert die Transparenz und den Schutz vor den unterschiedlichsten Angriffen
- Überwacht externe Bedrohungen, Insider mit Zugriffsrechten sowie raffinierte Bedrohungen innerhalb der Datenbank
- Minimiert Risiko und Haftungsansprüche, indem Angriffe aufgehalten werden, bevor sie Schaden anrichten können
- Spart dank schnellerer Bereitstellung und einer effizienteren Architektur Zeit und Geld
- Bietet die Flexibilität, problemlos die IT-Infrastruktur Ihrer Wahl zu nutzen
- Integriert sich in Kernprodukte von McAfee, z. B. die Verwaltungsplattform McAfee® ePolicy Orchestrator® (McAfee ePO™) sowie McAfee Vulnerability Manager for Databases

Mit McAfee Database Activity Monitoring erlangen Unternehmen Transparenz all ihrer Datenbankaktivitäten – auch bei lokalem berechtigtem Zugriff und ausgefeilten Angriffen aus der Datenbank heraus. Die Lösung 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 die Lösung 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
- Zugang zu sensiblen Daten zu Audit-Zwecken protokollieren, einschließlich vollständiger Transaktionsdetails
- Richtlinien-verletzende Sitzungen beenden und verdächtige Benutzer isolieren, damit keine Daten kompromittiert werden
- Die Abgrenzung der Verantwortungsbereiche beibehalten, die 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 Daten in Datenbanken können über das Netzwerk stattfinden, jedoch auch von lokal beim Server angemeldeten Benutzern durchgeführt werden. Sogar innerhalb der Datenbanken selbst sind Angriffe über gespeicherte Prozeduren oder Auslöser möglich. McAfee Database Activity Monitoring nutzt im Speicher verankerte Sensoren, um alle drei Arten von Bedrohungen mit einer einzigen, nichtintrusiven Lösung zu erfassen. Dank dieser Informationen kann bei Audits Compliance nachgewiesen und die Gesamtsicherheit der wertvollsten Unternehmensdaten verbessert werden.

Unmittelbare Erkennung von Bedrohungen sowie Minimierung von Risiken und Haftungsansprüchen

Im Gegensatz zu grundlegenden Audits oder Protokollanalysen, die Ereignisse immer erst im Nachhinein anzeigen können, werden Kompromittierungsversuche durch Funktionen zur Echtzeitüberwachung und zum Eindringungsschutz blockiert, noch bevor sie Schaden anrichten können. Warnungen werden direkt an das Überwachungs-Dashboard gesendet. Dabei werden sämtliche Daten zur Richtlinienverletzung zwecks Problembehebung gleich mitgeliefert. Für schwerwiegende Verletzungen kann im Vorfeld festgelegt werden, dass verdächtige Sitzungen automatisch beendet und böswillige Benutzer isoliert werden. Dies verschafft dem Sicherheitsteam Zeit, um den Eindringungsversuch genauer zu untersuchen.

Virtuelle Patches schützen vor bekannten Exploits und vielen Zero-Day-Angriffen

Anbieter-Patches können nicht in jedem Fall sofort installiert werden, da diese Aktualisierungen häufig Anwendungstests und Ausfallzeiten nach sich ziehen. Zudem greifen einige Anwendungen noch auf alte Datenbankversionen zurück, für die keine Patches mehr angeboten werden. McAfee Database Activity Monitoring erkennt Angriffe, die bekannte Schwachstellen sowie die üblichen Bedrohungsvektoren ausnutzen. Die Lösung kann so konfiguriert werden, dass sie eine Warnung ausgibt oder die Sitzung in Echtzeit beendet. Virtuelle Patches werden regelmäßig für neu entdeckte Schwachstellen herausgegeben und können ohne Datenbank-Ausfallzeiten implementiert werden. Sie schützen sensible Daten, bis die vom Datenbank-Anbieter herausgegebenen Patches installiert werden.

Schnelle und unterbrechungsfreie Bereitstellung mit minimalem Ressourcenaufwand

Die Implementierung und der Schutz der Datenbanken können bei McAfee Database Activity Monitoring, einer reinen Software-Lösung, in weniger als einer Stunde erfolgen. Dabei sind keine spezialisierte Hardware oder zusätzliche Server notwendig. Die Bereitstellung wird zusätzlich dadurch beschleunigt, dass McAfee Database Activity Monitoring im Netzwerk nach Datenbanken sucht und mit einem Assistenten ausgestattete Vorlagen für unterschiedliche Regulierungsvorgaben nutzt. Auf diese Weise können Benutzer umgehend individuelle Sicherheitsrichtlinien erstellen und so die Anforderungen von Audits erfüllen. McAfee Database Activity Monitoring gibt die Verantwortung für die Implementierung der Sicherheitsrichtlinien an autonome Sensoren weiter, die auf jedem Datenbank-Server ausgeführt werden. Dadurch werden Kosten effektiv skaliert, was insbesondere Großunternehmen zugute kommt.

Unterstützung der modernen IT-Infrastruktur dank Virtualisierung und Cloud Computing

Andere Datenbank-Überwachungssysteme setzen zur Entdeckung von Richtlinienverletzungen auf die Analyse des Netzwerkverkehrs. Diese Strategie erweist sich bei dynamischen und verteilten Architekturen, die bei der Virtualisierung von Rechenzentren oder dem Cloud Computing zum Einsatz kommen, als ineffizient oder sogar nutzlos. Die Sensoren von McAfee können hingegen so konfiguriert werden, dass sie sich automatisch an jede neue Datenbank anfügen, die Sicherheitsrichtlinien anhand der darin gespeicherten Daten abrufen und dann alle Warnungen an den Verwaltungs-Server senden. Selbst wenn die Netzwerkverbindung unterbrochen wird, sind die Daten geschützt, da der Sensor die Sicherheitsrichtlinie lokal anwendet und Warnungen in einer Warteschlange speichert, bis der Verwaltungs-Server wieder erreichbar ist.

Integration in die Plattform McAfee ePolicy Orchestrator

McAfee Database Activity Monitoring ist vollständig in die Software McAfee ePolicy Orchestrator (McAfee ePO) integriert, die über Dashboards eine zentrale Berichterstellung und Zusammenfassung für alle Datenbanken in Ihrem Unternehmen bietet. McAfee ePO verbindet sich mit weiteren McAfee-Sicherheitslösungen, die andere Bereiche als den Datenbankschutz abdecken, und ermöglicht dank der zentralen Benutzeroberfläche einfache Verwaltung sowie vollständige Transparenz.

McAfee-Datenbanksicherheitslösungen

McAfee bietet eine Reihe von Datenbank-sicherheitslösungen an, die Ihnen eine vollständige Übersicht über Ihre Datenbanken und deren Sicherheitslage gewähren. Weitere Informationen erhalten Sie unter www.mcafee.com/de/products/database-security/index.aspx oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten bzw. -Händler.

Über McAfee-Lösungen zum Endgeräteschutz

McAfee-Lösungen zum Endgeräteschutz bieten Sicherheit für alle Geräte, die darauf verarbeiteten Daten sowie ausgeführten Anwendungen. Unsere umfassenden und angepassten Lösungen verringern die Komplexität und errichten einen mehrstufigen Endgeräteschutz, der die Produktivität nicht beeinträchtigt. Weitere Informationen finden Sie unter www.mcafee.com/de/products/endpoint-protection/index.aspx.

[1] *Verizon Business-Studie*, 2013.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de