



Secure Your Databases for Sustainable SOX Compliance

Key Advantages

- Monitors external threats, privileged insiders, and sophisticated threats from within the database
- Minimizes risk and liability by stopping attacks before they cause damage
- Saves time and money with faster deployment and a more efficient architecture
- Gives you the flexibility to easily deploy on the IT infrastructure you choose
- Unparalleled visibility into database security posture
- Scans multiple databases across the enterprise from a centralized console
- Accelerates time to compliance and minimizes audit cycles, resulting in significant cost savings
- Generates customized reports in an easy-to-understand format for various user roles
- Offers centralized management through McAfee ePolicy Orchestrator® (McAfee ePO™)

Have your databases passed a SOX audit? If so, congratulations. But if you've achieved that compliance on the strength of your Database Management System's native tools, you're probably well aware of their limits. If you configure your tools for granular logging they degrade system performance by anywhere from 20 to 50 percent. Most can't detect unauthorized activity in real time, or issue alerts automatically. Most store log information in DBA-accessible files, so there's no way to enforce segregation of duties. In short, native audit tools provide limited visibility into the events that affect your data, and very little real security.

The Marathon of Manual Audit Preparation

And then there's the immense, repetitive workload of preparing for each SOX audit—updating the systems inventory, documenting patch levels, tracking entitlement changes, and examining every single log file. Because most native tools offer no automation or cross-platform integration, these tasks are inescapably manual, time consuming, and error-prone—a recurring waste of skilled manpower.

Securing your databases for SOX compliance in a sustainable manner—one that satisfies your auditor, secures your data, doesn't penalize system performance, or handicap your IT organization—requires a higher level of functionality than native audit tools can deliver. It takes granular transaction logging that doesn't affect database performance. It takes policy awareness to detect and block unauthorized activity and issue alerts in real time. It takes segregation of duties enforcement capability. And perhaps most importantly, it takes comprehensive automation support for activity monitoring, system discovery, configuration assessment, patch management, and audit reporting.

The Solution: McAfee® Data Center Security Suite for Database

McAfee addresses all of these database compliance and security requirements with an integrated suite of products that provide comprehensive database activity monitoring and vulnerability assessment with minimal system performance impact and centralized management and reporting.

McAfee Database Activity Monitoring renders all system activity easily visible, from local privileged access to sophisticated attacks from within the database itself. It detects unauthorized activity as it occurs, issues real-time alerts to the management console, and can be configured to terminate non-compliant sessions and quarantine suspicious users. All access to sensitive data is logged for auditing with complete transaction details, and role-based separation of duties is easily enforced. Virtual patching capabilities protect against known and newly-discovered vulnerabilities until vendor patches can be tested and safely applied. In addition, the McAfee virtual patching solution qualifies as compensating control for legacy databases.

As a software-only solution, McAfee Database Activity Monitoring can be deployed and configured to begin protecting databases in just minutes. It automatically discovers databases across the network and uses wizard-driven templates to guide the creation of custom security policies for SOX and other regulatory mandates. By distributing the responsibility for implementing security policy to small-footprint sensors running in memory on each server, McAfee Database Activity Monitoring scales cost-effectively to support the largest enterprise environments, with minimal impact on database performance.

One Fortune 100 pharmaceutical company deployed McAfee Data Center Security Suite for Databases to help automate SOX compliance and enhance database security. With more than 500 databases, multiple data centers worldwide, and an outsource DBA team, the firm was challenged to monitor access and enforce segregation of duties.

With McAfee Data Center Security Suite for Databases, the firm has been able to:

- Centralize database security management with strong segregation of duties
- Block unauthorized database access in real time
- Automate privileged user entitlement change reporting
- Achieve compliance with internal governance policies and SOX

A leading supplier of laboratory equipment and supplies recently deployed McAfee Data Center Security for Databases after its SOX auditor raised serious security management issues. Following several acquisitions, the firm was having difficulty identifying all its databases, assessing their configuration status, bringing them under central management, and monitoring the activity of privileged users.

With McAfee Data Center Security Suite for Databases, the firm's IT organization has been able to:

- Automatically discover 112 databases subject to SOX (and PCI) mandates
- Automatically assess the version and patch status of each database
- Create and enforce access policies to enable separation of duties
- Initiate real-time activity monitoring with automated blocking of unauthorized activities

McAfee® Vulnerability Manager for Databases provides unparalleled visibility into your organization's database security posture. It automatically discovers databases on your network, determines whether the latest patches have been applied, and identifies tables containing sensitive information. It scans each system against a knowledgebase of more than 4,500 known vulnerabilities in Oracle, SQL Server, DB2, and MySQL releases. Findings are prioritized and presented in preconfigured reports for specific compliance standards, including SOX, accompanied with remediation recommendations and fix scripts. Vulnerability Manager lets you automate many data collection and documentation tasks that are central to SOX compliance, including privileged user and entitlement change reporting.

McAfee ePolicy Orchestrator® (McAfee ePO™) software simplifies database security management and SOX compliance reporting by providing a single, centralized security management console for databases across your environment. With its scalable architecture, flexible automation, fast time to deployment, and ability to support enterprise systems, McAfee ePO software is the most advanced security management solution available today.

Requirement	McAfee Data Center Security Suite for Databases
Real-time visibility into database activity	Continuous monitoring of all database activity with real-time alerting on non-compliant activity, automatic session termination, and user quarantine
Minimal database performance impact	In-memory sensors on each database consume a maximum 5 percent of CPU capacity, even in multi-instance implementations
Privileged user activity monitoring	All access to sensitive data by all users is logged for audit with full transaction detail
True segregation of duties enforcement	Role-based entitlements and centralized security management make it easy to set up and reliably enforce segregation of duties
Automated database discovery and vulnerability assessment	Global, automated database discovery, vulnerability assessment, and mandate-specific reporting that includes risk prioritization, response recommendations, and remediation scripts
Centralized security management and compliance reporting	All database security controls are integrated with McAfee ePolicy Orchestrator for simple, centralized management

Making Database Security and SOX Compliance Sustainable

McAfee Data Center Security Suite for Database delivers all the capabilities needed to secure your databases for reliable SOX compliance, with minimal impact on system performance or the productivity of your IT organization. For more information, visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller.

