Defend Legacy Databases and Operating Systems

Extend protection and compliance to EOL servers and databases

Why are so many companies running unsupported legacy databases and operating systems? The answers range from "if it's not broken, why fix it?" to operational concerns about business continuity, application compatibility, and cost-prohibitive migration paths. Regardless of the reasons for running end-of-life (EOL) platforms, one thing is clear—databases are the number one target for both hackers and disgruntled insiders. The security experts at McAfee understand how to protect databases effectively—even in the absence of vendor-issued security patches. Our innovative solution has quickly gained support and popularity among customers and auditors alike.

High-profile database breaches and a steady stream of regulatory mandates have placed security teams and compliance managers under the microscope. Every database and operating system has security flaws and vulnerabilities that must be carefully managed. Database and operating system vendors understand this, which is why they regularly issue security patch updates to address newly discovered vulnerabilities. But when database and operating system vendors end support for an older version of their product, security patches are no longer developed. Unfortunately this does not stop the discovery of new vulnerabilities affecting those versions.

When these systems reach EOL status, your options to protect them become limited to these three:

- *Upgrade to a newer, fully-supported version*—This option involves significant total cost of ownership (TCO) costs: upgrade fees, licensing costs, and the costs for testing and modifying existing applications. It's not a simple, plug-and-play process. Databases must be brought offline for upgrades to occur. In many cases, the new database version requires rewriting or modifying applications, which means you must have access to the application source code, skilled developer resources, and the time to test and validate all changes. Even when application recoding isn't required, most companies perform complete regression testing on all applications against the new database version. In some cases, a lengthy and expensive re-certification process is also needed.
- *Do nothing and hope for the best*—While the database may be working fine, security concerns and auditing/compliance issues will continue to mount, making this a short-term option
- *Protect your end-of-life database*—Implement a virtual patching and OS-hardening solution

McAfee Virtual Patching Drives Greater Value for Auto Industry Leader

The inability to pass compliance audits was a serious roadblock to one of the world's largest automobile manufacturers. After a thorough competitive review, the company quickly secured its EOL databases and achieved compliance using McAfee Virtual Patching for Databases. Key selection criteria included affordability, ease of installation, no database downtime, minimal database performance impact, and a proven compliance track record.

Why Companies Don't Pull the Plug on EOL Systems

Legacy systems still deliver value, even though vendors have ended support for these systems. Here are the reasons most companies cite for continuing to run EOL databases:

- Migration and upgrades may be cost prohibitive, often including new licensing fees, operating system upgrades, and hardware upgrades
- The migration process for production databases and applications may disrupt business operations
- Application compatibility issues with new OS/database versions often require time-consuming application development and regression testing

The McAfee Legacy Database Solution

McAfee has a simple, proven approach to securing EOL databases that combines two best-in-class technologies recognized by compliance officers as valid compensating control for legacy database platforms:

- McAfee® Virtual Patching for Databases protects legacy databases by detecting and preventing attempted attacks and intrusions without requiring database downtime or application testing/ modification.
- McAfee Application Control adds another layer of protection by hardening legacy operating systems. For compatibility reasons, EOL databases often run on servers with vulnerable EOL operating systems. McAfee Application Control locks down the operating system, protecting it from unauthorized applications and code.

McAfee Virtual Patching Advantages

- Gain protection from threats on systems for which vendor-released patches no longer exist
- Eliminate the need for IT and security teams to have DBMS-specific knowledge
- Keep production databases online, thanks to non-intrusive software design
- Protect databases seamlessly with automatic distribution of updates
- Facilitate compliance with PCI DSS, HIPAA, and other standards

How does McAfee Virtual Patching work?

Virtual patching creates a security layer around the database. This solution monitors all activity occurring in the database memory, detecting patterns of real-time exploits based on either known database code vulnerabilities or suspicious database behavior. When a match or policy violation occurs, a real-time alert is issued, the suspicious session is terminated, and the offending user is quarantined. This approach has proven highly effective for securing databases that have reached EOL support status, such as Oracle 8i, Oracle 9i, and Microsoft SQL Server 2000. In addition, McAfee Virtual Patching protects current database versions during the window of vulnerability that exists between the time a new vendor patch is issued and when they are actually deployed.

The McAfee Virtual Patching solution is continuously updated by the McAfee security team to address newly discovered vulnerabilities. New protection policies are added and seamlessly distributed and applied on average once per month. The solution protects against more than 500 vulnerabilities (as of Q2 2012).

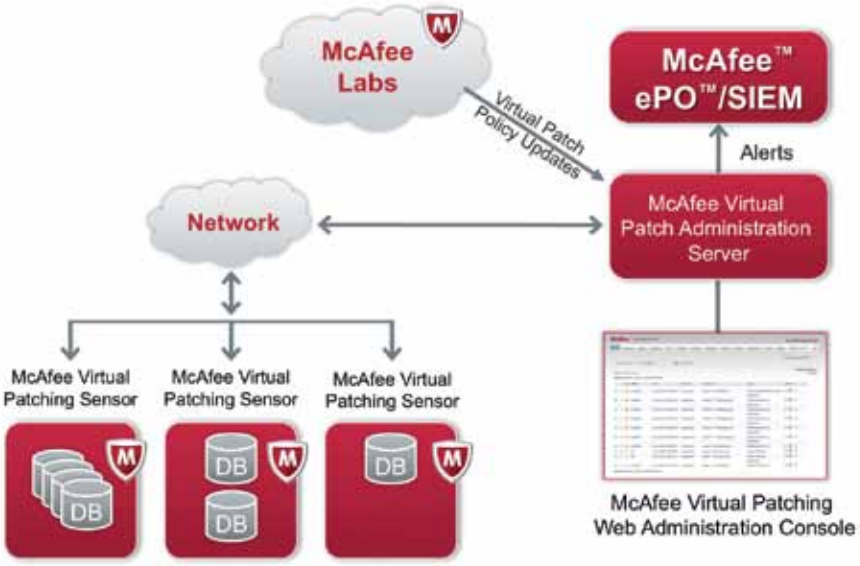

Figure 1. The McAfee security team routinely researches and monitors database security issues. When an issue is discovered, McAfee deploys the virtual patching rules to a central server. Protected databases poll the central McAfee Virtual Patching servers and either deploy protection automatically or according to a predefined schedule. Once a security update is downloaded, it is pushed immediately to relevant sensors.

How does McAfee Application Control work?

There's a reason why operating system vendors provide security patches for their current products: the operating system can serve as a launching point for attacking databases and other applications. However, operating systems such as Microsoft Windows NT and Microsoft Windows 2000 have reached EOL status, and security patch updates are no longer available from Microsoft.

McAfee Application Control blocks unauthorized access to system resources and foils advanced persistent threats using sophisticated whitelisting technology. In the context of legacy database protection, it locks down the database's underlying operating system, allowing only authorized staff and update processes to make operating systems modification. McAfee Application Control software also prevents whitelisted applications from being exploited via memory buffer overflow attacks—a common hacking technique. Plus, it provides an audit trail of all unauthorized change attempts.

Figure 2. McAfee Application Control uses a dynamic trust model to simplify the whitelisting process and eliminate manual whitelist administration.

McAfee Application Control Advantages

- Gain protection from threats on unsupported legacy operating systems, such as Microsoft Windows 2000 and Windows NT
- Automatically accept new software added through your authorized processes
- Maintain user productivity and server performance with a low-overhead solution
- Prevent databases from being exploited via memory buffer overflow attacks on Windows 32- and 64-bit systems
- Automate enterprise security management thanks to integration with McAfee® ePolicy Orchestrator® software

Leading Energy Company Extracts Greater Value from Legacy Databases

A large multinational energy company faced a growing problem—how to secure hundreds EOL Oracle databases distributed around the world. Compliance issues escalated rapidly as auditors raised high priority audit concerns and established tight deadlines for the company's IT and security staff to provide a solution. One option, a massive upgrade of these legacy databases, would require extensive resources, time-consuming application regression testing, disruption of business services, major license fee increases, and, in many cases, costly hardware upgrades.

This energy leader chose McAfee Virtual Patching for Databases because it offered several unique advantages, including these capabilities:

- Visibility into every transaction that takes place in database memory, rather than simply sniffing SQL packets over the network or in "local host" pipes
- Effective thwarting of database attacks, even when the database itself cannot be physically patched
- Solution deployment without disrupting business operations

Compliance auditor concerns were addressed in record time. Within one month of purchase, the solution was deployed to more than 700 databases, with very little assistance from McAfee engineers. A year later, the solution is performing as expected on more than 1,000 EOL databases.

Keep Your Legacy Databases Safe and Available

At McAfee, we realize your databases store your most critical business assets. They must be available around-the-clock to power your business. And, just as your databases don't take a day off, neither do we. Our team of database security experts remains relentlessly focused on keeping your sensitive information safe and available, while helping your company ensure compliance with internal policies and industry regulations.

For more detailed information on how McAfee Virtual Patching for Databases and McAfee Application Control can help you protect your legacy databases and operating systems, visit www.mcafee.com/dbsecurity, or contact your local McAfee representative or reseller.

Follow us on Twitter: @McAfee_DBSecure.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

49200brf_legacy-db-os_0812_fnl_ASD