Rimini Street®

Rimini Street Advanced Database Security

Supported Platforms

Rimini Street Advanced Database Security is available for Oracle, SAP, IBM Db2, Microsoft SQL Server, PostgreSQL, MySQL, MariaDB, and MongoDB databases.

The Rimini Street Advantage

- Deep application knowledge
- Award-winning support
- Accelerated engineering services
- Cost advantage

"[Virtual patching provides] protection against both known and unknown vulnerabilities, including 'Zero-Day' exploits."[1]

Solution Overview

Rimini Street Advanced Database Security is a next-generation database security solution enhanced with technology from McAfee that protects databases from known and unknown vulnerabilities by monitoring and analyzing database memory, and blocking attempted attacks using virtual patching before they reach the database.

Virtual patching provides database users with a faster time-to-protect the database in comparison to traditional software vendor patching. It is often more comprehensive, more effective, faster, safer and easier to apply than traditional vendor patching, and provides organizations a faster time-to-protection against vulnerabilities with a more cost-effective solution, without any need to impact production systems.

Security Challenges

Security professionals find that traditional vendor security patching models are outdated and provide ineffective security protection. Due to late delivery, complexity of applying patches and the expense of code regression testing, traditional vendor patching can leave enterprise systems vulnerable for months, sometimes even years.

Many companies apply security patches only once per year — if at all — due to the significant downtime, labor and cost of deployment. With the average half-life of vulnerabilities at less than 30 days, the majority of cyber-attacks happen before a patch is released by the database software vendor.[2]

[1] Aberdeen Group, "Why Adopt Virtual Patching vs. Vendor Patching for Enterprise Software Security?", January 2022
[2] Qualys Research, "The Laws of Vulnerabilities 2.0," 2009.

According to the Aberdeen Group3, issues with traditional vendor patching include:

- **Delayed patch availability:** There is often a significant lag time between the public disclosure of a vulnerability and the availability of a patch from the vendor, which can leave many enterprise systems vulnerable for months.

- **Limited Scope:** About 20% of known vulnerabilities in the typical enterprise computing infrastructure remain unpatched a full quarter after they are publicly disclosed.

- **Burdensome:** The amount of time required and business disruption created in applying vendor-delivered security patches leads many organizations to delay or forgo applying patches altogether.

- **Costly**: Research data highlights that for an enterprise with 2,000 database instanses, the traditional vendor security patching model has a median cost of around $4M.

Key Features & Capabilities

- **Patches and protects known and unknown vulnerabilities** without taking databases offline

- **Reduces risk with accelerated update delivery** within 24 to 48 hours after a vulnerability is published or a patch is released by a database vendor — unlike traditional vendor patching

- **Eliminates the need for time-consuming and costly code regression testing** since direct modifications to the resource being protected are not required

- **Provides comprehensive coverage and more effective protection** for a wide range of databases including: Oracle Database, Microsoft SQL Server, IBM Db2, SAP ASE, SAP SQL Anywhere and SAP Advantage Server (collectively the former SAP Sybase family of database products), SAP HANA, PostgreSQL, MySQL, MariaDB, and MongoDB

- **Security best practices and guidance of virtual patching** from Rimini Street Global Security Services and implementation guidance for Rimini Street Advanced Database Security

- **Tuning guidance and log analysis for system optimization**, provided by Rimini Street Global Security Services team

- **A single point of contact** by an assigned Primary Support Engineer with an average of 20+ years of experience for Advanced Database Security support and other database support issues

[3] Aberdeen Group, "Why Adopt Virtual Patching vs. Vendor Patching for Enterprise Software Security?", January 2022

Benefits

Rimini Street Advanced Database Security enables organizations to gain a holistic approach to security across the enterprise. Rimini Street provides clients with actionable security intelligence to reduce potential exposure. From tailored security vulnerability analysis reports to expert advice in the identification and selection of critical security controls (and vendors), Rimini Street helps clients ensure that they successfully reduce and manage risk far beyond ERP applications and databases.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. www.mcafee.com