DATASHEET

Rimini Protect™

Rimini Protect™ Advanced Application and Middleware Security

PRODUCTS SUPPORTED

Applications

- E-Business Suite
- JD Edwards
- PeopleSoft
- Hyperion
- Agile PLM
- AGT Web Commerce
- Oracle Retail
- Oracle TMS
- Oracle Life Sciences
- Oracle Fusion Middleware (SOA, B2B, ESB)
- Oracle Primavera
- Oracle Product Management
- Oracle Enterprise Manager
- Oracle GoldenGate
- Oracle OBIEE
- SAP BusinessObjects (Java)

Application Servers

- Oracle WebLogic
- IBM WebSphere
- SAP NetWeaver
- Jboss
- Goldfish
- Apache

Powered by Waratek

WARATEK

The Business Challenge

With more than 25,000 new security vulnerabilities[1] reported to the NIST National Vulnerability Database in 2022, the number of vulnerabilities continues to increase over time along with the number of patches issued by some vendors.[2] The importance of mitigating security risks cannot be understated, with the average cost of a breach at an all-time high.[3] However, many organizations find it difficult to remediate these vulnerabilities within timelines required by their own business, external partners, and regulatory programs.[4]

Attack vectors are also evolving: Common Weakness Enumeration (CWE) rankings trend up as vulnerability exploitations associated with CWEs become well known, understood, and exploitable. CWEs with accessible attack vectors tend to trend high in the Mitre top 25,[5] as a result of increasing rates of exploited vulnerabilities associated with the CWE.[6]

PROACTIVE

FAST AND COST-EFFECTIVE

PERSONALIZED

The Rimini Street Solution

Rimini Protect Advanced Application and Middleware Security (AAMS) is a next-generation Java run-time security solution that provides real-time, zero-day vulnerability protection to safeguard applications and middleware using runtime application detection and remediation including integrations for Java, .NET, etc.

AAMS is designed to deploy security updates to mitigate threats quickly and easily without operational disruptions and time-consuming implementation tasks for each software instance, including no planned downtime and no regression testing. Additionally, it helps protect against both known and unknown threats and vulnerabilities.

AAMS is embedded into the runtime of applications and middleware and provides protection at the Common Weakness Enumeration (CWE) level within the application code. This enables protection against entire classes/categories of vulnerabilities such as request forgery, cross-site scripting, and even remote code execution flaws such as insecure deserialization, even in custom code.

Rimini Street

KEY CAPABILITIES

Zero-Day Protection for Applications and Middleware

» Proactively blocks both known and unknown vulnerabilities with real-time detection and protection

» Zero-day control using rules-based monitoring that detects and helps protect against entire categories of vulnerabilities (CWE) including OWASP Top 10, and SANS Top 25.

» Protects web/application servers running Java 1.5 or higher

Easy Deployment and Maintenance

» No prerequisite code updates; no extensive regression tests

» Easy and prompt deployment of security updates without planned downtime

» Streamlined processes increase productivity while minimizing implementation costs

Autonomous Rule Management Runtime (ARMR) Technology

» Security controls provide continuous monitoring and protection

» Works at Java run-time to help remediate Common Vulnerability Exposure (CVE), Common Weakness Enumeration (CWE), and threats from additional data sources

» Automatic security hardening with full forensic data

Solution Benefits

- **Risk mitigation:** Proactive, zero-day protection for entire classes of security vulnerabilities
- **Protects against both known and unknown vulnerabilities:** Real-time detection of weaknesses, including protection for SQL injection, cross-site scripting, remote code execution, and Java object deserialization
- **Protection for current and older releases:** Protection for licensees on software releases that no longer receive software vendor security updates, and who do not wish to perform a potentially expensive upgrade just to receive security updates from the software vendor
- **Broad protection:** Provides protection for entire classes of security weaknesses without waiting for individual "unknown" vulnerabilities to be identified or for a patch to be developed for a new "known" vulnerability
- **Fast protection:** Deploys security updates to help mitigate threats quickly and easily without operational disruptions and time-consuming implementation tasks for each software instance, including no planned downtime and no regression testing
- **Cost effective:** Threat updates can be deployed almost immediately, providing quick threat protection without meaningful deployment cost
- **Eliminates false positives:** Allows you to focus on real attacks, with minimal performance impact
- **Flexible Java support:** Applications continue to run un-modified on Java releases version 1.5 or higher without upgrades or interoperability issues

Rimini Protect™

Rimini Protect™ is a family of security products and services that provide proactive, fast, and cost-effective security protection, personalized to an organization's unique enterprise software environment and landscape.

At Rimini Street, we understand that every enterprise software ecosystem is unique and personalized to accomplish specific business objectives. We tailor custom configurations of our services and solutions for your unique enterprise software ecosystem to help mitigate risk, assist you on your path to compliance, and improve your security posture.

Learn more about Rimini Protect™ and all of our security services and solutions.

[1] CVEdetails.com

[2] Example: 327 new Oracle security patches in January 2023 vs. 433 new security patches in April 2023

[3] Ponemon Institute: The average cost of a breach is at an all-time high of $4.35 million in 2022

[4] CISA Binding Operational Directive 22-01: Critical vulnerabilities must be remediated within 15 calendar days of initial detection. PCI DSS v4.0: Critical or high-security patches/updates ... are installed within one month of release.

[5] Mitre: Trends in Real-World CWEs: 2019 to 2023

[6] Mitre: About CWE

Rimini Street

riministreet.com | info@riministreet.com | linkedin.com/company/rimini-street | twitter.com/riministreet