Rimini Protect™

Rimini Street™ Advanced Database Security

Rimini Protect™

Advanced Database Security (ADS) is part of a zero-day database security solution that monitors the memory activity of databases (especially the execution plan) and proactively protects against exploitation of most database vulnerabilities by addressing entire categories of weaknesses for which most CVE's fall within. This technology can also be referred to as virtual patching; however, virtual patching is only one of the many features and capabilities of our solution. Rimini Street's Advanced Database Security provides full visibility into DBMS user activity and can issue alerts or terminate suspicious activities based on predefined rules and custom rules.

Advanced Database Security works in parallel with other security solutions within the Rimini Protect suite. The key advantages of Rimini's Advanced Database Security include:

- Protects versions of Oracle database including those that are under sustaining support[1]
- Prevention of intrusion, data theft, and other attacks on the DBMS
- Prevention of Denial of Service and SQL Injection via built-in packages.
- Prevention of Privilege Escalation and OS access via Java
- Prevention of Buffer Overflow in a built-in-packages
- General Real SQL Injection Protection
- Monitoring of DBMS activities, including the activities of authorized and privileged users
- Rule-based policies for users, queries, and DBMS objects
- Quarantine rogue users
- Quick and easy deployment and configuration
- Attack vector agnostic (application, network, host, or intra-database based protection)

In addition to being able to protect you from these common types of attacks, the ADS solution integrates into your SOC environment (typically a SIEM solution) and provides alerts for malicious behaviors.

The alerts include relevant session information such as:
- User information (database, application, etc)
- Location of the attack origin (hostname, IP address, application modules)
- Specific attack methodology (including underlying SQL leveraged in the attack)
- Historical records of relevant incidents for investigative purposes

This information enhances incident response capabilities by facilitating the correlation of detailed information for the incident response team while responding to and protecting against database attacks.

---

[1] Oracle Software Technical Support Policies

Rimini Protect™

The ADS sensor attaches itself to the DB's instance memory in the SGA. Using the read-only mechanisms and application programming interfaces (APIs), it monitors the database by continuously monitoring the memory. The currently running and previous statements are analyzed and using a predefined policy received from the sever, the sensor determines which statements should trigger alerts or be blocked.

ADS is purpose built to protect databases including Oracle. To help mitigate risk, we employ a combination of our products and services offered in our Rimini Protect™ portfolio.

Rimini Protect Advisory Security Services:
Guidance and proactive intelligence services that can help to prevent and mitigate vulnerabilities months and even years before they are discovered and resolved by vendor security patches.

- Level 1 Security Assessments
    We give our clients the ability to prioritize focus areas to help with risk mitigation. Our experts analyze the security posture of the environment while considering the client's specific compliance needs and concerns.
- Hardening Guides
    Our security teams provide guidance on mitigating risk by strengthening the configuration of many popular enterprise software ecosystems. Hardening guides are proprietary to Rimini Street, written in conjunction with security leaders in those platforms.
- Security Vulnerability Analysis Reports (SVARS)
    SVARs are intelligence reports analyzing reported security vulnerabilities and providing mitigation options and strategies.
    - Oracle: Quarterly analysis following the critical patch update vulnerabilities
    - SAP: Monthly analysis of Security Patch Day vulnerabilities
- Zero-day Advisories
    When the unexpected happens and zero-day or proof of concept exploits are loose in the wild, we publish off cycle advisories which include mitigation strategies, direct mitigations, and information regarding our security solutions' ability to provide protection against these exploits. We also include guidance for your own independent validation.
- Security Cases
    Rimini Protect clients can leverage the same industry leading support process and SLAs for security related cases.
    - ✓ 10-minute guaranteed response time for P1 critical issues
    - ✓ Frequent cadence of update communications for every case
    - ✓ 4-hour resolution targets for the most common service requests

Rimini Protect™

Rimini Protect Fee-Based Security Services:

- In-depth Security Assessments
  - Evaluate the security posture of enterprise software ecosystems and provide guidance for improving processes and infrastructure by our team of security experts.
- Security Enhancements
  - Our security team has extensive experience in implementing security solutions and control enhancements identified by either client needs or through Rimini Street provided security assessments.
- Strategic Security Roadmaps
  - Security roadmaps that account for the organizations' overall IT and ERP strategy, risk management and compliance needs. We start by identifying the existing gaps and provide options to help achieve your overall strategic objectives, accounting for your unique business requirements and strategies.

Rimini Street®

Worldwide Headquarters, 3993 Howard Hughes Parkway, Suite 500. Las Vegas, NV 89169, USA Phone: 702.839.9671
Toll-free in the USA: 1.888.870.9692 riministreet.com linkedin.com/company/rimini-street
twitter.com/riministreet