DATASHEET

Rimini Protect™

Application Risk Mitigation (ARM)

Powered by RedShield

PRODUCTS SUPPORTED

Fully managed services can be deployed to enterprise applications, including legacy, third-party, and custom-built applications.

BENEFITS

- **Cost-effective**
- **Adaptive**
- **Tailored**

The Business Challenge

When considering a few recent statistics and the fact that, on average, close to 80 new vulnerabilities per day were submitted to NIST in the form of CVEs in 2023[1], the need to protect your enterprise web applications has never been clearer.

- Web applications were the most breached asset in 2023[2]
- In 2023, it took organizations 204 days to identify a breach and an additional 73 days on average to contain it[3].
- Researchers concluded that 40% of intrusions prioritized data theft in 2022; however, adversaries were observed prioritizing data theft that likely indicates intellectual property theft or espionage-related end goals in 22% of investigations[4].
- The average time for a vulnerability to be exploited once it becomes known was only about 7.5 days in 2021[5].

However, there is a positive side. If industry expert planning assumptions are correct, by 2026 organizations can reduce two-thirds of breaches by prioritizing threat exposure management programs[6].

Rimini Protect™ Application Risk Mitigation (ARM) is an excellent solution for enterprise application and middleware security threat exposure. It provides continuous management of security threats through the detection and mitigation of vulnerabilities in web content, application communications, and internal application access authorization and policies. Rimini Protect™ ARM **continually validates and improves protection** as vulnerabilities relevant to clients are discovered.

The Rimini Street Solution

Enterprise applications communicate with numerous business systems through various network protocols. Rimini Protect™ Application Risk Mitigation (ARM) is designed to monitor and filter communications, remediate vulnerabilities in the communication itself (referred to as “content”), and validate the effectiveness of remediations.

MONITORING AND REMEDIATING COMMUNICATIONS

Incoming network communications for an application are routed for inspection at the network, transport, and application layers of the OSI model[7] using a process similar to a reverse proxy.

1 CVEdetails.com https://www.cvedetails.com/browse-by-date.php
2 Verizon 2023 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/ p18
3 Cost of a Data Breach Report 2023 - Ponemon Institute sponsored by IBM https://www.ibm.com/reports/data-breach p14
4 Mandiant “M-Trends 2023” https://www.mandiant.com/resources/blog/m-trends-2023 p26
5 “How To Implement a Risk-Based Vulnerability Management Methodology” Gartner, Published 20 April 2023 - ID G00777685
6 “Top Trends in Cybersecurity for 2024” Gartner, Published 2 January 2024 – ID G00802944
7 OSI model defined in ISO/IEC 7498 https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Rimini Street

ARM leverages industry-leading technologies:

Infrastructure
- » F5
- » AWS
- » Splunk

Automation
- » Ansible
- » Kubeflow
- » Puppet

Auditing
- » Rapid7
- » Burp Suite
- » Tenable

Assurance
- » Zendesk
- » Site24x7

Protection is applied in two stages:

- The first stage provides the functions of a managed WAF, DDoS, and Bot Controls[8] as a managed service customized to each client.
- The second stage applies "shields," designed to address vulnerabilities that can compromise security.

At either stage, various actions can be taken when a vulnerability is identified:

- The communication can simply be blocked or denied.
- Defined steps can be taken, such as issuing an alert or querying a Muti-Factor Authentication service before permitting the communication to proceed.
- A shield can modify the communication, rendering the attack utilizing a vulnerability benign while allowing communication to proceed in a protected manner.

Rimini Protect™ ARM can inspect and shield a wide range of APIs and application traffic, including HTTPS, HTML, JSON, JavaScript, and even proprietary technology stacks such as SAP by enforcing Secure Network Communications (SNC).

DEVELOPMENT OF SHIELDS

Shields are software programs designed to target vulnerabilities or groups of vulnerabilities, including known and unknown vulnerabilities sharing similar characteristics. Shields can modify the contents of communications, rendering a vulnerability or malicious communication ineffective. Shields are selected and deployed based on each client's needs.

Rimini Protect™ ARM features a collection of shields and configurations known as playbooks that can be used to achieve specific security objectives for each client. A full set of shields and playbooks is available to assist in implementing best practices, ranging from mitigating security risks to enhancing change management and meeting industry standards for compliance.

THE RIMINI DIFFERENCE

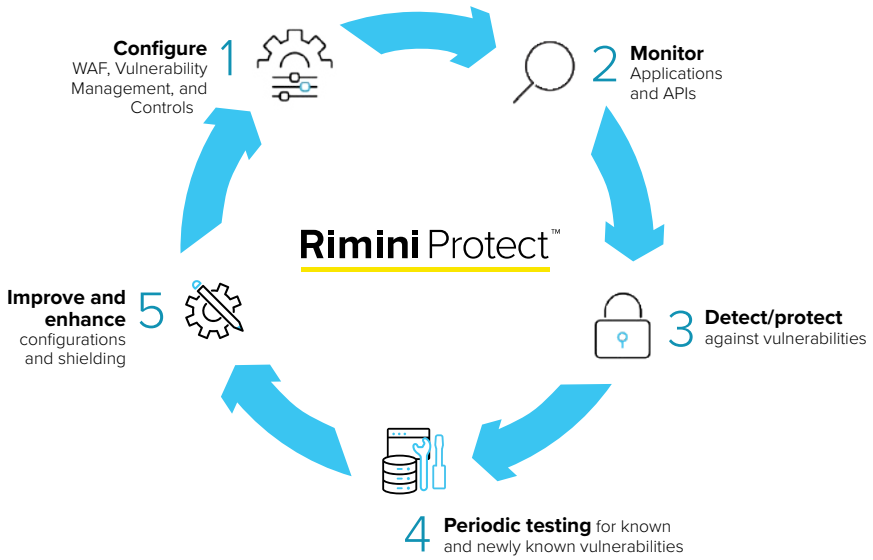
Rimini Protect™ ARM also includes access to a library of supplemental shields developed exclusively for Rimini Street clients. These shields are designed to offer specialized protection to client enterprise software and middleware environments by combining Rimini Street's threat intelligence services, deep knowledge of ERP systems, and additional partner threat research. If a client's unique ecosystem requires additional shields to improve its security posture, additional shields can be custom developed.

CONTINUOUSLY EVOLVING PROTECTION

After deployment, applications are periodically tested against **known and newly identified vulnerabilities and exploits**. Available exploit code is run against protected applications as part of the managed service. Application and API traffic is also scanned at regular intervals to identify new vulnerabilities. If an application or API is found to be vulnerable, the client is notified, allowing the configuration of managed services and/or shields to be adjusted to improve and enhance protection.

8 DDoS, and Bot Controls are features implemented as a part of a Rimini Protect™ ARM cloud deployment.

Rimini Protect™ ARM in Action:



Experience the Rimini Street Difference

Benefits	
Cost Effective	A single control can be leveraged to secure multiple applications minimizing the need for downtime and testing. Fully managed services can be deployed to any web application, including legacy (no longer supported), third-party, and custom-built applications.
Adaptive, Fast Protection	Continuous automated testing can rapidly assess zero-day vulnerabilities and validate effective protection for known vulnerabilities. If necessary, shields can be modified and deployed in hours without downtime or regression testing.
Proactive	Shields can be designed to protect against specific known vulnerabilities or groups of known and unknown vulnerabilities sharing similar characteristics.
Tailored	Managed services for WAF, DDoS, and Bot Controls customized to each client. Select the shields applicable to each client's needs or request custom shield development.
Ease of Deployment	Cloud deployment only requires a DNS change. On-premises installation requires a DNS change and the installation of four virtual machines (configuration is included as a part of managed services).
No Changes to Vendor Code	Protections monitor and remediate communications with enterprise applications requiring no updates to vendor code.
Multiple Use Cases	Use cases include support for Multi-Factor Authentication, file uploads, and monitoring security clouds and JavaScript libraries in real-time.