DATASHEET

Rimini Protect™

Rimini Protect™ for SAP Applications

TECHNOLOGY SECURED

- SAP BusinessObjects (Java)
- SAP NetWeaver and NetWeaver Process Integration
- HTTP/S traffic-based applications
- SOAP integrations

"RedShield's approach to removing vulnerabilities in web applications without touching a single line of application code can help accelerate digital transformation without compromising on security and that's a problem that businesses are facing globally."

Dr. Edward Amoroso, CEO of TAG Cyber

Zero-day, multilayer defenses for SAP applications

Solution Overview

Rimini Protect™ for SAP Applications is an always-on security solution that continuously protects SAP applications from cyberattacks. It is part of a powerful suite of security solutions from Rimini Street that includes Advanced Database Security and Advanced Application and Middleware Security solutions that complement the security advisory and support included in our standard support services.

From security monitoring and threat identification to remediation and reporting, Rimini Protect for SAP Applications is a proactive solution that keeps you ahead of attackers, without disrupting business operations. As a fully managed security service, Rimini Street's security experts take the lead in securing your SAP applications.

Security Challenges and Risks for SAP Environments

SAP ERP (enterprise resource planning) and other enterprise software applications are used by tens of thousands of organizations worldwide. These applications and the data behind them are an alluring target for bad actors. SAP customers are at high risk of ransomware attacks and data breaches that can be costly and disruptive and cause great reputational harm.

Addressing vendor patch strategy risk: Organizations relying primarily on SAP patches to secure their SAP software can be at a significant risk of cyberattacks and exploits until their software is adequately patched. However, SAP may not provide patches in a timely manner. If SAP does provide them, the patches will likely cover only known vulnerabilities and may only be available for product releases that are still covered under mainstream support. Finally, bad actors will use any suitable attack vector to breach a database environment, many of which are not remediated by vendor patches.

Managing vendor vulnerability reports and patches: SAP, like other enterprise software vendors, promotes identifying software vulnerabilities and offering corresponding patches as the primary way to secure their software. However, for many SAP users, patching may not be as secure or simple to implement as they believe. Users will generally

need to test patches before they are applied to verify that applications and customizations will still work properly. Also, vendor patches are typically installed during maintenance windows, which can be narrow or result in planned downtime. In the event of an urgent patch for high-risk vulnerabilities, SAP users could experience unplanned downtime that impacts user productivity.

Increasing security tools and skills: Security operations teams typically use dozens of tools to perform various functions, including web application firewalls (WAFs), security monitoring, performing scans, incident verification and analysis, and forensics. Each of these tools must be operated by trained security experts. Finding and hiring the right experts can be a difficult and costly process.

RedShield, a leader in web application security, removes the risk of web application vulnerabilities. Using the new approach of shielding application vulnerabilities, RedShield works to solve cybersecurity's toughest problems and secure one of the most targeted areas of a business by bad actors, its web applications.

Securing SAP Applications — Enhanced with Technology from RedShield

Rimini Protect for SAP Applications is a comprehensive managed security service built on a foundation of market-leading security technologies. This service was specifically designed to secure SAP applications by combining best-of-breed application-shielding technology from our partner RedShield (https://www.redshield.co) — a recognized leader in web application security — with our extensive expertise in supporting SAP applications and environments. This innovative approach enables Rimini Street to create and deploy SAP-specific shields to secure SAP applications and customizations against known and unknown vulnerabilities.

Rimini Protect for SAP Applications enhances a defense-in-depth strategy, which is a far more comprehensive approach to securing applications than simply relying on vendor patching. Where vendor patching is limited to vendor-provided code, Rimini Protect employs multiple layers of defense to protect applications, data, and related components against a variety of attack vectors.

Two Deployment Models to Choose From

Rimini Street clients have two deployment options for the service: cloud deployment and a private node deployment.

Cloud deployment: This option is a simplified deployment model where web traffic to SAP applications is securely redirected to a cloud security stack that monitors and protects the application and sessions using WAFs and anti-distributed denial of service (DDoS) capabilities.

Private node deployment: This option provides a flexible model that protects web applications by building web application security controls in your locations and keeping your data local.

"Bringing critical systems down in order to apply a patch was problematic, and we didn't have the resources to perform time-consuming regression testing, so our patching was late and infrequent at best. Our previous security strategy wasn't practical, making our databases vulnerable. We knew vendor patches were frequently delayed, plus we couldn't test and apply them quickly. Even if all the stars aligned, our system wasn't equipped to alert us to an attack on our database!"

Ron Traub
Senior Operations Manager, Suburban Propane

BENEFITS OF RIMINI PROTECT FOR SAP APPLICATIONS

- **Bypasses the need for and reliance on updates to SAP source code:**
  SAP-specific shields focus on vulnerabilities and threats and avoid the consequences of code changes such as planning downtime and testing. The service delivers continuous, rapid security protection, without taking applications out of production.

- **Proactively detects and mitigates vulnerabilities:**
  Weekly scanning for auditing and vulnerability discovery validates the effectiveness of shielding to maintain optimal defenses.

- **Offers extensive security controls:**
  The service incorporates many advanced security technologies such as WAFs, anti-DDoS capabilities, security monitoring, incident response, and customized shields to fully protect SAP applications.

- **Reduces cost and complexity:**
  The solution includes best-of-breed capabilities and technologies, combined with expert resources that many organizations would not be able to afford or provide through in-house resources.

- **Increases visibility and confidence:**
  With access to live service status, dashboards, and regular reporting via a portal, you will gain unprecedented insights into the security status of your SAP applications and the steps employed to protect them.

- **Delivers a fully managed security service:**
  Rimini Protect for SAP Applications is a fully managed service, staffed 24x7x365 by our team of security experts. They continually monitor your SAP applications for security alarms and events and respond immediately to all security threats. You do not have to worry about finding security talent and managing operational processes.

Rimini Street