R&S®Web Application Firewall – Enterprise Edition

Extensive Application Security

R&S®Web Application Firewall – Enterprise Edition is the most comprehensive solution offering a full range of features to manage application security at enterprise level. Designed to protect critical business applications, including existing legacy applications and custom APIs from complex attacks while respecting data privacy requirements, it is suitable for any customer environment and supports global high-performance web applications and continuous development of new software.

Key benefits

- All-in-one powerful solution designed for public and private sector enterprise customers who value innovation and flexibility to meet their specific needs
- Helping organizations in a DevOps mode of operation by reducing security risk while improving application performance
- Fully scalable and technology agnostic, allowing to consistently manage applications deployed in multi-cloud or hybrid cloud environments avoiding vendor lock-in and escalating costs
- Able to address the most stringent compliance and audit requirements: PCI DSS, PSD2, NIS Directive, GDPR

ROHDE&SCHWARZ
Cybersecurity

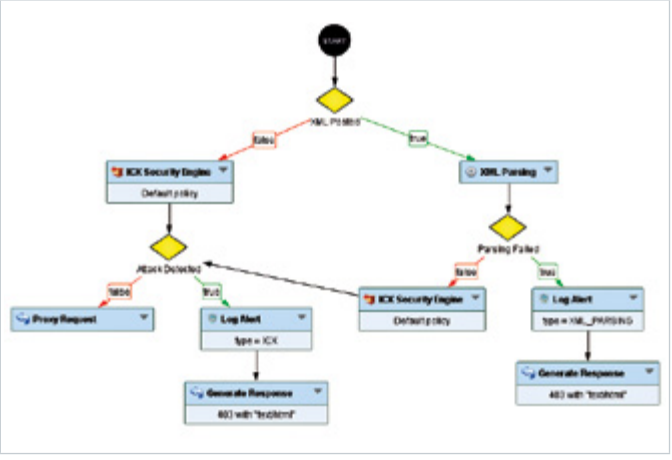
Product Flyer | 01.01

Deployment

- Range of physical and virtual appliances selected and tested for maximum performance (from 21,000 to 100,000 transactions per second)
- Available on AWS and Microsoft Azure marketplaces
- Preconfigured policy templates for standard applications: e.g. Microsoft® SharePoint™, SAP®, WordPress, Drupal
- Active-passive and active-active deployments for high availability
- Supports distributed architectures: multiple DMZs and 'Pooling Mode' for high security deployments

Core Product Capabilities

- Proactive protection against known and unknown threats that can lead to data loss, sabotage, denial of service
- Proven effective against OWASP Top 10 attacks
- Ability to sign, verify signature, encrypt, decrypt, modify any part or entity of request or response
- Standard security based on generic patterns and scoring mechanism complemented by advanced security engines for more granular and accurate detection
- Log replay for policy testing & forensics analysis
- User reputation scoring to prevent online fraud and theft by deterring illegitimate users
- Proactive bot detection and mitigation
- JSON Firewall and XML parsing and validation
- Seamless integration with third party file scanners (ICAP)
- Application learning for stronger protection and improved performance during software development cycle
- Swagger Import / Export for API security and DevOps
- IP Geolocalization



Graphical Workflow Configuration

- Accessible and intuitive management interface
- With a click, switching from blocking to logging mode on all or specific parts of security policy
- Visualization of traffic processing and inspection flows
- Configurable attack response based on context
- Ability to chain multiple security engines via the workflow for accurate detection and reduced rate of false-positives
- Low touch false positives management

Optional Modules:

- **Extended API Security**
  - Securing API-based custom applications & Machine-to-Machine communications
  - XML / JSON ciphering and signature
  - JSON Web Token parsing and generation
- **Web Access Manager**
  - Streamlining user authentication via web SSO
  - Adaptive authentication based on user context
  - Integration with LDAP, AD, Radius
- **IP Reputation**
  - Adding current, comprehensive and actionable threat intelligence feed into security policy
  - Guaranteeing performance optimization by filtering out requests originating from malicious IP sources
  - Reducing the risk of false positives by adjusting the policy based on the origin of request
  - Disregarding requests from unwanted robots
- **Management Console**
  - Dedicated platform for centralized provisioning and management of all devices and applications
  - Automated deployment of application security policy across all instances, including cloud-based
  - Monitoring of web applications in real time
  - Role-based access for distributed management tasks
  - Customizable dashboard with drilldown capability

Services & Support

- Expert technical support team based in Europe
- 24/7 portal to log support tickets for all types of incidents
- 24/7 phone support available as an option
- Product Certification Training for partners and administrators
- Permanent Bug Bounty program run by Data & Application Research Center (DARC)

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3607.6850.32 | Version 01.01 | February 2019 (sch)
R&S®Web Application Firewall – Enterprise Edition

3607685032

3607.6850.32 01.01 PDP 1 en