Because every business needs a Web Application Firewall to protect their core applications and websites, Rohde & Schwarz Cybersecurity built R&S®Web Application Firewall – Business Edition to counter the most common threats such as denial-of-service attacks, data loss and identity theft while maximizing operational efficiency.

**Key benefits**

- Entry-level on-premises solution designed for easy deployment and management with a reduced total cost of ownership
- Actively protecting web applications and web services by filtering and monitoring incoming traffic and blocking attacks
- Helping to cost effectively fulfill industry and compliance requirements: PCI DSS, PSD2, NIS Directive, GDPR
Deployment
- Physical and virtual appliance models for limited bandwidth requirements (up to 21,000 transactions per second)
- Preconfigured policy templates (security, acceleration, authentication) for standard applications: e.g. Microsoft® Outlook Web Access™, Exchange™, SharePoint™ and SAP®, WordPress, Drupal, Joomla
- 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 or sabotage, denial of service
- Effective against OWASP Top 10 attacks
- Ability to sign, verify signature, encrypt, decrypt, modify any part or entity of request or response
- Normalization engine to interpret any HTTP request and prevent hackers bypassing security engines using various encoding techniques
- Blacklist and whitelist engine based on generic signatures for maximum protection against known attacks
- Scoring engine powered by machine learning able to identify real traffic attacks and prevent zero day exploits
- Log replay for policy testing & forensics analysis
- Seamless integration with third party file scanners (ICAP)
- IP Geolocalization

API Security
- Extends security measures to attacks targeting APIs
- Ability to parse and validate schemas, manipulate JSON / XML data
- Ability to detect API-specific attacks, including XML External Entities (XXE)

Graphical Workflow Configuration
- Intuitive management interface for all levels of expertise
- Visualization of traffic processing and inspection flows
- With a click, switching from blocking to logging mode on all or specific parts of security policy
- Configurable attack response based on context
- Low touch false positives management

Optional Modules:
- 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
  - Monitoring of web applications in real time
  - Role-based access for distributed management tasks

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)