Rohde & Schwarz Cybersecurity

R&S®WEB APPLICATION FIREWALL – ENTERPRISE EDITION

R&S®Web Application Firewall – Enterprise Edition bietet den vollen Funktionsumfang zum Management der Anwendungssicherheit auf Enterprise-Level. Sie garantiert optimalen Schutz kritischer Unternehmensanwendungen inklusive Legacy-Anwendungen und benutzerdefinierter APIs vor komplexen Angriffen unter Berücksichtigung von Datenschutzregelungen. Sie eignet sich für alle Kundenumgebungen und unterstützt hochleistungsfähige globale Webanwendungen sowie die stete Entwicklung neuer Software.

Hauptmerkmale

- Hochleistungsfähige Komplettlösung für öffentliche Institutionen und Unternehmen, die Wert auf Flexibilität und Innovationsfähigkeit bei der Erfüllung ihrer spezifischen Anforderungen legen
- Unterstützung im DevOps-Modus durch Reduzierung von Sicherheitsrisiken und Verbesserung der Leistungsfähigkeit von Anwendungen
- Komplett skalierbar und technologieunabhängig für ein konsistentes Management in Multi-Cloud- oder Hybrid-Cloud-Umgebungen
- Kosteneffiziente Einhaltung gesetzlicher Bestimmungen: PCI-DSS, Zahlungsdienstrichtlinie (PSD2), NIS-Richtlinie, EU-DSGVO, OZG

Produkt-Flyer
Version 02.01

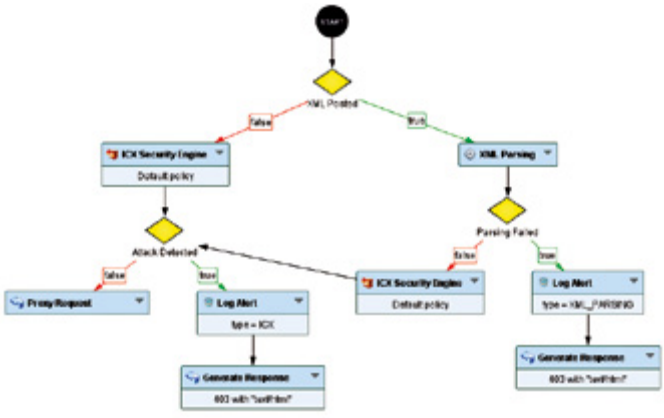
ROHDE&SCHWARZ
Make ideas real

Installation

- Große Auswahl physischer & virtueller Appliances mit zertifiziert hoher Leistungsfähigkeit (21.000 -100.000 Transaktionen/ Sekunde)
- Verfügbar auf Amazon Web Services und Microsoft® Azure™ Marketplace
- Vorkonfigurierte Regelvorlagen für Standard-anwendungen: z. B. Microsoft® SharePoint™, SAP®, WordPress, Drupal
- Aktiv-Passiv- und Aktiv-Aktiv-Installationen für Hochverfügarkeitskonfigurationen
- Unterstützung dezentraler Architekturen: mehrfache DMZ und „Pooling-Modus“ für Hochsicherheitsinstallationen

Leistungsumfang des Kernprodukts

- Proaktiver Schutz vor bekannten und unbekannten Bedrohungen, die Datenverlust, Datensabotage oder Denial-of-Service-Angriffe begünstigen
- Schutz vor allen Angriffen in den OWASP Top 10
- Signieren, Verifizieren von Signaturen, komplette/ teilweise Verschlüsselung, Entschlüsselung oder Modifikation von Anfragen/ Antworten
- Basisschutz mit generischen Mustern und Scoring-Mechanismen, ergänzt durch erweiterte Security-Engines für detailliertere, genauere Erkennung
- Protokollwiedergabe zur Regelprüfung & forensischen Analyse
- Reputation-Scoring, das Betrug und Diebstahl im Internet durch Abwehren illegitimer Nutzer verhindert
- Proaktive Bot-Erkennung und -Entschärfung
- JSON-Firewall, XML-Parsing und -Validierung
- Nahtlose Integration externer Dateiscannern (ICAP)
- Maschinelles Lernen für höchste Sicherheit und Leistungsfähigkeit in der Entwicklung
- Swagger-Import/ Export für API-Sicherheit in DevOps-Umgebungen
- IP-Standortbestimmung



Grafische Workflow-Konfiguration

- Intuitive Managementschnittstelle
- Per Click zwischen Blocken oder Protokollieren aller oder bestimmter Teile der Sicherheitsrichtlinien wechseln
- Visualisierung der Datenverkehrs- und Inspektionsabläufe
- Konfigurierbare, kontextbasierte Angriffsreaktion
- Möglichkeit zur Verkettung mehrerer Sicherheits-vorrichtungen über den Workflow für exakte Erkennung und geringe False Positives
- Einfaches False-Positives-Management

Optionale Module

Erweiterte API-Sicherheit

- Sicherheit benutzerdefinierter API-basierter Anwendungen & M2M-Kommunikation
- Verschlüsselung und Signierung von XML/ JSON
- Parsing und Erstellen von JSON Web Tokens

Web Access Manager

- Effiziente Benutzerauthentifizierung über WebSSO
- Adaptive, kontextbasierte Authentifizierung
- Integration mit LDAP, AD, Radius

IP Reputation

- Verwendung der aktuellsten Bedrohungsdatenbank
- Garantierte Leistungsoptimierung durch Herausfiltern von Anfragen schädlicher IP-Quellen
- Reduziertes Risiko von False Positives durch Sicherheitsregeln nach Ursprung der Anfragen
- Ignorieren von Anfragen unerwünschter Robots

Management Console

- Plattform für zentrale Bereitstellung und Management aller Geräte und Anwendungen
- Automatische Installation auch in cloud-basierten Instanzen
- Monitoring in Echtzeit
- Rollenbasierter Zugriff auf verteilte Managementaufgaben
- Konfigurierbare Dashboards mit Drilldown

Services & Support

- In Europa ansässiges technisches Support-Team
- Durchgängig erreichbares Portal zur Erstellung von Support-Tickets für alle Incident-Typen
- Durchgängig erreichbarer Telefonsupport auf Anfrage
- Zertifizierungstraining für Partner und Administratoren

Rohde & Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

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

PD 3607.6850.31 | Version 02.01 | August 2020 (sch)
R&S®Web Application Firewall – Enterprise Edition
Daten ohne Genauigkeitsangabe sind unverbindlich | Änderungen vorbehalten

3607685031

3607.6850.31 02.01 PDP 1 de