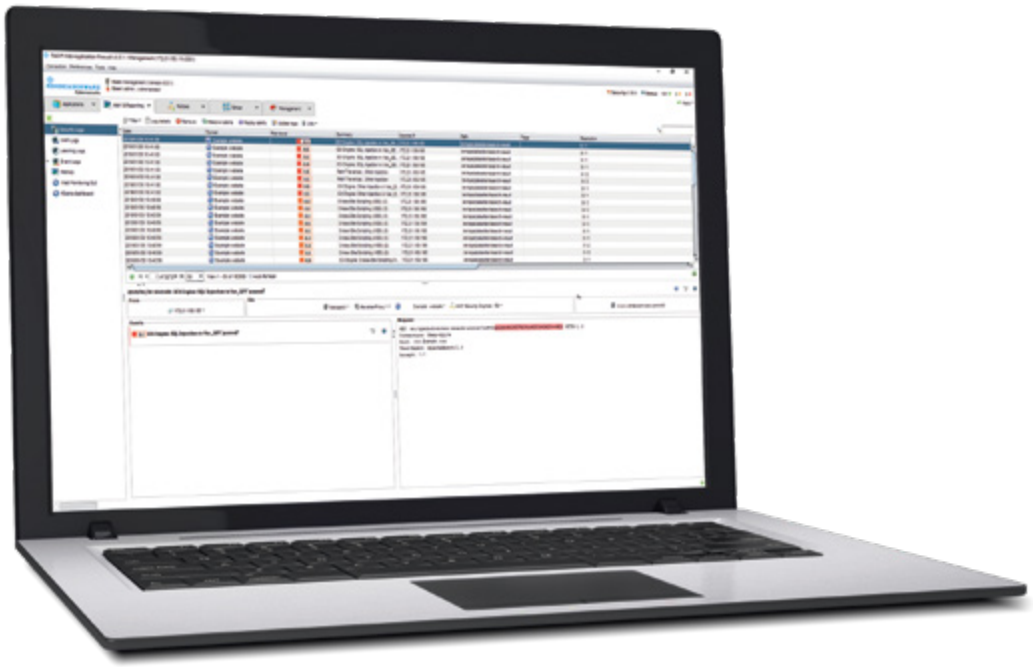
R&S®Web Application Firewall Business Edition

Sécurité applicative essentielle

Parce que chaque entreprise a besoin d'un pare-feu applicatif Web pour protéger ses applications et ses sites Web, Rohde&Schwarz Cybersecurity a conçu R&S®Web Application Firewall – Business Edition pour contrer les menaces les plus courantes telles que les attaques par déni de service, la perte de données et le vol d'identité tout en optimisant l'efficacité opérationnelle.

Avantages clés

- Solution d'entrée de gamme on-premise (sur site) conçue pour un déploiement et une gestion facile avec un coût total de possession réduit
- Protège activement les applications Web et les services Web en filtrant et en surveillant le trafic entrant et en bloquant les attaques
- Aide à répondre de manière efficace aux exigences industrielles et aux normes de conformité : PCI DSS, PSD2, Directive NIS, GDPR



ROHDE&SCHWARZ
Cybersecurity

Dépliant produit | Version 01.00

Déploiement

- Modèles d'appliances physiques et virtuelles pour des besoins limités en bande passante (jusqu'à 21 000 transactions par seconde)
- Modèles de sécurité préconfigurés (sécurité, accélération de performances et authentification) pour les applications standard telles que Microsoft® Outlook Web Access™, SharePoint™ et SAP, WordPress, Drupal, Joomla
- Déploiements actif-passif et actif-actif pour une haute disponibilité
- Supporte des architectures distribuées : plusieurs DMZ et 'Pooling Mode' pour des déploiements de sécurité élevée

Principales fonctionnalités du produit

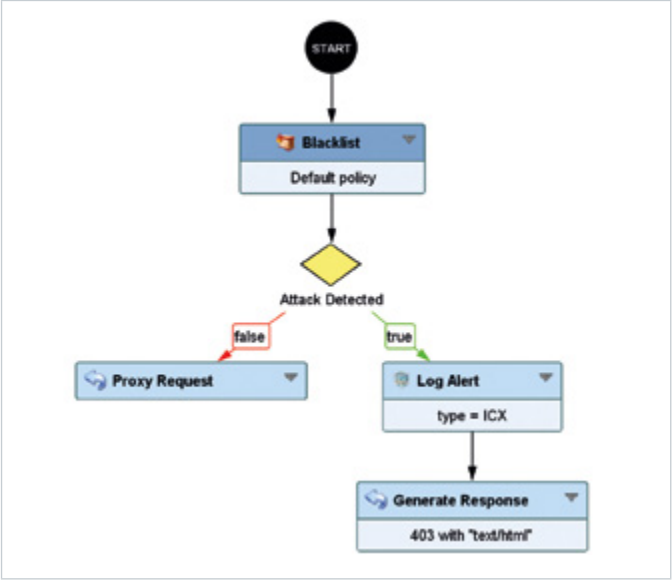
- Protection proactive contre les menaces connues et inconnues qui peuvent entraîner la perte ou le sabotage de données, le déni de service
- Efficace contre les 10 principales attaques de l'OWASP
- Capacité à signer, vérifier la signature, chiffrer, déchiffrer, modifier toute ou partie de la demande ou de la réponse
- Moteur de normalisation pour interpréter toute requête HTTP et empêcher les pirates de contourner les moteurs de sécurité en utilisant différentes techniques d'encodage
- Moteur de blacklist et de whitelist basé sur des signatures génériques pour une protection maximale contre les attaques connues
- Moteur de scoring alimenté par un système de machine learning pour identifier les attaques réelles du trafic et prévenir les exploitations de type Zero Day
- Rejeu des logs pour tester les politiques et mener une analyse forensic
- Intégration transparente avec des scanners de fichiers tiers (ICAP)
- Géolocalisation des IP

Sécurité des API

- Étend les mesures de sécurité aux attaques ciblant les API
- Possibilité d'analyser et de valider des schémas, de manipuler des données JSON / XML
- Capacité de détecter les attaques spécifiques à l'API, y compris XML External Entities (XXE)

Configuration graphique du workflow

- Interface de gestion intuitive pour tous les niveaux d'expertise
- Visualisation du traitement du trafic et des flux d'inspection
- Réponse d'attaque configurable en fonction du contexte
- Gestion minimisée des faux positifs
- En un clic, passer d'un mode de blocage à un mode d'enregistrement sur toutes ou parties de la politique de sécurité



Modules en option :

- **IP Reputation**
  - Ajouter à la politique de sécurité une base de connaissances des menaces à jour
  - Garantir l'optimisation des performances en filtrant les requêtes provenant de sources IP malveillantes
  - Minimiser les faux positifs en ajustant la politique en fonction de l'origine des requêtes
  - Ignorer les demandes de robots non désirés
- **Console de Management**
  - Plate-forme centralisée dédiée pour la configuration et la configuration de toutes les instances et applications
  - Gestion des applications web en temps réel
  - Accès basé sur les rôles pour les tâches de gestion distribuée

Services & Support

- Équipe support technique basée en Europe
- Portail 24/7 pour la gestion des tickets de support pour tous types d'incidents
- Assistance téléphonique 24h/24 et 7j/7 en option
- Formation certifiante des produits à destination des partenaires et des administrateurs
- Programme Bug Bounty permanent géré par le Data & Application Research Center (DARC)

Rohde&Schwarz Cybersecurity SAS
Parc Tertiaire de Meudon
9-11 Rue Jeanne Braconnier | 92366 Meudon, France
Info: +33 (0)1 46 20 96 00
Email: sales-fr.cybersecurity@rohde-schwarz.com

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Allemagne
www.rohde-schwarz.com/cybersecurity

PD 3607.6838.33 | Version 01.00 | mars 2019 (sch)
R&S®Web Application Firewall – Business Edition
Données sans tolérance : sans obligation | Sous réservé de modification

3607683833

3607.6838.33 01.00 PDP 1 fr