R&S®Web Application Firewall Enterprise Edition

Sécurité renforcée des applications

R&S®Web Application Firewall – Enterprise Edition est la solution la plus complète offrant une large gamme de fonctionnalités pour gérer la sécurité des applications pour les entreprises. Elle est conçue pour protéger les applications métier les plus critiques – y compris les applications existantes et les API personnalisées – contre les attaques les plus complexes tout en respectant la confidentialité des données. Elle s'adapte à tous les types d'environnement client et supporte les applications Web à hautes performances ainsi que le développement continu de nouveaux logiciels.

Avantages clés

- Solution puissante tout-en-un, conçue pour les entreprises des secteurs public et privé qui valorisent l'innovation et la flexibilité pour répondre à leurs besoins spécifiques
- Aider les organisations dans un mode de fonctionnement DevOps en réduisant les risques de sécurité tout en améliorant les performances des applications
- Entièrement évolutive et agnostique sur le plan technologique, elle permet de gérer de manière cohérente les applications déployées dans des environnements cloud, multi-cloud ou hybrides et évite l'adhérence au fournisseur ou les hausses de coûts
- Capable de répondre aux exigences les plus rigoureuses en matière de conformité et de contrôle : PCI DSS, PSD2, Directive NIS, RGPD

ROHDE&SCHWARZ
Cybersecurity

Dépliant produit | Version 01.00

Déploiement

- Large gamme d'appliances physiques et virtuelles sélectionnées et testées pour des performances maximales (de 21 000 à 100 000 transactions par seconde)
- Disponible sur les places de marché AWS et Microsoft® Azure™
- Modèles de sécurité préconfigurés pour les applications standard telles que Microsoft® SharePoint™, SAP, WordPress, Drupal
- Déploiements actif-passif et actif-actif pour une haute disponibilité
- Supporte les architectures distribuées : plusieurs DMZ et 'Pooling Mode' pour des déploiements avancés

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
- Sécurité standard basée sur des patterns génériques et un mécanisme de scoring combiné avec des moteurs de sécurité avancés pour une politique plus granulaire
- Rejeu des logs pour tester les politiques et mener une analyse forensic
- Scoring de réputation des utilisateurs pour prévenir la fraude et le vol en bloquant les utilisateurs illégitimes
- Détection et mitigation proactives des robots
- Pare-feu JSON et parsing et validation XML
- Intégration facile avec des scanners de fichiers tiers (ICAP)
- Mode apprentissage des applications pour une protection renforcée et de meilleures performances pendant le cycle de développement logiciel
- Import/Export de swagger pour la sécurité des API dans un environnement DevOps
- Géolocalisation des IP

Configuration graphique du workflow

- Interface de gestion intuitive pour tous les niveaux d'expertise
- Possibilité de passer d'un mode de bloquant à un mode journalisation sur toutes ou certaines parties de la politique de sécurité
- Visualisation du traitement du trafic et des flux d'inspection
- Configuration de la réponse d'attaque en fonction du contexte
- Capacité à 'enchaîner' plusieurs moteurs de sécurité via le workflow pour une détection précise et pour réduire les faux positifs
- Gestion simplifiée des faux positifs

Modules en option :

- **Extented API Security**
  - Sécurité des API d'applications personnalisées et des communications de machine à machine
  - Chiffrement et signature XML/JSON
  - Analyse et génération de Tokens Web JSON
- **Web Access Manager**
  - Simplification de l'authentification des utilisateurs via le web SSO
  - Authentification adaptée au contexte utilisateur
  - Intégration avec LDAP, AD, Radius
- **IP Reputation**
  - Ajout de renseignements sur les menaces à jour à la politique de sécurité
  - Garantie l'optimisation des performances en filtrant les requêtes provenant de sources IP malveillantes
  - Réduction du risque de faux positifs en ajustant la politique selon l'origine des demandes
  - Ignore les requêtes de robots non désirés
- **Console de Management**
  - Plate-forme unique pour la configuration et la gestion centralisée de toutes les instances et applications
  - Déploiement automatisé de la politique de sécurité des applications au travers de toutes les instances, incluant le cloud
  - Surveillance 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 produit et certification pour les partenaires et 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 3607.6850.33 | Version 01.00 | mars 2019 (sch)
R&S®Web Application Firewall – Enterprise Edition
Données sans tolérance : sans obligation | Sous réservé de modification

3607685033

3607.6850.33 01.00 PDP 1 fr