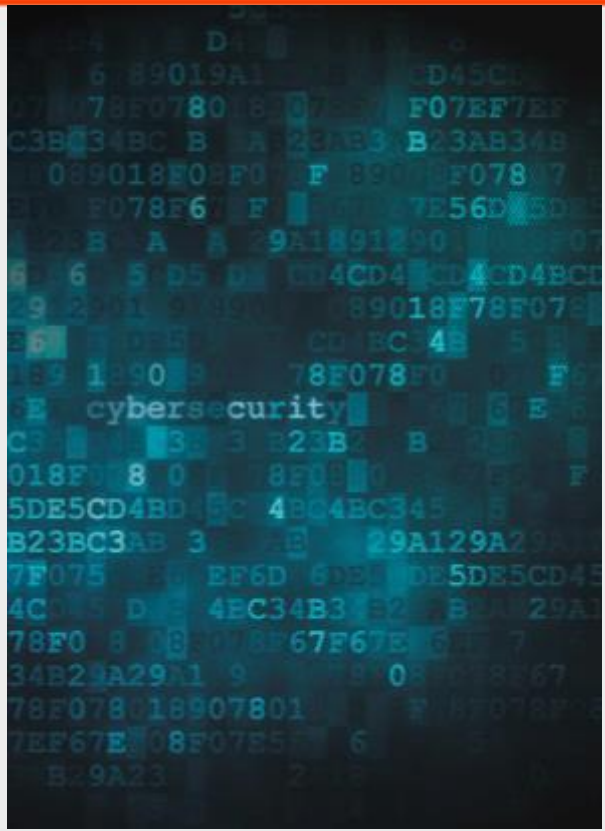
Rohde & Schwarz Cybersecurity

Stéphane de Saint Albin

Profitez d'une vie digitale sécurisée

Rohde & Schwarz Cybersecurity

- **Des solutions de sécurité certifiées et primées**
- **+20 ans d'expérience en sécurité informatique**
- **7 centres de compétence en Allemagne, en France et au Danemark**
- **450 employés**
- **Stratégie de croissance**
  - Combine 5 entreprises européennes innovantes de sécurité informatique
  - Devenir leader européen de la cybersécurité



Le fournisseur européen de confiance pour la Cybersécurité

Sécurité des communications
Applications et périphériques de chiffrement vocal
Messagerie sécurisée
Cryptage fax et radio

Gestion de confiance
CA, PKI, HSMs
Gestion des cryptes
Configuration, politique
Déploiement du microprogramme

ROHDE&SCHWARZ Cybersecurity

Des solutions de confiance d'une source unique

Sécurité endpoints
Chiffrement de disque
Navigation sécurisée
Bureau et mobile sécurisés

Sécurité des applications
Web Application Firewall
Web Services Firewall
Web Access Management
Dynamic Application Security Testing
Document-centric encryption

Chiffrement WAN / Réseau
Cryptage IP de couche 3
Cryptage Ethernet de couche 2
Accès distant sécurisé

Sécurité et analyse des réseaux
Pare-feu NexGen & UTM
Gestion des vulnérabilités
Inspection profonde des paquets DPI

DenyAll en quelques mots…

15

ANNEES D'EXPERIENCE DANS LA SECURITÉ APPLICATIVE

Certification et Qualification de 1er Niveau pour les WAFs

Co-fondateur de l'alliance pour la cybersécurité et la confiance numérique

Visionnaire dans le Magic Quadrant WAF 2015

Siège à Paris
70 personnes
dont 30 en R&D
Commerciaux à travers l'EMEA

+60 000

Applications protégées

600

Clients toutes industries dans 30 pays

DETECT **PROTECT**

App Web & Web Services

MANAGE **CONNECT**

35%

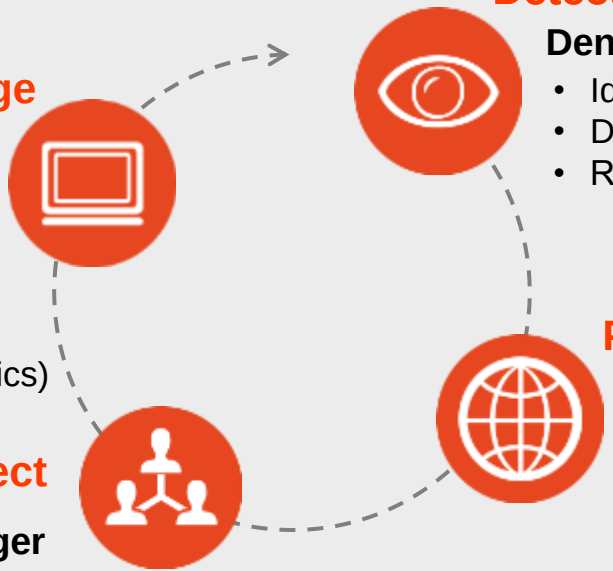
de CA à l'international

Ils nous font confiance

EDF, STIHL, edp, Allianz, Ministère de l'Intérieur, VEOLIA WATER, JCDecaux, Deloitte., DARTY, BOSCH SIEMENS, SAFRAN, Aktia, bouygues, BPCE, NATIXIS, gemalto, AIRBUS, ROHDE&SCHWARZ, RENAULT, Danske Bank, CRÉDIT AGRICOLE, VSC technologies


denyall
a Rohde & Schwarz Cybersecurity company
Gamme DenyAll

Outils de sécurité applicative pour l'ère digitale



Detect

DenyAll Vulnerability Manager

- Identifier les actifs
- Détecter et prioriser les vulnérabilités
- Remédier, réduire la surface d'attaque

Protect

DenyAll Web Application Firewall
DenyAll Web Services Firewall

- Bloquer les attaques, empêcher la fuite de données, le vol d'identités
- Sécuriser APIs et communications machine-à-machine
- Evaluer la réputation des utilisateurs

Connect

DenyAll Web Access Manager

- Appliquer la politique d'authentification
- Simplifier la sécurité pour les utilisateurs (SSO)
- Adapter l'authentification au contexte

Manage

Tous produits DenyAll

- Simplifier déploiement
- Automatiser la réponse aux comportements dangereux
- Monitoring et reporting, analyse à posteriori (forensics)

Le WAF de nouvelle génération

1. Découverte et test des applications
2. Protection efficace des applis et Services Web
3. Simplifier et sécuriser l'accès aux applications
4. Cout de possession faible, environnement ergonomique

Detect

- Trouver et profiler les apps, identifier leurs vulnérabilités
- Prioriser et remédier les vulnérabilités, assigner des tâches
- Tester au travers du WAF pour affiner la politique (patching virtuel)

Protect

- Bloquer les attaques ciblant apps et services Web
- Sécurité négative et positive, heuristique, détection avancée
- Analyser le comportement utilisateur dans son contexte

Connect

- Appliquer la politique d'authentification aux applis Web
- Web Single Sign On (apprendre et rejouer)
- Adapter l'authentification au contexte et comportement

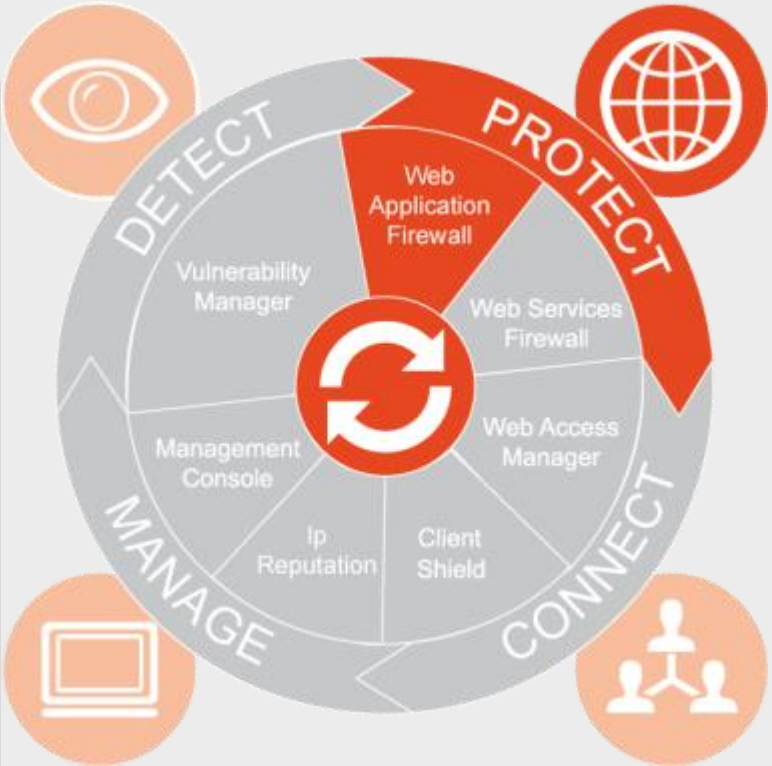
Manage

- Politique définie visuellement (workflow), apprentissage
- Déploiement industriel en environnement hybride (APIs)
- Gouvernance centrale (monitoring, alerting, reporting)

DenyAll Web Application Firewall (WAF)

FONCTIONS CLÉS

- Définition visuelle de la politique de sécurité et des flux (workflow)
- Automatisation de la sécurité des applications
- Apprentissage des applications (HTTP et REST)
- Moteurs de sécurité multiples :
  - ICX (signatures génériques)
  - Liste de pointage (heuristique)
  - Moteurs avancés de détection (analyse grammaticale)
- Protection contre les robots
- Scoring de la réputation des utilisateurs
- Patching virtuel
- Tableau de bord personnalisable pour la surveillance et le reporting



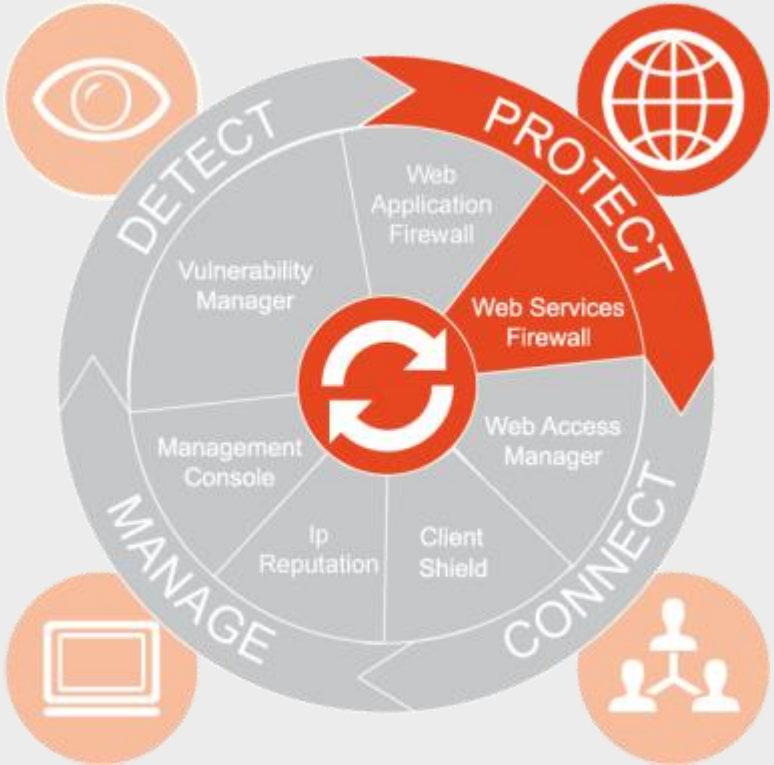
DIFFÉRENCIATEURS

- Environnement d'administration productif
  - Configuration par workflow
  - Profilage, politiques prédéfinies
  - Apprentissage du trafic (sitemap)
  - API d'orchestration
- Efficace contre les attaques OWASP Top 10 & zéro day, les robots et les tentatives d'évasion
  - Sécurité positive et négative
  - Chaînage de moteurs multiples pour une sécurité maximale et efficace
- Ajuster la réponse à l'évolution du contexte et du comportement des utilisateurs
- Capacités complémentaires:
  - Web Services Firewall pour sécurité et routage Ides APIs et Web Services
  - Web Access Manager pour Web SSO et Authentification Adaptive
  - Intégration avec DenyAll Vulnerability Manager

DenyAll Web Services Firewall (WSF)

FONCTIONS CLÉS

- Définition visuelle de la politique de sécurité et des flux (workflow)
- Routage des Web services
- Apprentissage du trafic REST (sitemap)
- Validation du schéma XML / SOAP
- Signature et chiffrement des messages XML
- Authentification des membres du web service
- Signatures d'attaque spécifiques aux Web services
- Patching virtuel
- Tableau de bord personnalisable pour la surveillance et le reporting



DIFFÉRENCIATEURS

- Environnement d'administration productif
  - Configuration par workflow
  - Profilage, politiques prédéfinies
  - Apprentissage du trafic (sitemap)
  - API d'orchestration
- API Gateway combinée avec sécurité des Web services de première classe
- Routage et filtrage SOAP / XML & REST / JSON
- Validation des messages et de l'ntégrité des données
- Signature et chiffrement XML
- Autonome ou intégré avec le WAF

RENAULT

Bénéfices

- Fiabilité des plateformes
- Facilité d'usage 40 workflows pour 300 applications
- Management centralisé
- Respect des réglementations en vigueur

Solution

- Les solutions WAF et web services sont déployées sur 50 appliances protègeant plus de 300 applications depuis le datacenter en France. Russie, Iran et Chine. Solution de Web SSO aussi

Client

RENAULT est le 4eme constructeur mondial d'automobiles.

Renault regroupe 117 000 collaborateurs dans le monde. Renault est implanté dans 128 pays

Problématique

- Besoin de protéger les applications pour les concessionnaires, la DMZ interne et la DMZ donnant accès au réseau partagé avec les partenaires et fournisseurs
- Sensibilité et criticité de certaines activités du groupe impliquant le respect des réglementations


denyall
a Rohde & Schwarz Cybersecurity company
Browser in the Box

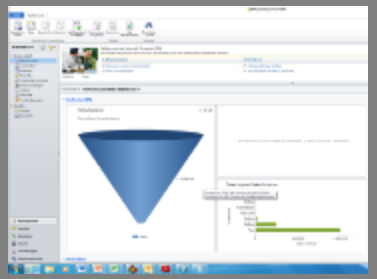
BitBox : surfer en sécurité sur Internet

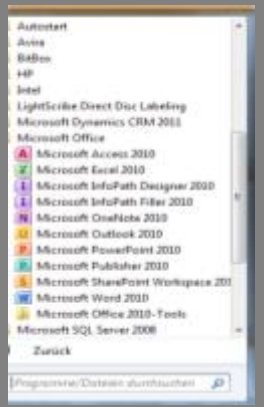
- **La technologie**
  - L‘isolement du navigateur web via la virtualisation
- **Caractéristiques**
  - Haute sécurité en conservant toutes les fonctionnalités du web
    - Isolement de bureau contre internet
    - Transparent à l’utilisateur
  - Économique en utilisant les ressources du client existantes
    - Facile à installer et une administration centralisée

Deux stratégie de navigation

INTRANET

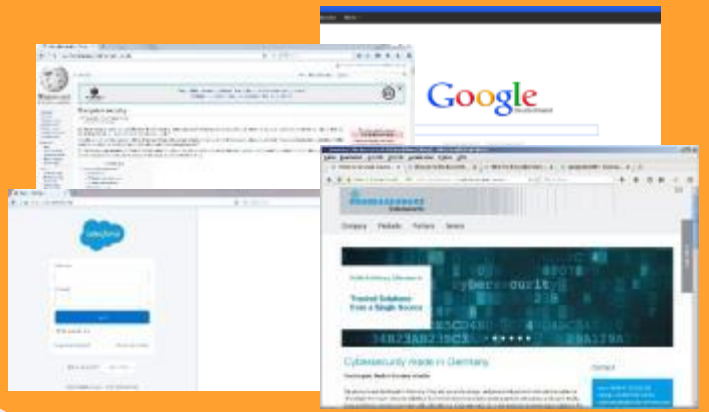
- Les applications web locale
- Propriété intellectuelle
- Concept stratégique
- E-mails





BROWSER IN THE BOX (BitBox)

- Applications web commerciale
- Applications et services web
- Recherche



Fonctions de sécurité BitBox

- **Isolation par machine virtuelle (VM)**
- **Isolation avec un compte BitBox**
- **Analyse de sécurité de la technologie VM avec l'Office fédéral de la sécurité de l'information (BSI, Allemagne)**
- **Linux endurci comme système d'exploitation (OS)**
- **Démarrage à zéro, snapshot signé**
- **Tunnel IPsec sécurisé vers la passerelle, seules les données de BitBox sont acheminées vers Internet (et vice versa)**
- **Mise à jour sécurisée (uniquement des images signées)**


denyall
a Rohde & Schwarz Cybersecurity company
Gamme SITLine ETH

R&S SITLine ETH : chiffreurs Ethernet

- **Transmission sécurisée en temps réel pour les réseaux de communication**
  - Réseaux filaires
  - Réseaux hertziens
  - Réseaux satellites

Réduction des coûts de système

- **Installation et configuration aisées**
  - Technologie Plug&Play
  - Installation rapide dans l'architecture, peu d'impact
- **Faibles consommations énergétiques**
  - Compact, taille réduite 1U, consommation faible, multiports pour quatre lignes physiques
- **Coûts de transmission inférieurs à ceux du Managed IP**
  - Chiffrement Ethernet réduit le débit entre 0% et 13%
  - Chiffrement VPN/IPsec (Layer 3) impact le débit utile jusqu'à 60%
- **Réduction des coûts de maintenance et de mise à jour**
  - Indépendants des nouvelles applications des clients
  - Indépendants des opérateurs
  - Indépendants des versions de protocole IPV4 et IPV6

Réduction des coûts de système

- **Meilleure utilisation de la bande passante**
  - Chiffrement de groupe (Multipoint). Optimisé pour la visioconférence
  - Chiffrement du Multicast : Les données sont chiffrées et émises une seule fois indépendamment du nombre de destinataires. Ce n'est pas le cas du VPN
- **Pas de serveurs de clés centralisés ou dédiés**
  - Les appareils organisent le chiffrement de manière autonome sans composants externes. La panne d'un appareil n'a pas d'impact sur le reste du réseau.

6 raisons de choisir SITLine Eth

1. **A destination des environnements et applications en temps réel**
   - Transport et ferroviaire, Aviation civile et militaire, échanges financier, VoIP, Video HD, Streaming, VOD
2. **Chiffrement totalement indépendant des applications métiers et des services opérateurs**
   - La confidentialité et la sécurité est assurée directement chez le client
3. **Solution de haute sécurité avec sa PKI et son CA**
   - Plusieurs profils d'administration avec authentification basée sur des cartes à puce
   - Personne ne peut accéder aux chiffreurs ni même les admin en charge du réseau
4. **Indépendant de la couche transport IP/MPLS**
   - Modification ou dysfonctionnement du réseau opérateur sans impact sur la sécurité des données clients
   - Possibilité de choisir les liens les moins chers chez l'opérateur
5. **Meilleure performance et temps de latence inférieur à 3 micro sec**
   - Ipsec ne peut offrir des performances équivalentes
6. **MTBF > 7 ans**
   - Pas besoin de Cluster

Merci !

Stéphane de Saint Albin
VP Stratégie
Mobile : +33 622 560 150
sdesaintalbin@denyall.com