Security by Design and Scalability Using DPI Technologies in IoT Context

Dirk Czepluch
Managing Director
IPOQUE, a Rohde Schwarz company

ROHDE&SCHWARZ

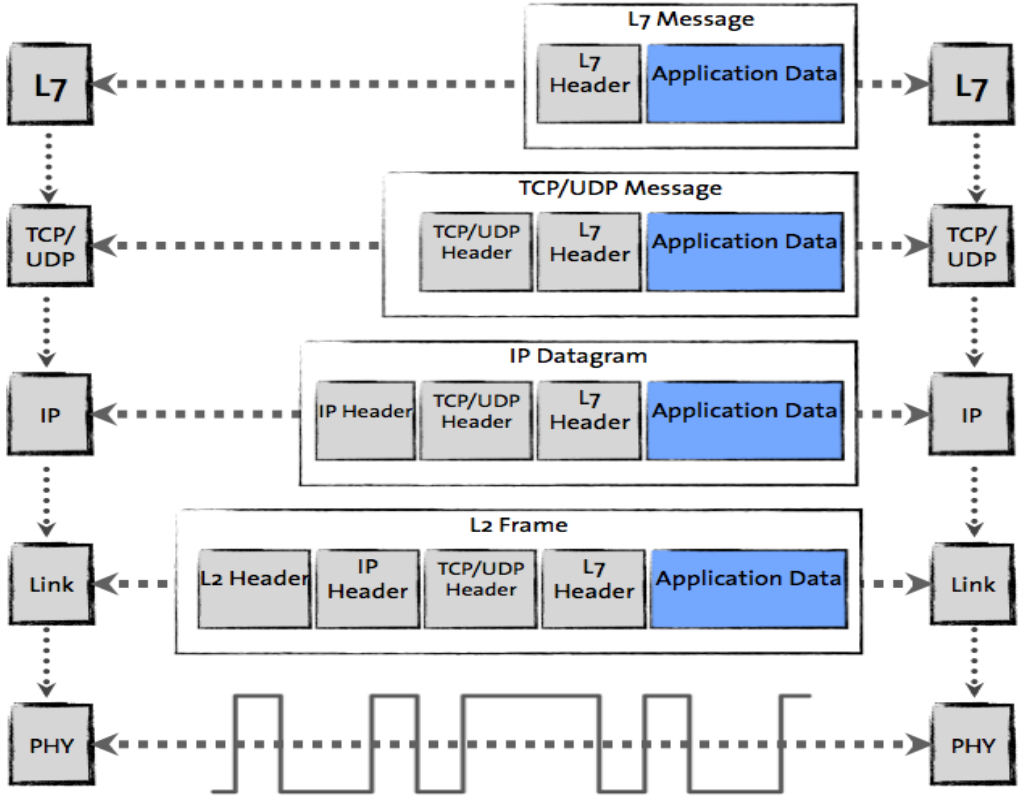
TECHNICAL MOTIVATION FOR DPI

- Problem: Network convergence
  - The Internet (IP Layer) is practically a single service network
  - Different applications have the different requirements

- Solution: Identify applications to manage them
  - Differentiated application/protocol handling requires reliable identification

APPLICATION IDENTIFICATION?

- TCP/UDP ports
  - Communication endpoints for programs (L7 Applications)
  - Encoded in L4 header --> efficient lookup possible
- Port assignment by IANA
  - “Well known ports”
  - Best effort/ rely on cooperation
  - Potential abuse



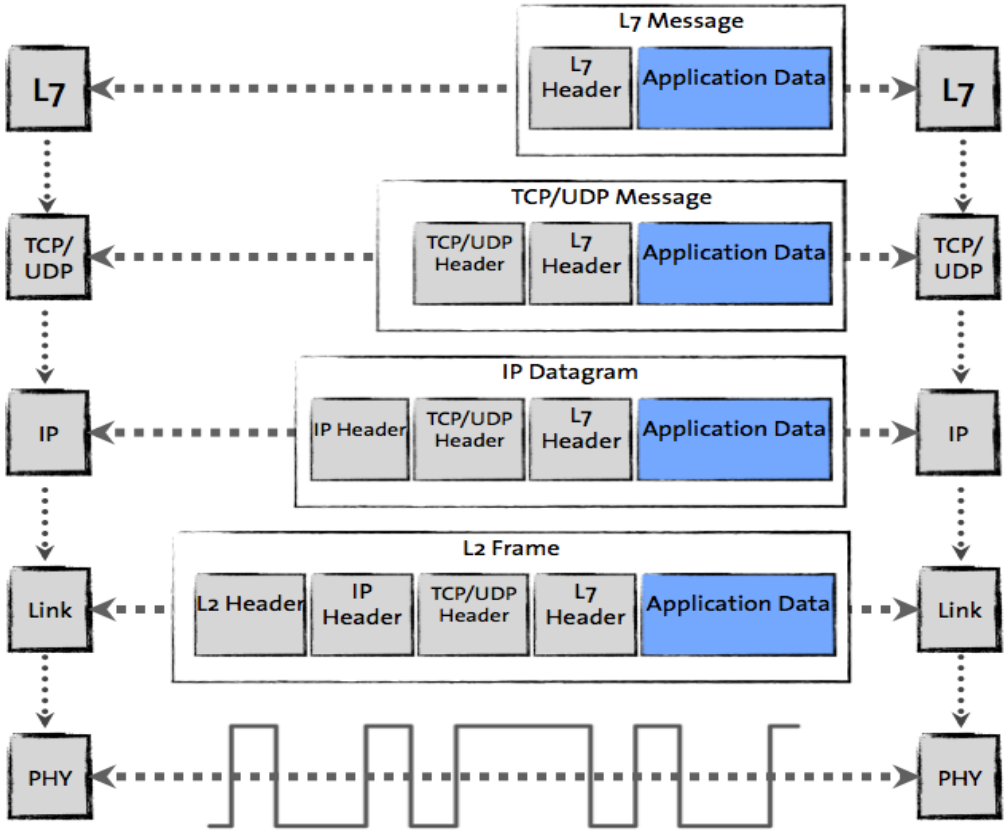
DPI SOLVES THE PROBLEM

- Use case: IP packet processing
  - Pros:

  Reliable application identification on Network Layer (IP)
  - Cons:

  Breaks encapsulation and layer isolation paradigm of ISO/OSI model

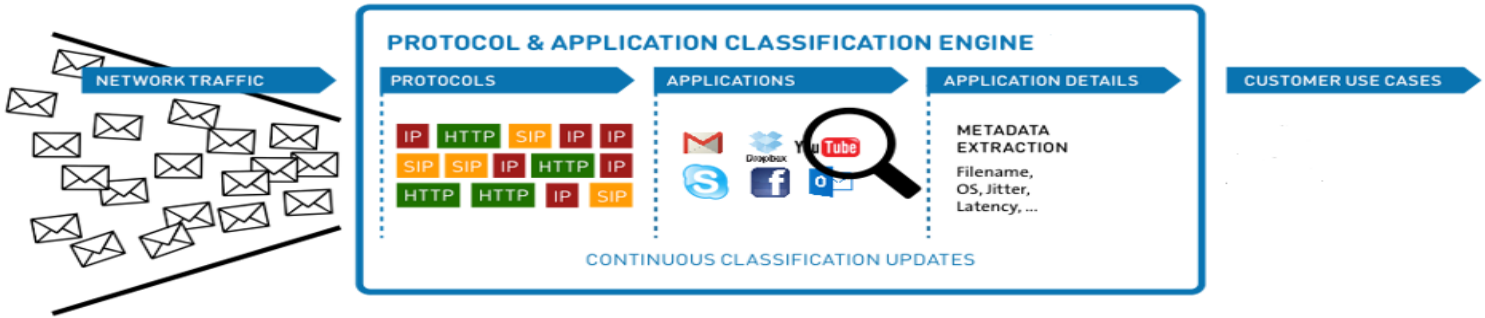
  Protocol detection usually not in first packet



System details
Protocol application detection capability

Tunnels support

ComodoUnite, CyberGhost, GRE, GTP, HTTPTunnel, HamachiVPN, IP in IP, IPSEC, ISAKMP, JAP, L2TP, MPLS, NetMotion, OpenVPN, PDProxy, PPP, PPTP, SSL, SSTP, Socks, SoftEthernet, TOR, Teredo, UltraSurf, VPN-X, VTUN, YourFreedom



DPI APPLICATIONS

- Traffic Management/Policy Enforcement
  - Bandwidth Optimization
  - QoS and QoE assurance
  - Data Plan Enforcement
- Security/ NG Firewalls:
  - Allow/Block Applications and Protocols
  - Virus scan in sensitive traffic only
- Network Probing
  - Statistics & Reporting
  - Traffic Forwarding
  - Test and Measurement

Net Sensor hardware platforms

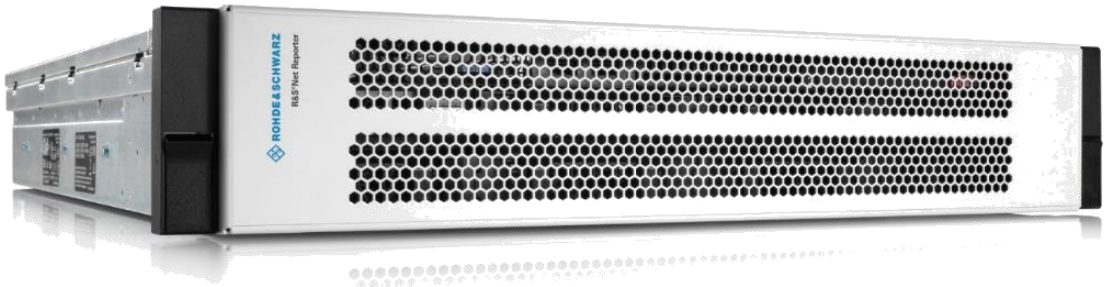
FP30 best suited for:
Small installations, low throughput, 1Gbps lines

FP60 best suited for:
Medium installations, low to medium throughput, 1Gbps and 10 Gbps lines

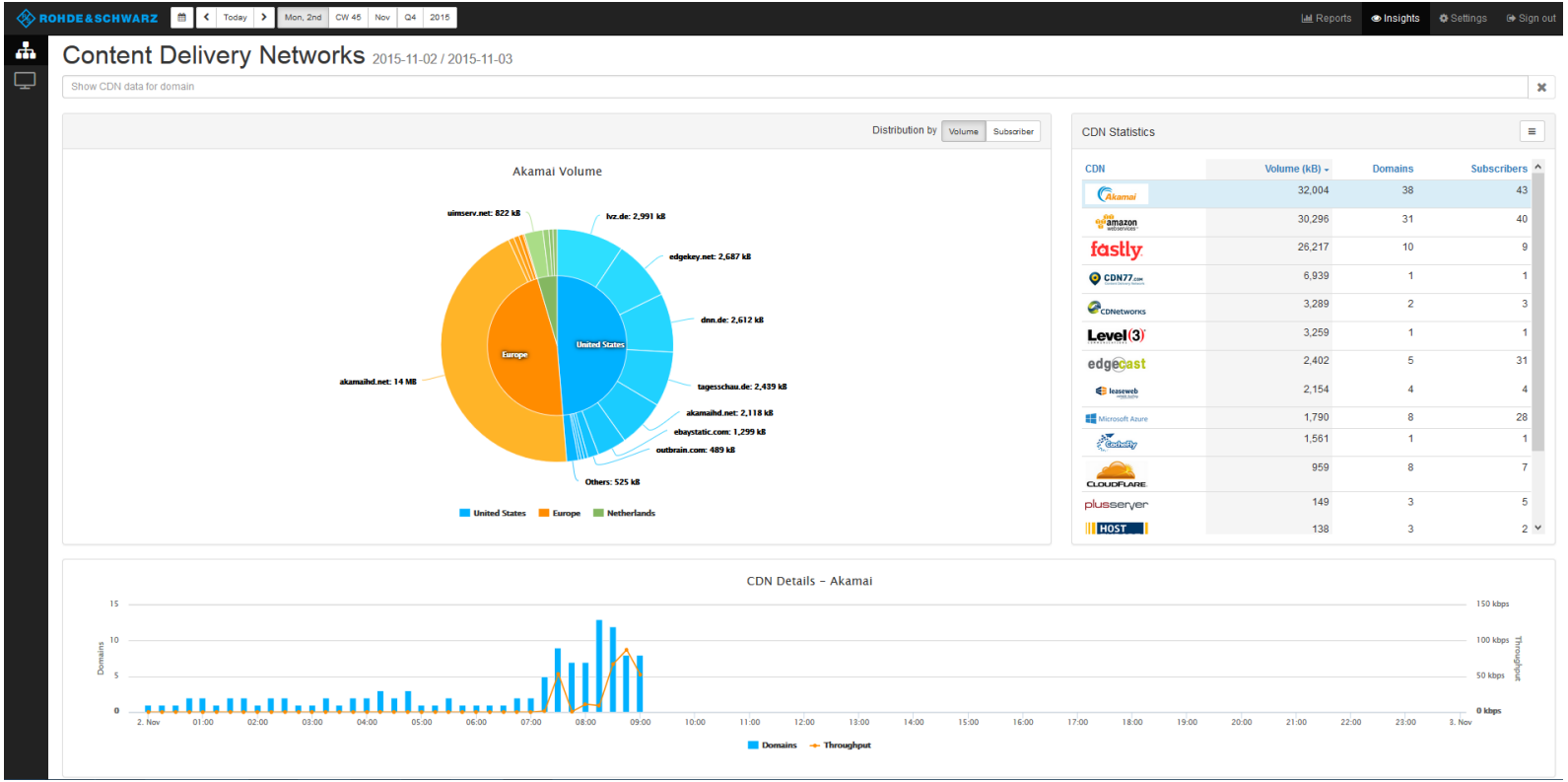
FP61 best suited for:
Larger installations, medium to high throughput, 1Gbps, 10 Gbps and 40 Gbps lines

Net Reporter capabilities

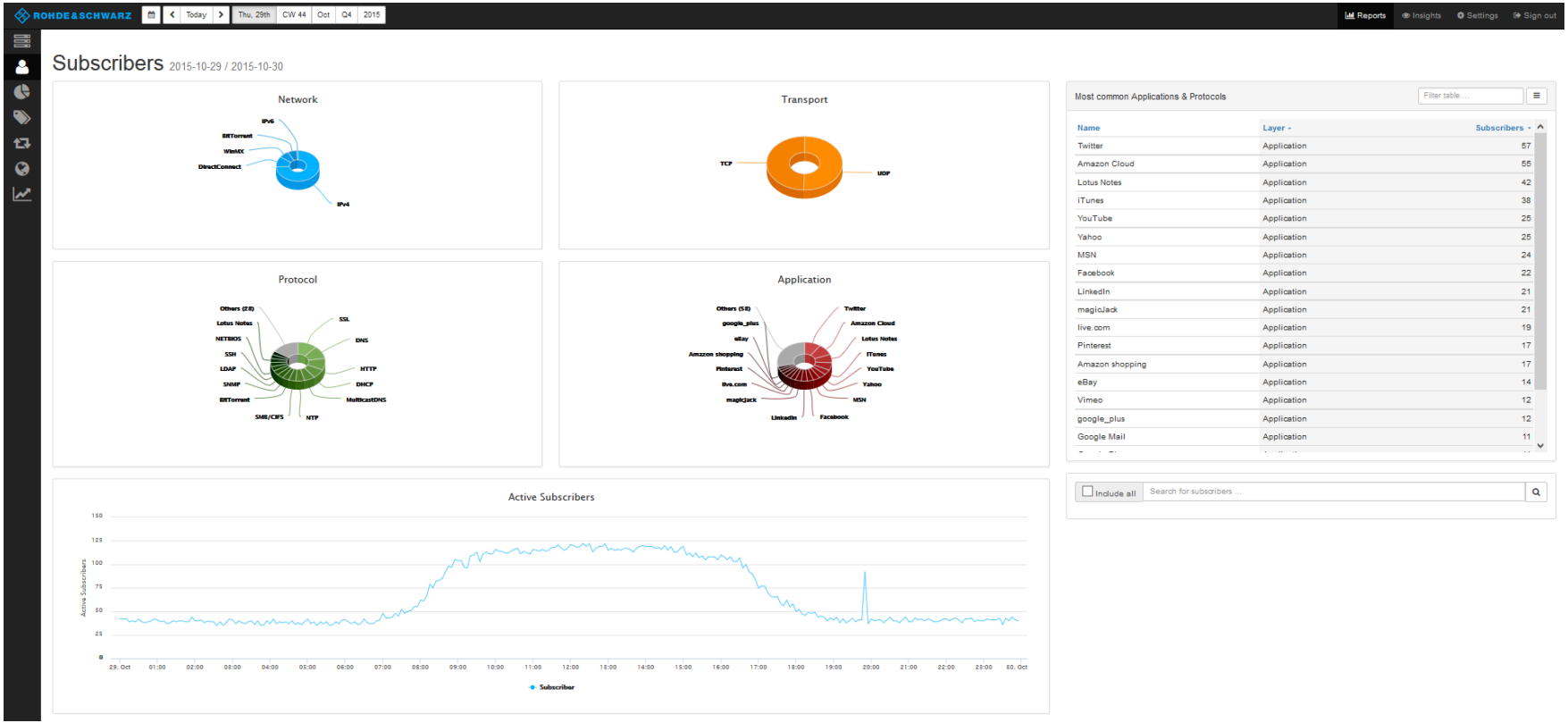
- Leverages ipoque's core technology, PACE (Protocol & Application Classification Engine)
- Turns protocol and application classification into valuable information
- Ties protocol and application information to subscriber groups, devices, data plans and more
- Provides APIs for integration with 3rd party systems (Big Data, CRM)
- Powerful operations on data
- Easy-to-use UI or direct access to analytics DB



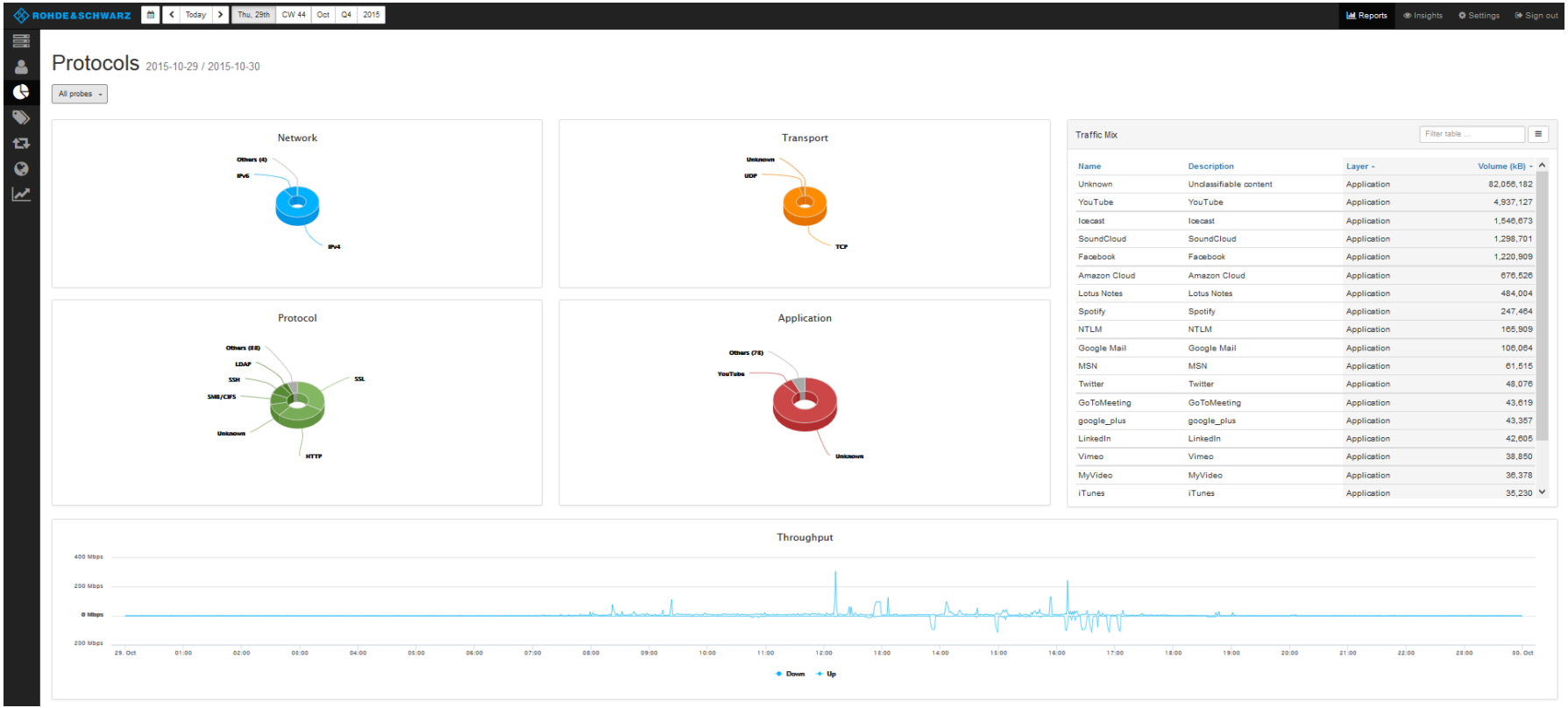
Net Reporter UI



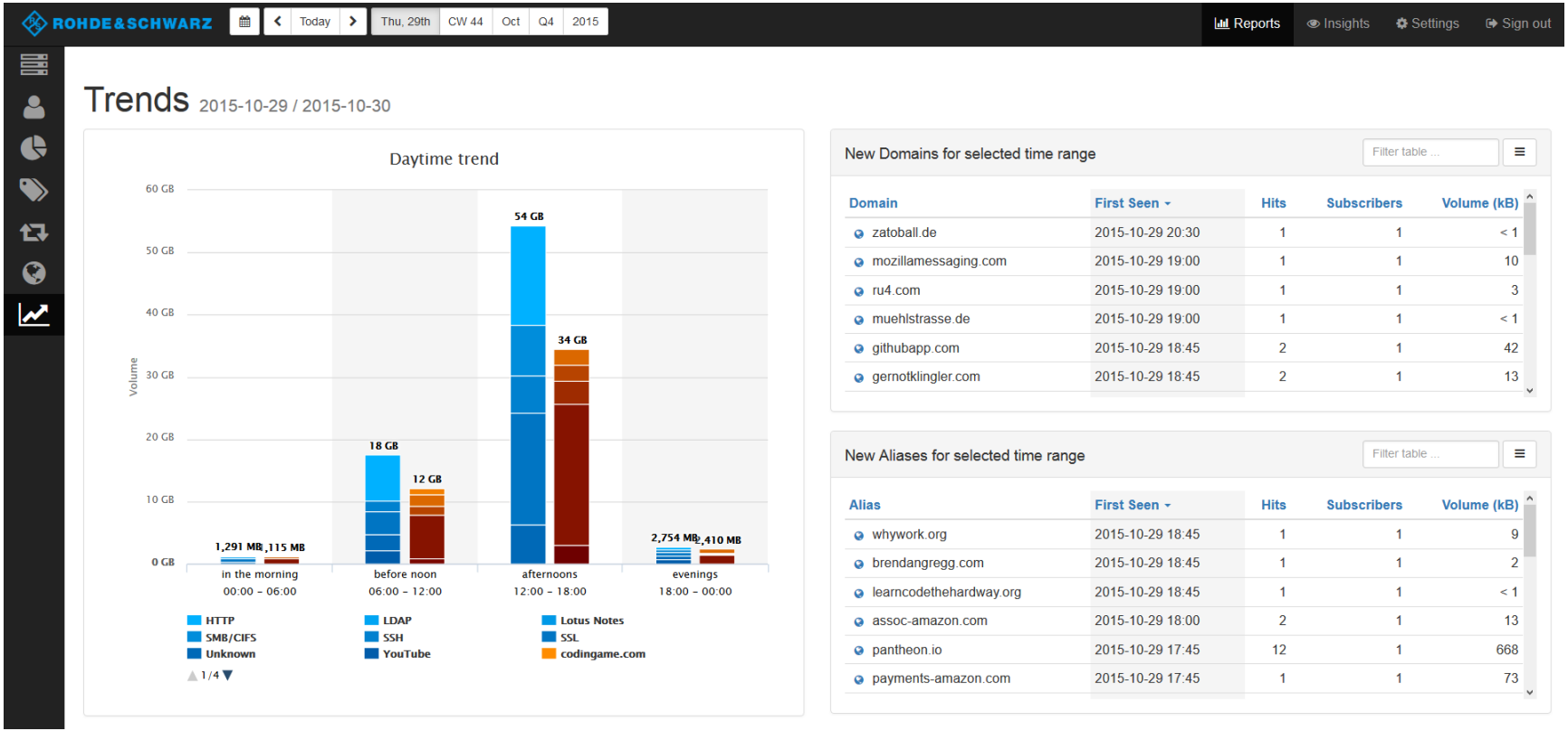
Net Reporter UI



Net Reporter UI

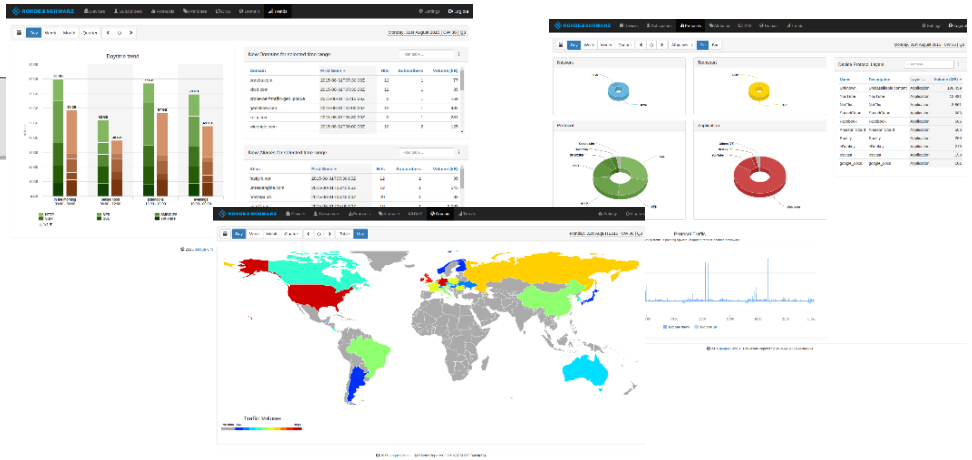


Net Reporter UI



R&S Industrie 4.0 and IoT concept – be aware

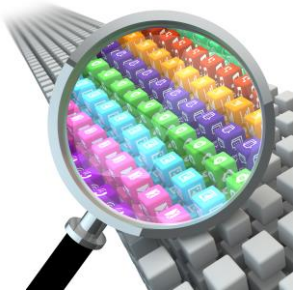
- Rohde & Schwarz Net Sensor / Net Reporter
  - Detect and alert anomalies in the IP traffice
  - Detect protocols with parameter settings (e.g. avoid a reset in a power plant)
  - Analyzing platform for a lot of applications
  - Inteligence and extenable IP Probe *Net Sensor* by using the R&S DPI Engine *PACE*



R&S Industrie 4.0 and IoT concept – make secure

- R&S Gateprotect Firewall includigng Rohde & Schwarz PACE Software
  1. Active protection with protocol validation – only approved protocols and parameter will pass
  2. First deployments of IEC 104 at the German powert stations (Stadtwerken)

- Rohde & Schwarz PACE
  1. Own DPI (Deep Packet Inspection) Engine, fast changes of protocols possible



Thank you!