Argus Project http://qosient.com/argus

- Argus is a network activity audit system
- The first real-time network flow monitor
  - First developed at Georgia Tech (Enslow, 1983)
  - Applied to cyber security at CMU/SEI CERT (1989)
  - Engineered for HPC at the Naval Research Lab (Dardy, 2000)
- Network activity/usage data models and analytics
  - Generates detailed data network metadata (CDR equivalent)
  - Source of near real-time and historical network awareness info
  - Supports the complete incident response life cycle
- Designed to support network situtation awareness
  - Operations - Service availability and operational status
  - Performance - End-to-end assessment of network traffic
  - Security - Audit / Non-Repudiation / Anomaly Detection
- Top 100 security tool used in the Internet today

QoSient

Argus Users

- Cyber Security Awareness
  - Defense Information Systems Agency
    - Standard for network forensics data generation Joint Regional Security Stack JRSS
  - Department of Homeland Security
    - Cyber Mitigation and Course of Action (COA) Development
  - National Security Agency
    - CYBERPILOT
- Network Situational Awareness
  - GLORIAD – INSIGHT (Cole)
  - NASA Ames HPC (Boscia, Shaw)
    - E2E QoS Analysis and Performance Assurance
- Network Research – Open Source
  - National Science Foundation AMI (Cole, Gregor)
  - Stanford Univ (McKeown, Gerth, van Reijendam)
    - SDN Dev Ops and Cyber Security Awareness

QoSient

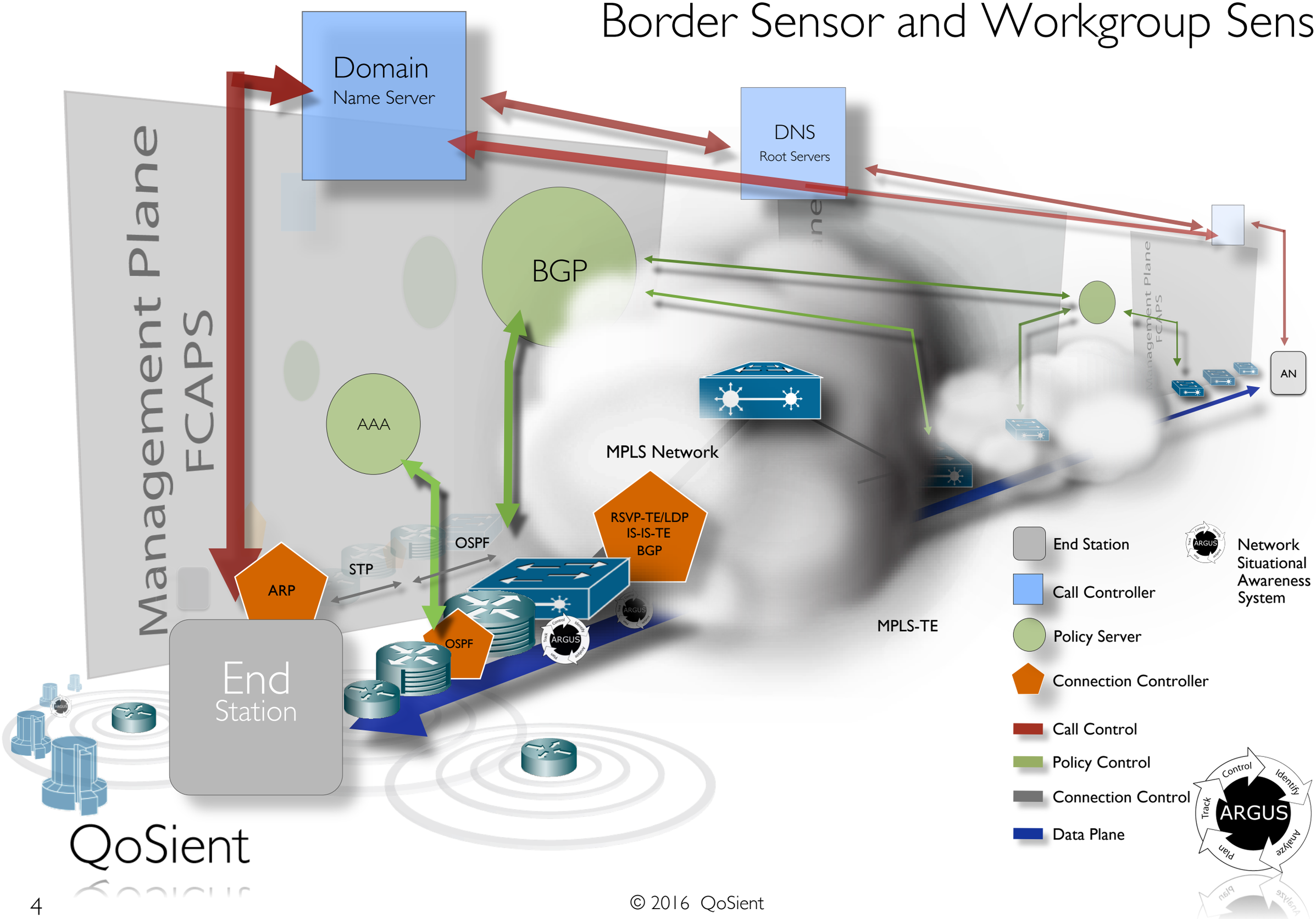
Argus Approach

- Advanced Sensors for Network MetaData Origination
  - Comprehensive accountability for all network activity
  - Ubiquitously deployable to enable a uniform sensing fabric
  - Mature data models to track all network strategies
    - Bi-directional flow tracking for tunneled, unicast, multicast, broadcast, connection-oriented and connection-less network transactions.
    - Control, Management and User plane traffic awareness
      - Ethernet, Infiniband, ATM, PPP, ARP, DHCP, VLANs, LDP, LLC, MPLS, RSVP, OSI IS-IS, SDN encapsulations, IPv4, IPv6, ESP, RTP, RDP, and general support for any/every other protocol.
  - Reporting conventional and novel network attributes
    - Multi-layer flow specs, content, flow disposition, behavioral metrics (PCR, Laterality), Packet Dynamics (keystroke reporting, burst behavior, queuing, load balancing)
  - Real-time sensing and reporting to enable active response
  - Designed for a large number of awareness applications

QoSient

Traditional Visibility Deployment Strategies

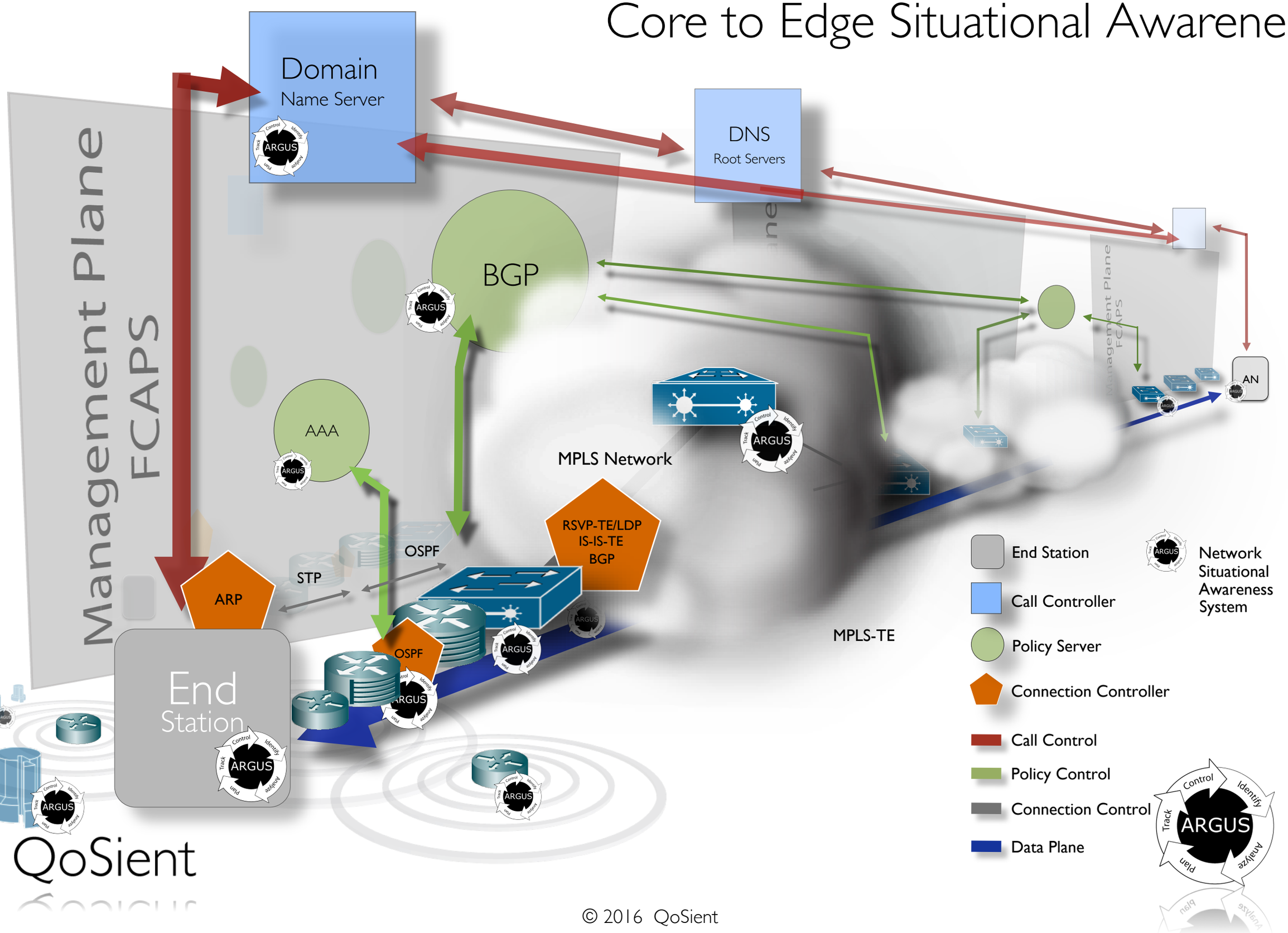
Border Sensor and Workgroup Sensor



QoSient

Comprehensive Deployment Strategies

Core to Edge Situational Awareness

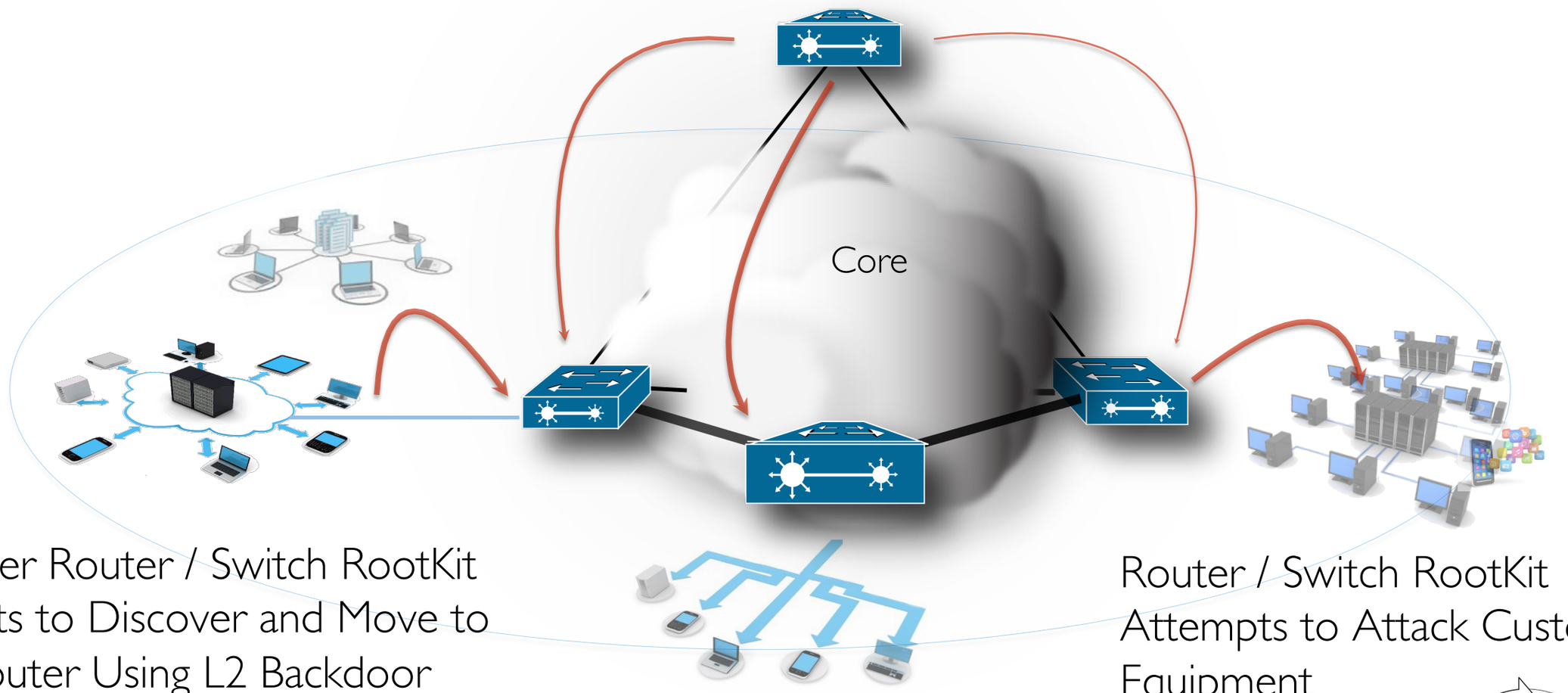


QoSient

Core Control Situational Awareness

ISP Rootkit Lateral Movement Scenario

Core RootKit Activates and Laterally Moves Within the Core
Using L2 Proprietary Covert Channels or Existing Embedded Agents



Customer Router / Switch RootKit
Attempts to Discover and Move to
Edge Router Using L2 Backdoor
Protocols

Router / Switch RootKit
Attempts to Attack Customer
Equipment

QoSient

Stanford / NASA 100Gbps Argus

- 100G SDN Control Demonstration for SC'16
  - Near real-time traffic identification and management with wire-line verification for traffic engineering
  - Demo moving big elephants between 10G and 100G services using Openflow and Argus
  - Combines sensing, sense-making, decision making and action to provide near-time active networking
- Dell, Mellanox, Napatech and QoSient technology
- Cooperative between Stanford, CENIC and NASA
  - Testing sensing and sense-making components today
  - Opportunity to test advanced packet dynamics monitoring at 100G over CENIC.

QoSient