Security Coordination with IF-MAP

Matt Webster, Lumeta

28 Sept 2010

Agenda

- Threat Landscape and Federal Networks
- Recap of TNC
- Explanation of IF-MAP
  - What is IF-MAP?
  - What problems does IF-MAP address?
  - How does IF-MAP solve those problems?
  - Use cases
- IF-MAP Adoption
- Summary
- For More Information

Cyber Threat Sources & Trends

- National Governments
- Terrorists
- Industrial Spies
- Organized Crime Groups
- Hacktivists
- Hackers
- Malware
- Botnets
- Cyber warfare
- Threats to VoIP and mobile devices
- The evolving cyber crime economy

Sources: US-CERT http://www.us-cert.gov/control_systems/csthreats.html; GTISC Emerging Cyber ThreatsReport for 2009 http://www.gtisc.gatech.edu/pdf/CyberThreatsRepoand rt2009.pdf

Automation & Continuous Monitoring

- Automate continuous monitoring
- Automate Access Control using SCAP
- Regularly assess effectiveness of security controls
- Adversaries exploit the weakest controls
- True security is dependent on all controls remaining effective over time

Source: NIST FAQ on Continuous Monitoring, June 1, 2010

Security Content Automation Protocol (SCAP)

Languages

Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

Metrics

Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

Enumerations

Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings

What is Trusted Network Connect?

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing

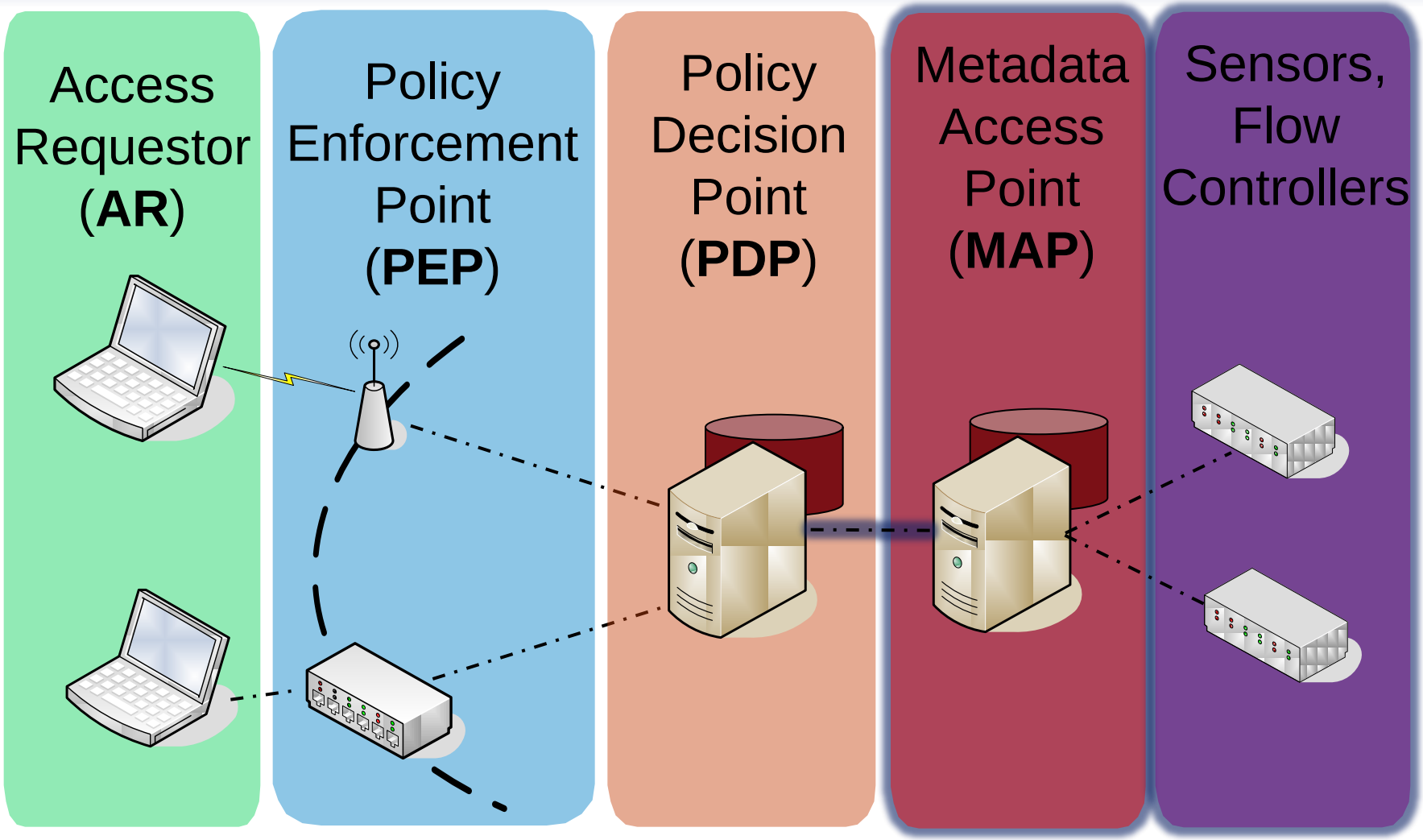
Open Standards for Network Security

- Full set of specifications available to all
- Products shipping for more than four years

Developed by Trusted Computing Group (TCG)

- Industry standards group
- More than 100 member organizations
- Includes large vendors, small vendors, customers, etc.

Where Does IF-MAP Sit Within TNC



What is IF-MAP?

Open Standard for Security and Network Coordination

- First published in May 2008 by the Trusted Computing Group
  - Industry consortium including most large IT vendors
- Freely available for anyone to implement
- Growing base of vendor and product support

Shared database for information on network devices, their state, and their activities

- "MySpace" for IP devices and systems

Aggregates real-time information from many different sources

- Both standard data types and vendor-specific extensions

Designed to scale for machine-to-machine coordination

Enterprise Connectivity

Problems Addressed by IF-MAP

Network and Endpoint Visibility

- Situational Awareness - Who and what's on my network?
- Are devices on my network secure? Is user/device behavior appropriate?

Network Enforcement

- Provide information on unauthorized users/devices
- Provide information on network events

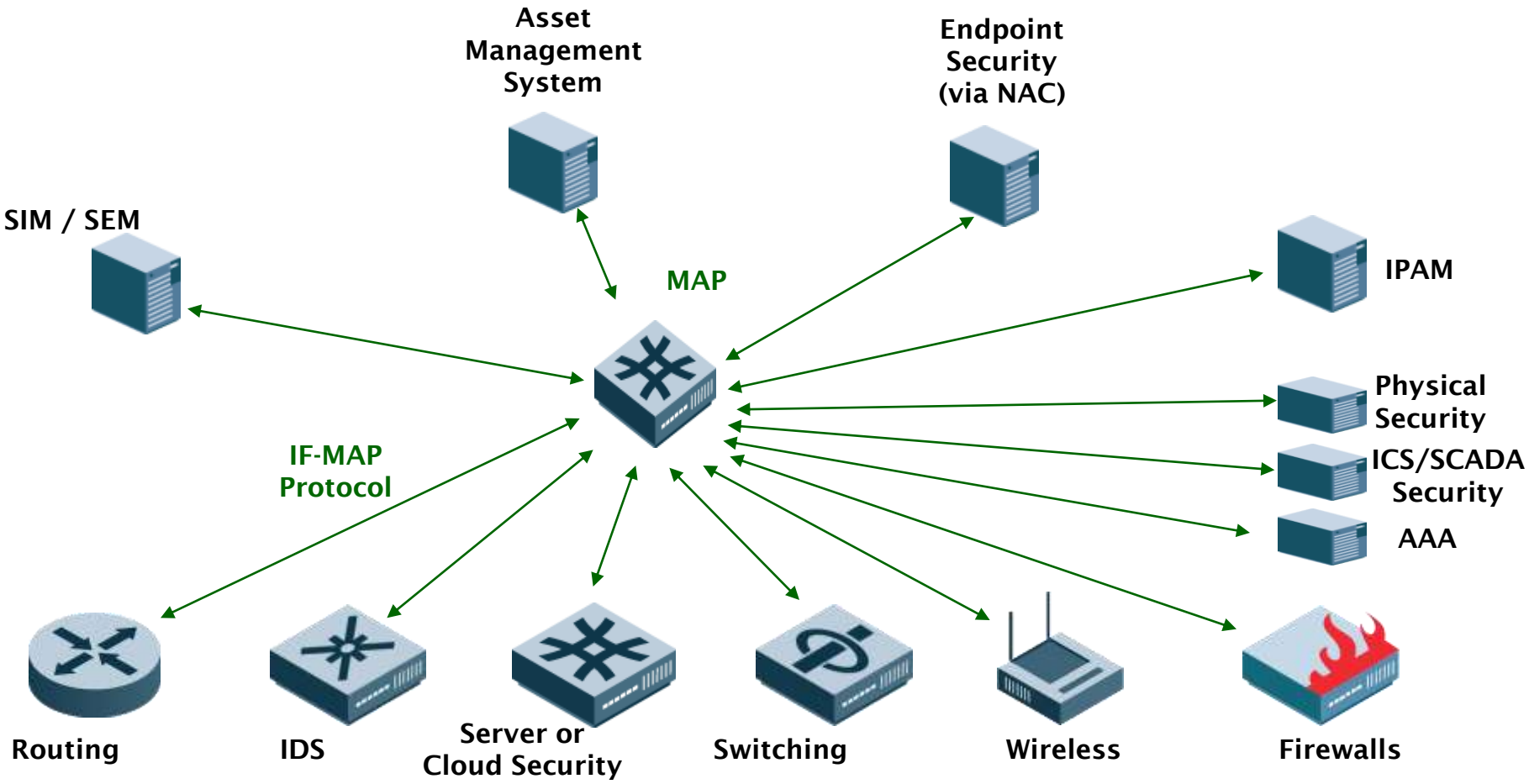
Security Automation

- Test access levels for users/devices
- Automate audit of security controls across a full suite of tools
- Validate remediation efforts

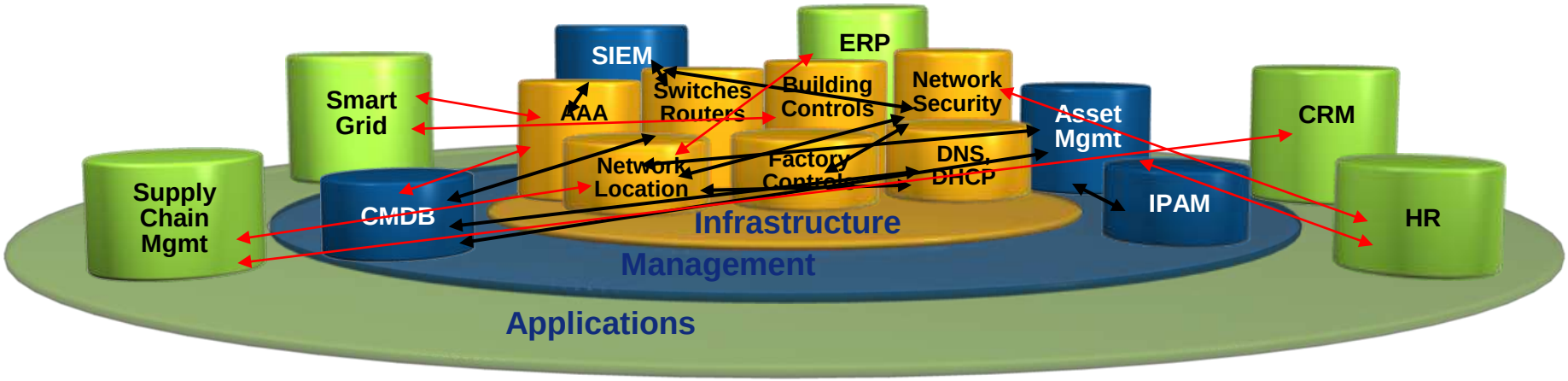
Systems Interoperability & Data Integration

- Automate security decision-making, with best available information
- Share real-time information about network events, users, devices, threats, etc.

Coordinated Security with IF-MAP



The Integration Challenge

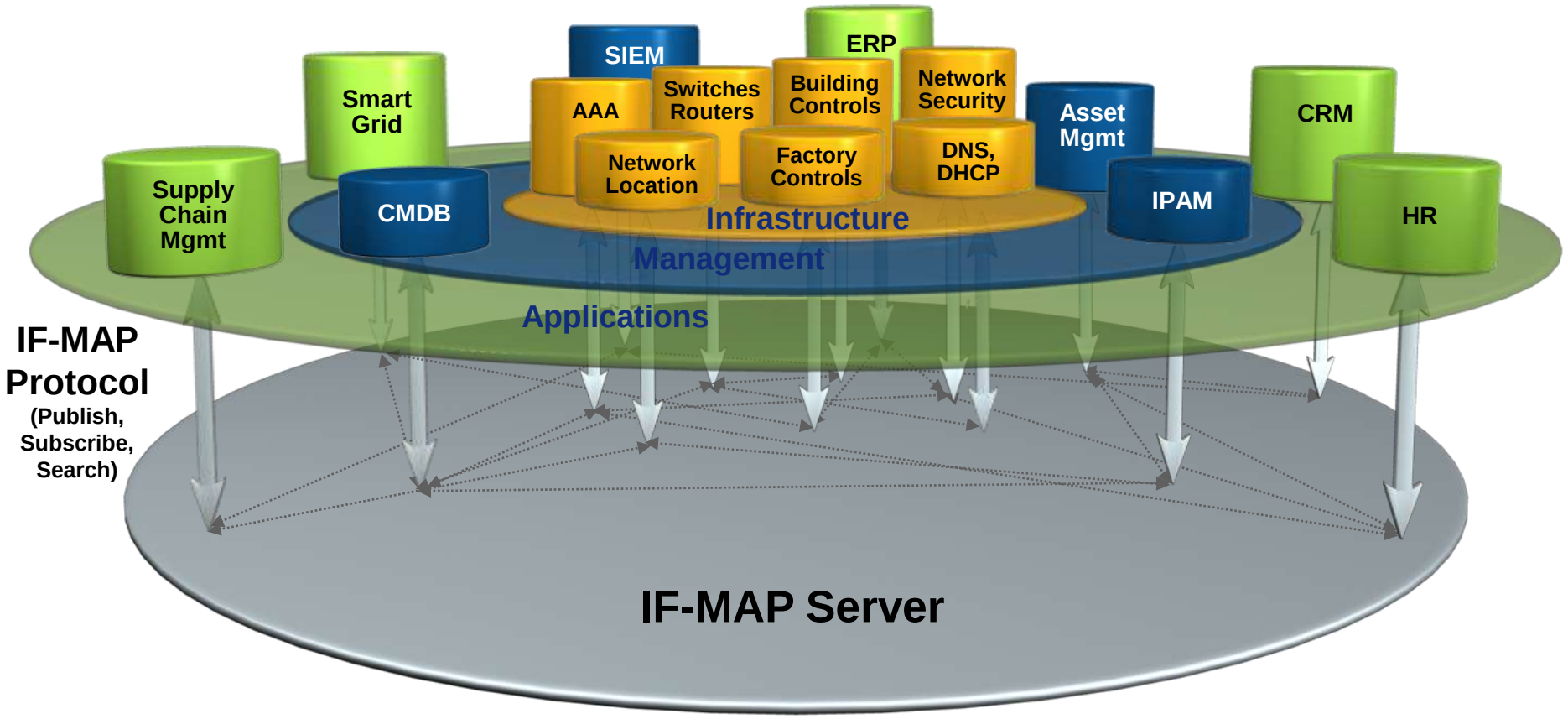


SNMP, Syslog, Netflow

Custom Integration – API's, Scripts

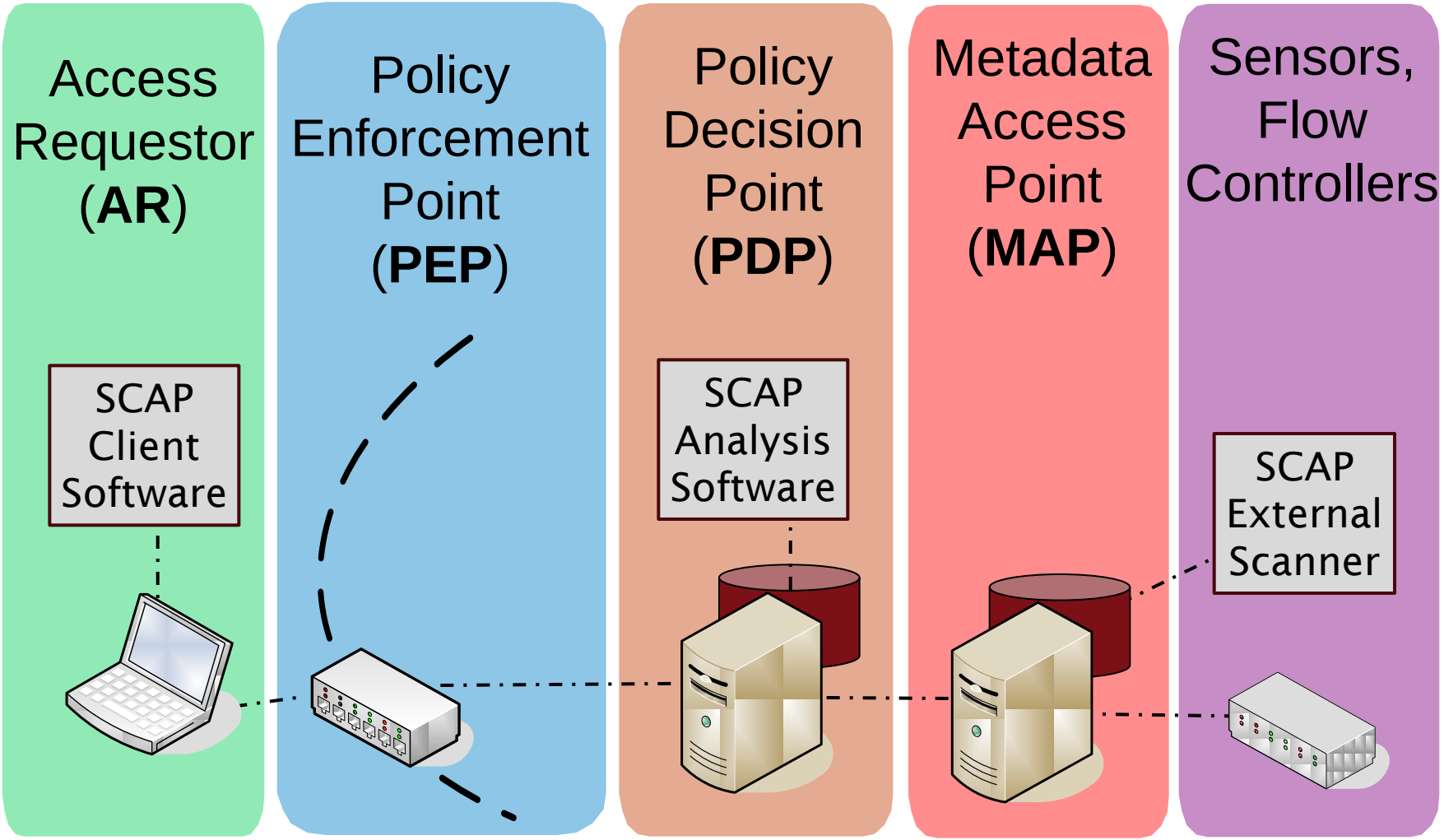
- Complex
- Costly
- Brittle
- High Maintenance

From Integration to Orchestration with IF-MAP



Automatically aggregates, correlates, and distributes data to and from different systems, in real time

TNC/IF-MAP and SCAP Together

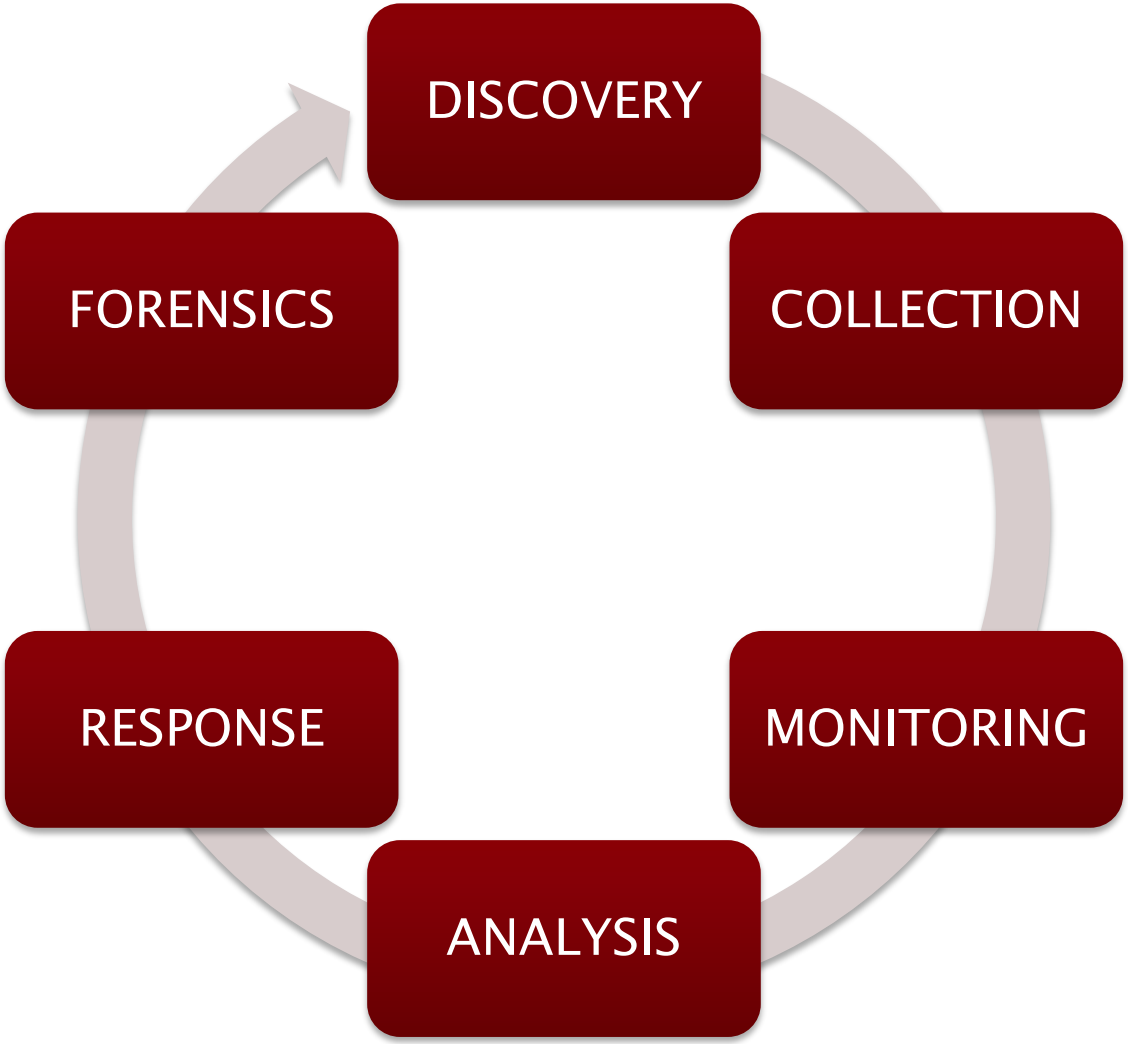


IF-MAP Standardization & Adoption

Agencies & Vendors benefit from Security Automation in multi-vendor environments

- Agencies leverage existing IT investments with interoperability; improve information sharing with standardized data
- Procurement & Gov't IT Leadership drive standards adoption among vendors
- Product integration costs & time greatly reduces through standards-based interoperability

From Baseline to Coordinated Security



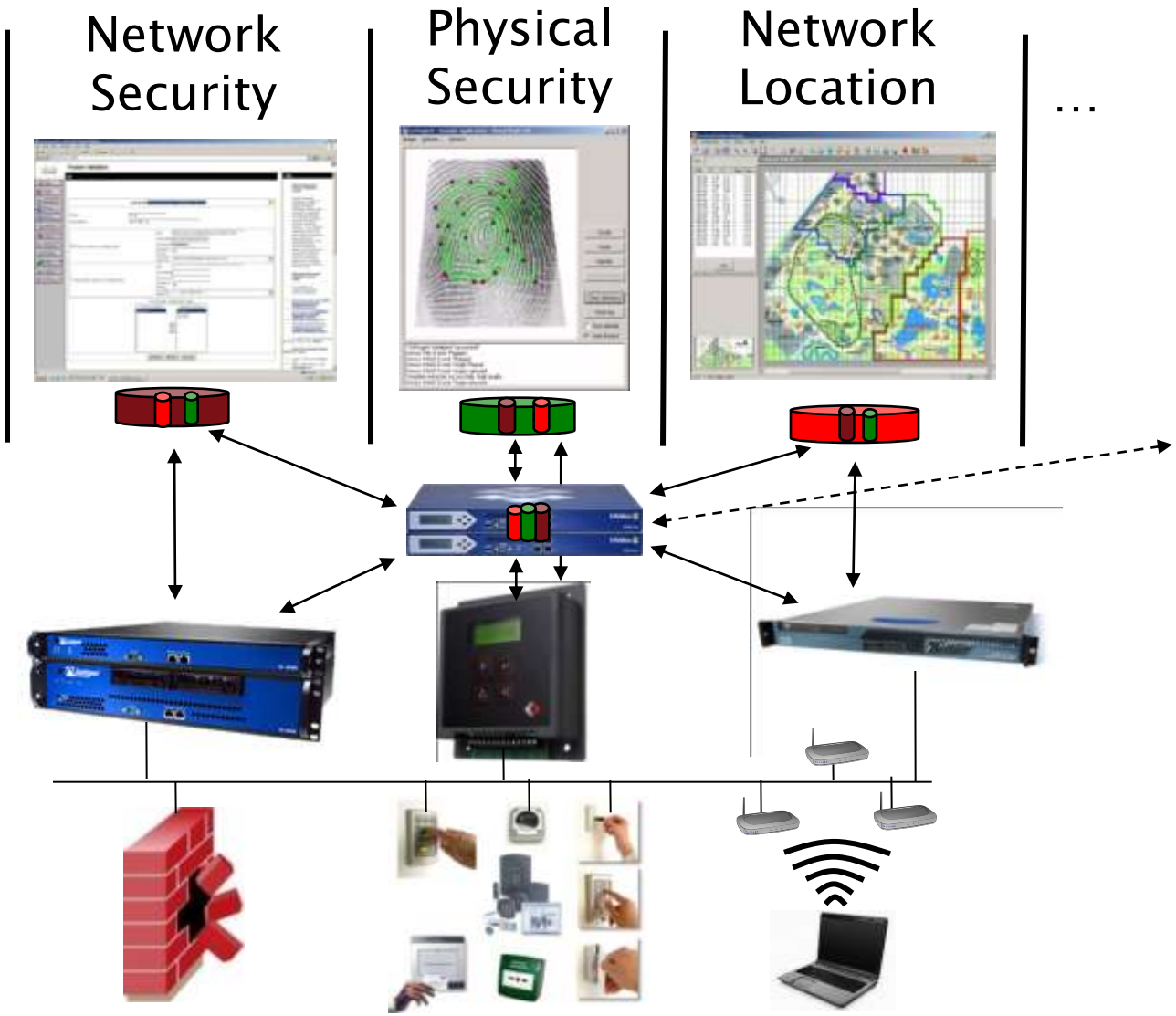
IF-MAP Lets Existing Systems to Share Data

Provisioning, Visualization & Analytics (Management)

IF-MAP Server

Decisions (Control)

Sensors & Actuators



Many New Applications are Emerging

– Just the Tip of the Iceberg…

Cyber/Physical (CyPhy) Convergence	IT Automation	Cloud Computing
•Don't allow users to connect to the network if they haven't badged into the building	•Track the location and status of all IT assets (IPs, MACs, devices, hardware, VMs, apps, users, etc.) in real time	•Federate authentication and authorization status across private & public clouds
•Don't allow a wireless device to connect if its located outside of the building	•Allocate assets on the fly, dynamically re-provision data centers	•Move computing workloads to the cloud when prices drop

Use Case – Quarantine a Leaking Device

Challenges:

- Manage network change
- Fight insider threats
- Ensure security policy compliance
- Enforce network segmentation

Consequences:

- Policy violations
- Unauthorized, unsecure network connections
- Worms, viruses, hackers, insider threat
- Inhibited situational awareness

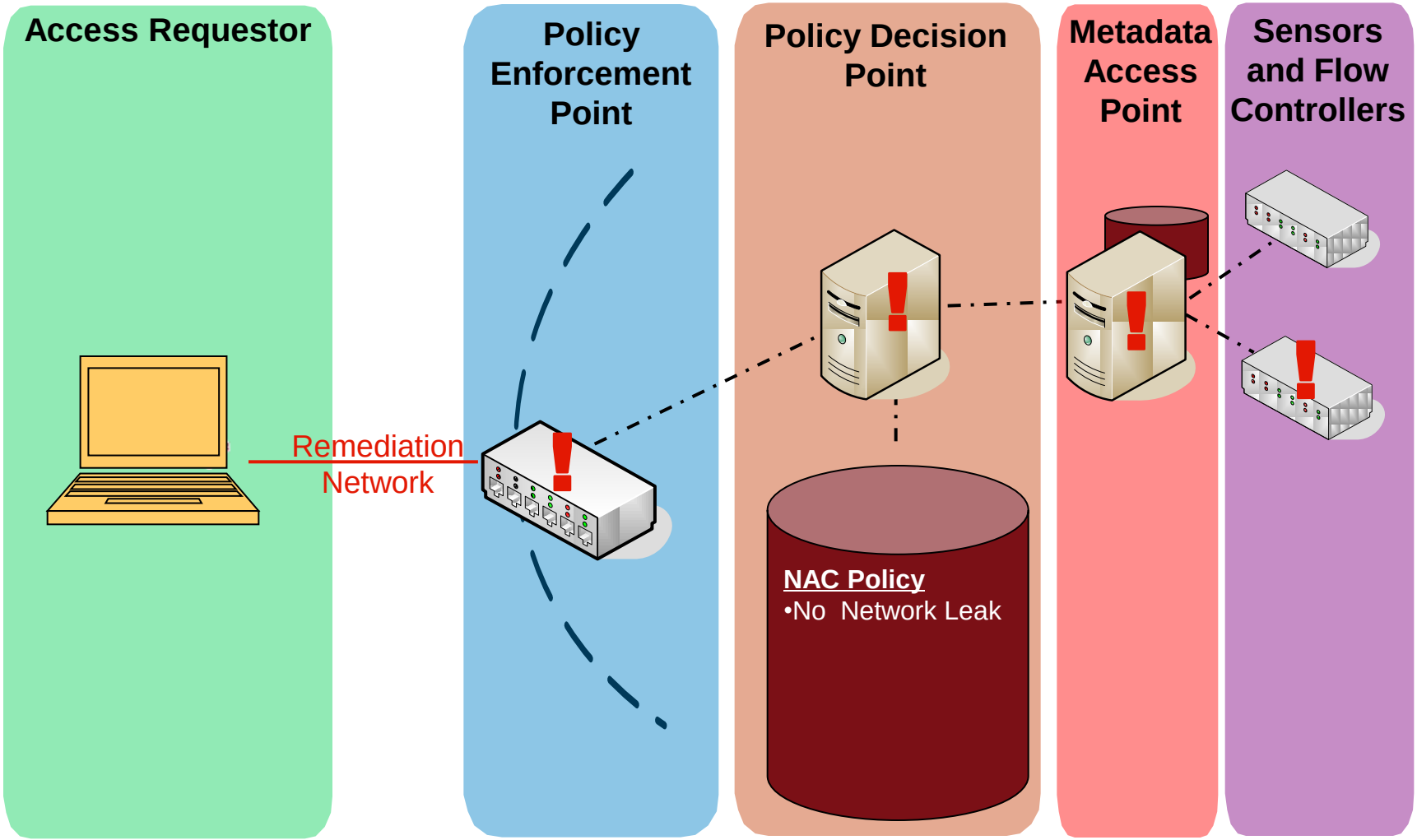
Solution:

- Lumeta IPsonar's Network Leak Discovery
  - Enable organizations to detect unknown, unauthorized and unsecure network connections
- Juniper Networks Unified Access Control
  - Automatically and securely remediate the situation
- Integrated network defense via TNC

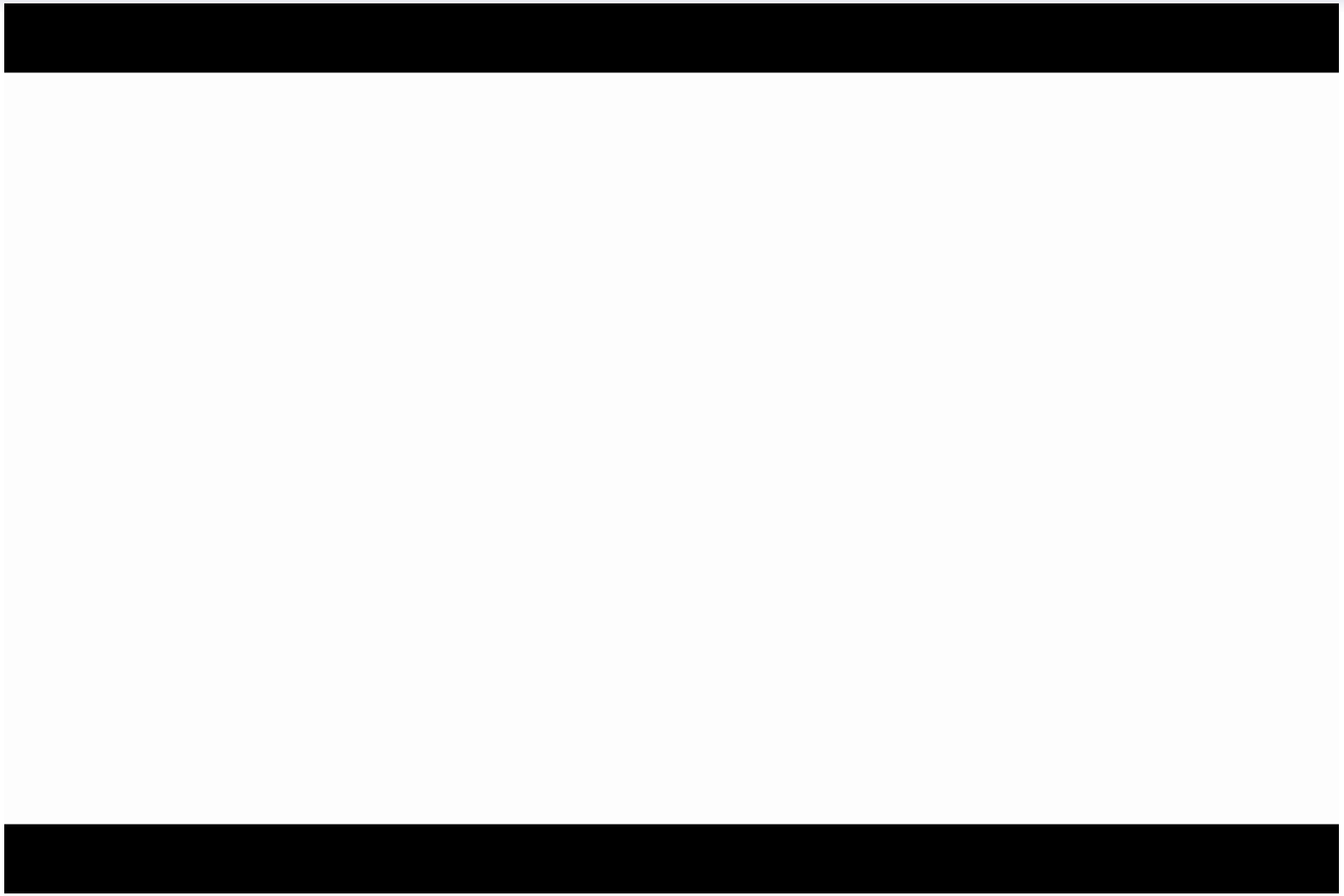
Lumeta's IF-MAP Client

- Lumeta is currently contributing member of TNC
  - Co-chair TNC adoption sub-group (Matt Webster)
- Beta IF-MAP client fall 2008
  - No significant development time or costs
- IPsonar version 4.5 contains IF-MAP client
  - GA in August of 2009
- Enables delivery of IPsonar Discovery events for automated remediation
- Significant interest with Government Clients
- Integrated network defense solution with Juniper

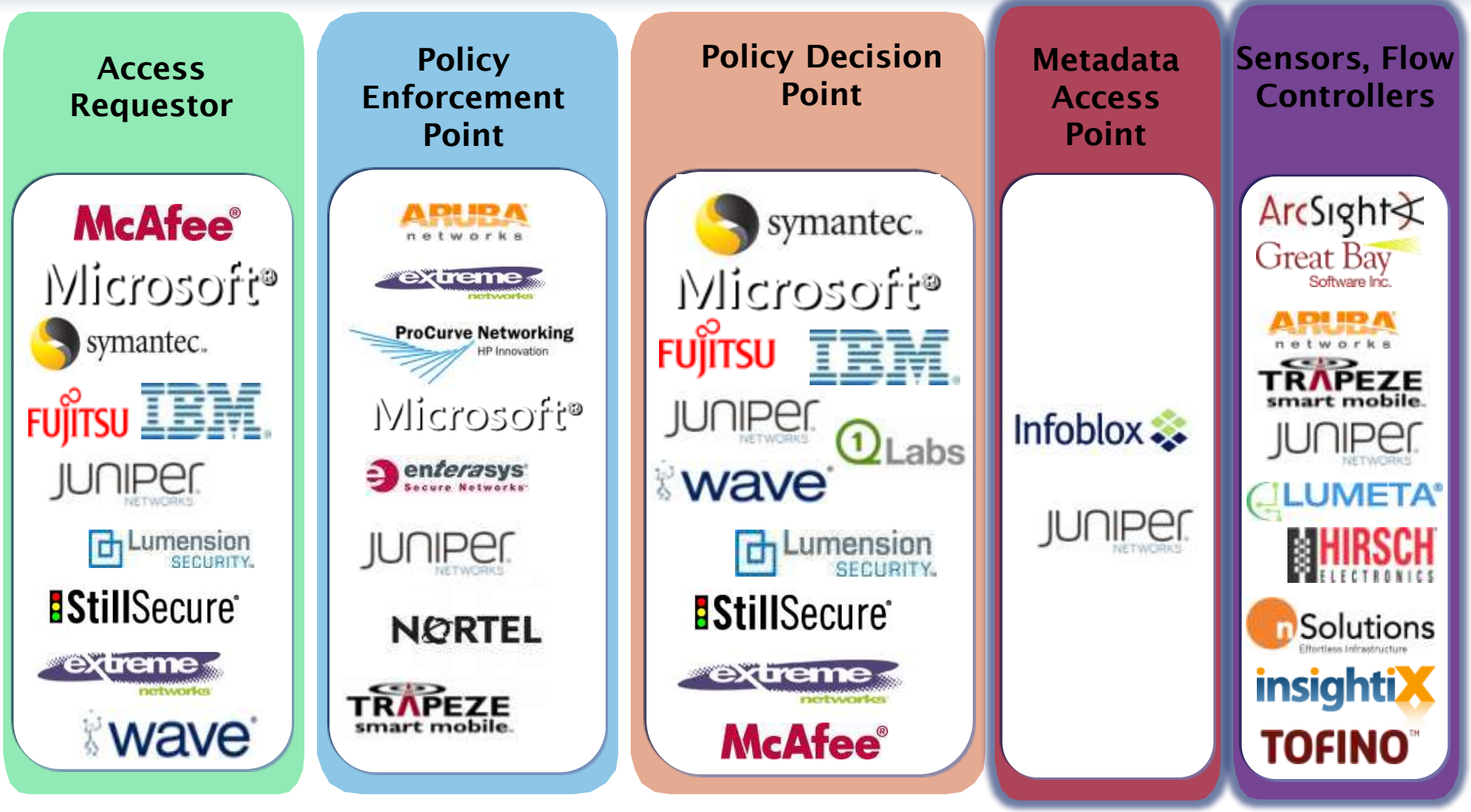
Policy Violation – Leaking Device



Use Case – Physical Security



IF-MAP Adoption



What About Open Source?

- Lots of open source support for TNC
  - University of Applied Arts and Sciences in Hannover, Germany (FHH)

    http://trust.inform.fh-hannover.de
    - tnc@fhh - the open source TNC implementation.
    - ISC DHCP - the open source DHCP implementation.
    - Nagios - the industry standard in IT infrastructure monitoring.
    - Snort - the open source network intrusion prevention and detection system.
    - netfilter/iptables - the packet filtering framework inside the Linux 2.4.x and 2.6.x kernel series.
  - omapd IF-MAP Server

    http://code.google.com/p/omapd
  - IF-MAP Client Code

    http://ifmapdev.com/

IT Situational Awareness via IF-MAP

- What's on the network?
- Are there patterns that I'm not seeing?
- Collect & correlate information on all users, events & devices
- Prioritize risk, take appropriate action
- Validate the success of remediation
- Repeatable, automated assessments of the IT environment
- Automated and Continuous

Upcoming TNC-Related Sessions

- TNC: Open Standards for Network Security Automation
  - There was just a presentation earlier today
  - If you missed that presentation, please check out the slide deck!

- Leveraging SCAP for TNC, Endpoint Sensor Grid and Automated Remediation
  - In-depth look at TNC-SCAP integration
  - See a demo of TNC-SCAP Integration!
  - After the IF-MAP session in Ballroom I (Tuesday, 4:45-5:30 PM)

For More Information

- **TNC Web Site**

  Technical

  http://www.trustedcomputinggroup.org/developers/trusted_network_connect

  Business

  http://www.trustedcomputinggroup.org/solutions/network_security

- **TNC-WG Co-Chairs**

  Steve Hanna

  Distinguished Engineer, Juniper Networks

  shanna@juniper.net

  Paul Sangster

  Chief Security Standards Officer, Symantec

  Paul_Sangster@symantec.com

Thank you!