InformationWeek
WEBCAST

Automate to Win: The Business Case for Standards-based Security

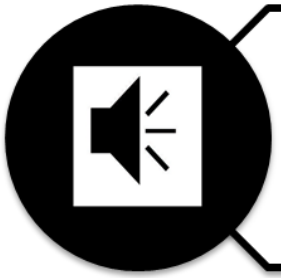
An InformationWeek Webcast

Sponsored by



UBM
TechWeb

Webcast Logistics



No Sound?

This is a streaming audio event. Make sure the sound on your PC is turned on.



Questions?

Type your questions using the Ask a Question Text Box



Technical problems?

Click the “Help” link below the media player.

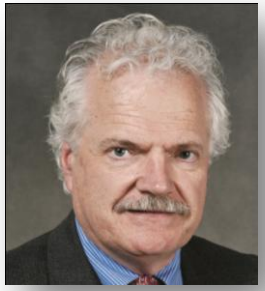
Today's Presenters



Paul Korzeniowski,
Contributing Editor
InformationWeek



Steve Hanna,
Co-chair , Trusted Network Connect Work Group
Trusted Computing Group
Distinguished Engineer
Juniper Networks



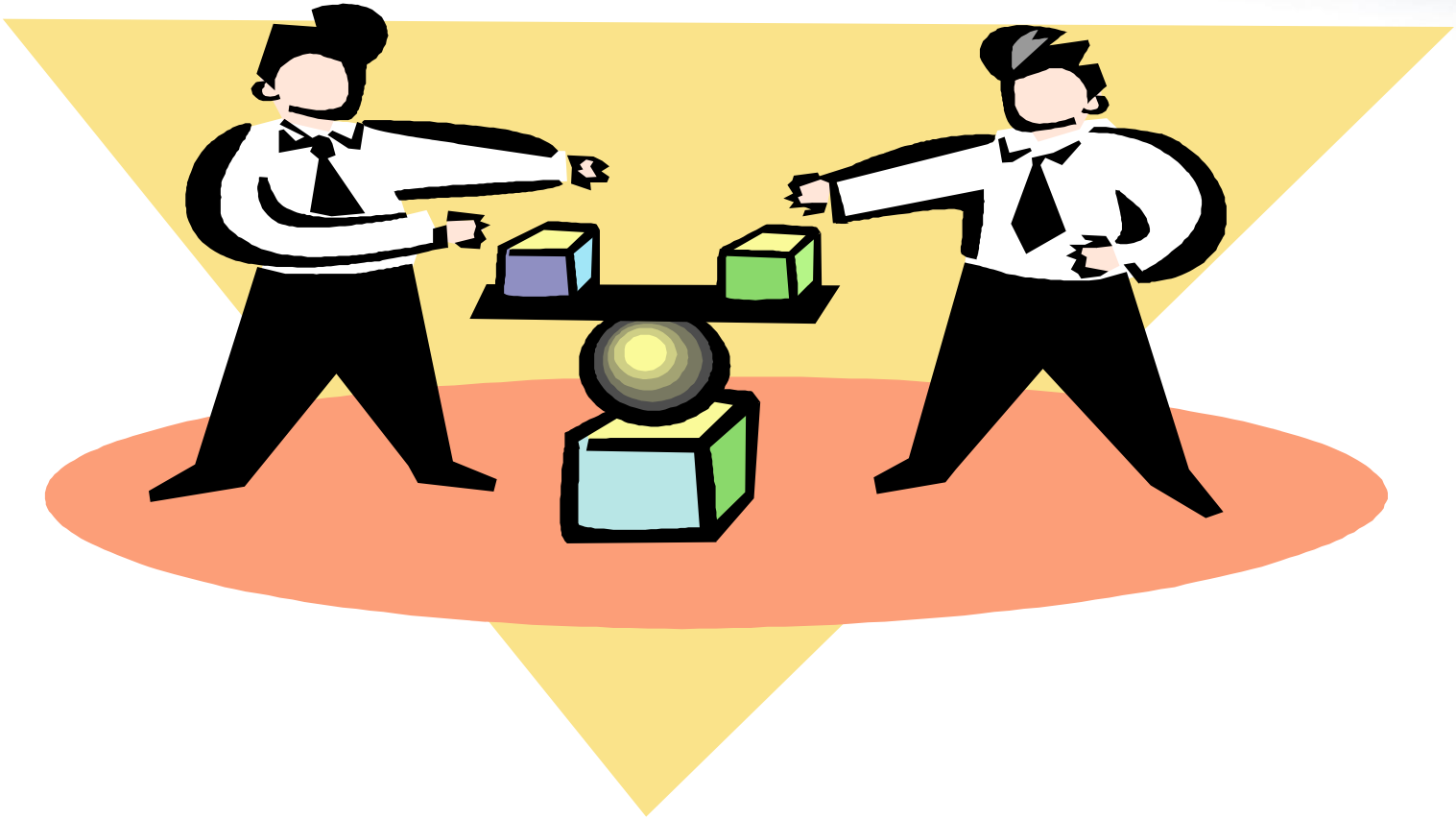
Craig Dupler
Technical Fellow
The Boeing Company

Poll Question 1

1. **How important is it for you to have the ability to implement security solutions using standards-based products from multiple vendors? (choose one)**

   – Extremely important
   – Somewhat important
   – Not important

Security: A Delicate Balancing Act



Paul Korzeniowski
InformationWeek

The Changing Workplace

- Companies becoming more mobile
  - Work at home
  - Work on the road
- More connections to customers
  - Guest access expected
  - Social Networking
- More end user devices
  - Laptops
  - Smartphones
  - Tablets



More Flexibility, Less Security

- Data is more dispersed, more chances for intrusion emerge
- 345,124,400 records have been breached since 2005
- Organized Crime's role
- Cost is high: $6.65 million per affected corporation ($202 per record)



More Visibility and Control Needed

- Who is entering your network?
- What data are they accessing?
- What is happening at the end point?



Current Security Constraints

- Increased complexity
- Lower budgets
- Balance security risks versus security investments



Network Security Needs

- Inexpensive
- Comprehensive
- Easy to deploy
- Works with a broad range of devices



Poll Question 2

2. How much do you know about the TNC architecture and standards? (choose one)

- I consider myself an expert
- I've read a few papers
- I've seen TNC demos at trade show or event
- I'm just getting started
- This is the first I've heard of TNC



Trusted Network Connect
Standards for Network Security

Copyright © 2011 Trusted Computing Group

Trusted Network Connect

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing
- Original focus on NAC, now expanded to Network Security

Open Standards for Network Security

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

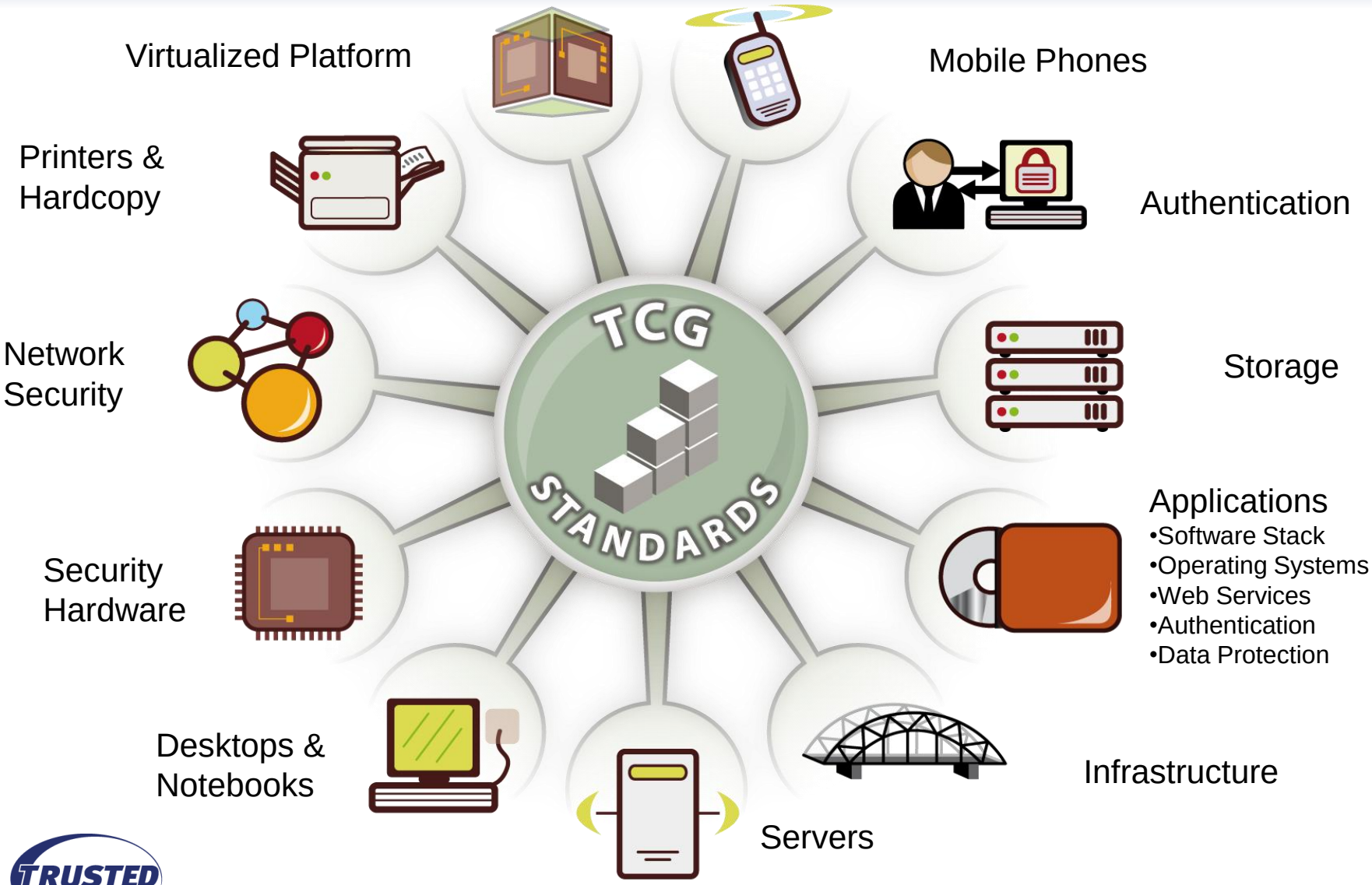
Developed by Trusted Computing Group (TCG)

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

TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group

TCG: Standards for Trusted Systems



Copyright© 2011 Trusted Computing Group

Problems Solved by TNC

Network and Endpoint Visibility

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

Network Access Control (NAC)

Network Enforcement

- Block unauthorized users, devices, or behavior
- Grant appropriate levels of access to authorized users/devices

Device Remediation

- Quarantine and repair unhealthy or vulnerable devices

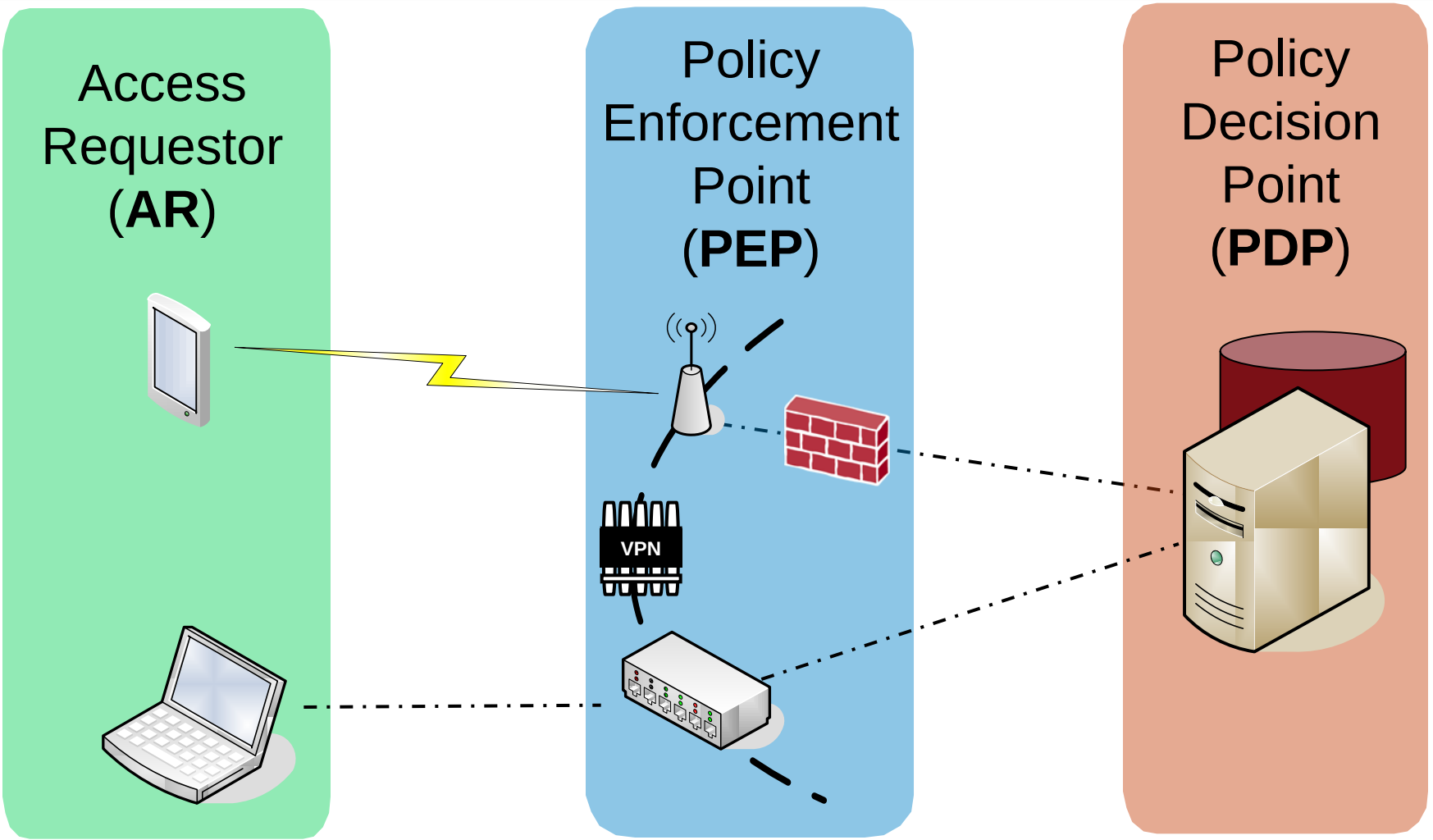
Security System Integration

- Share real-time information about users, devices, threats, etc.

Coordinated Security

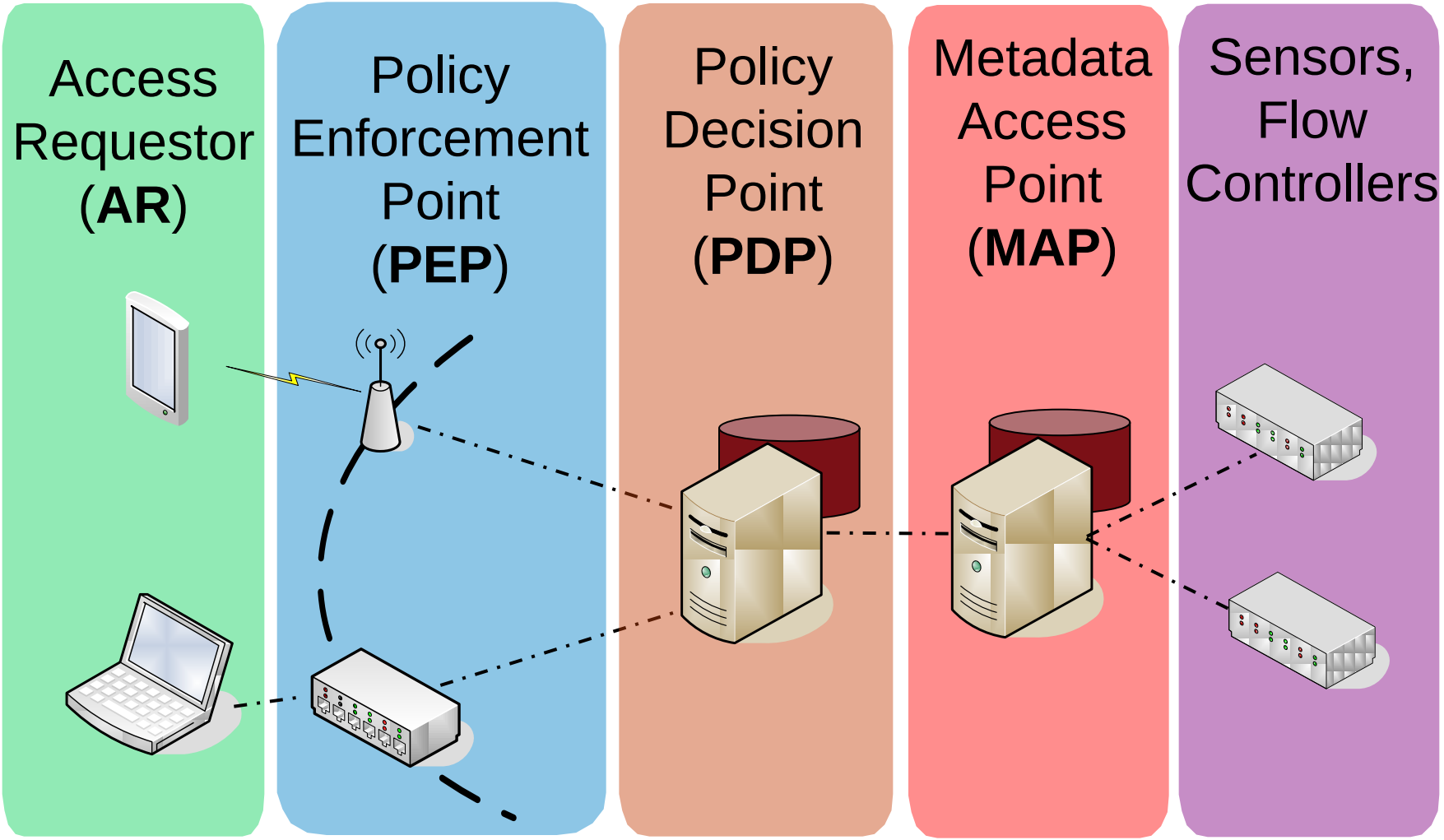
Copyright© 2011 Trusted Computing Group

Basic NAC Architecture



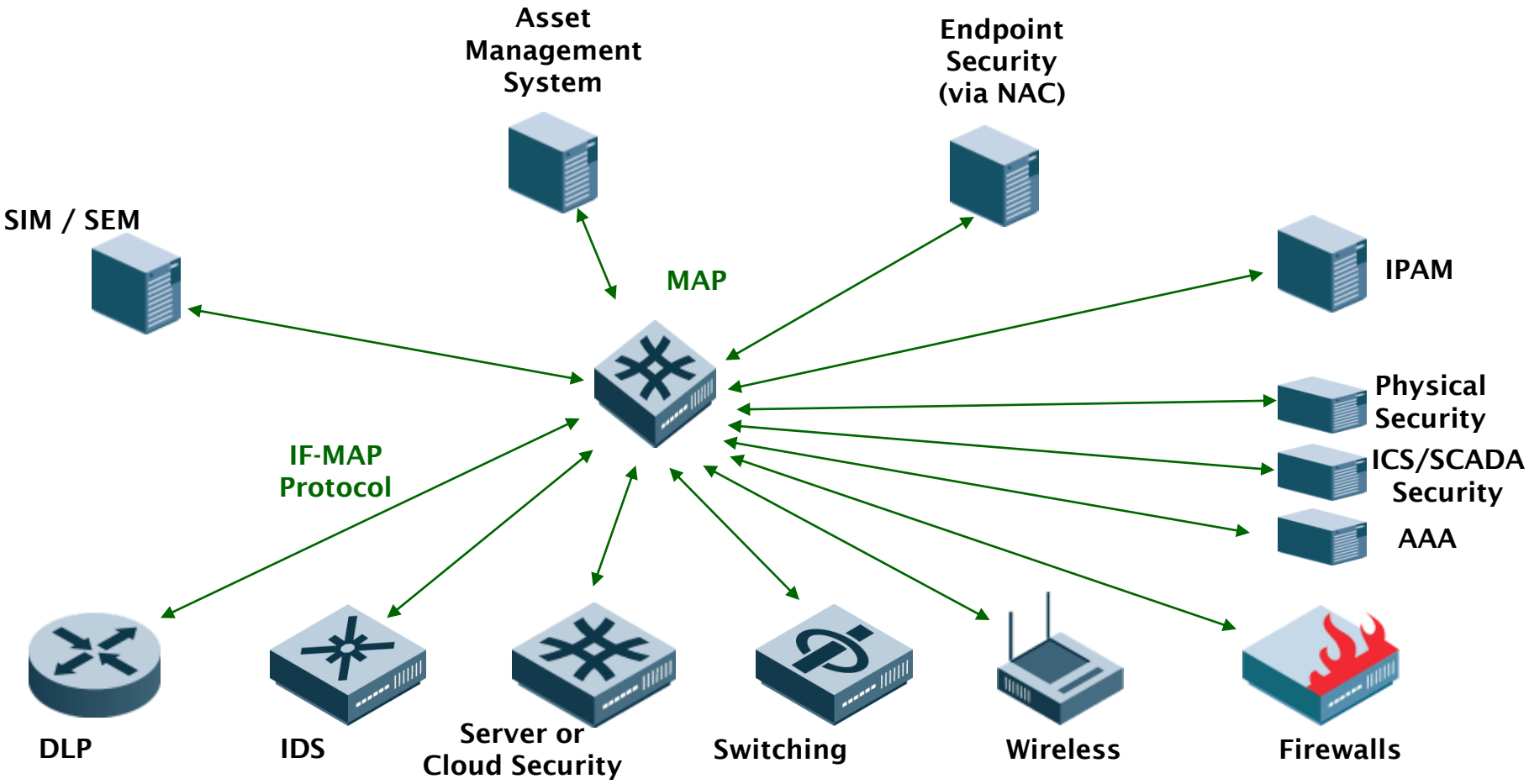
Copyright© 2011 Trusted Computing Group

Integrating Other Security Devices



Copyright© 2011 Trusted Computing Group

Coordinated Security



Copyright© 2011 Trusted Computing Group

Typical Uses for IF-MAP

Multi-Vendor Network Security

- Share Information (Identity, Role, etc.) Among Security Systems
- Automated Incident Response

Asset Management

- Immediately Detect and Analyze New Devices When They Connect

Compliance Management

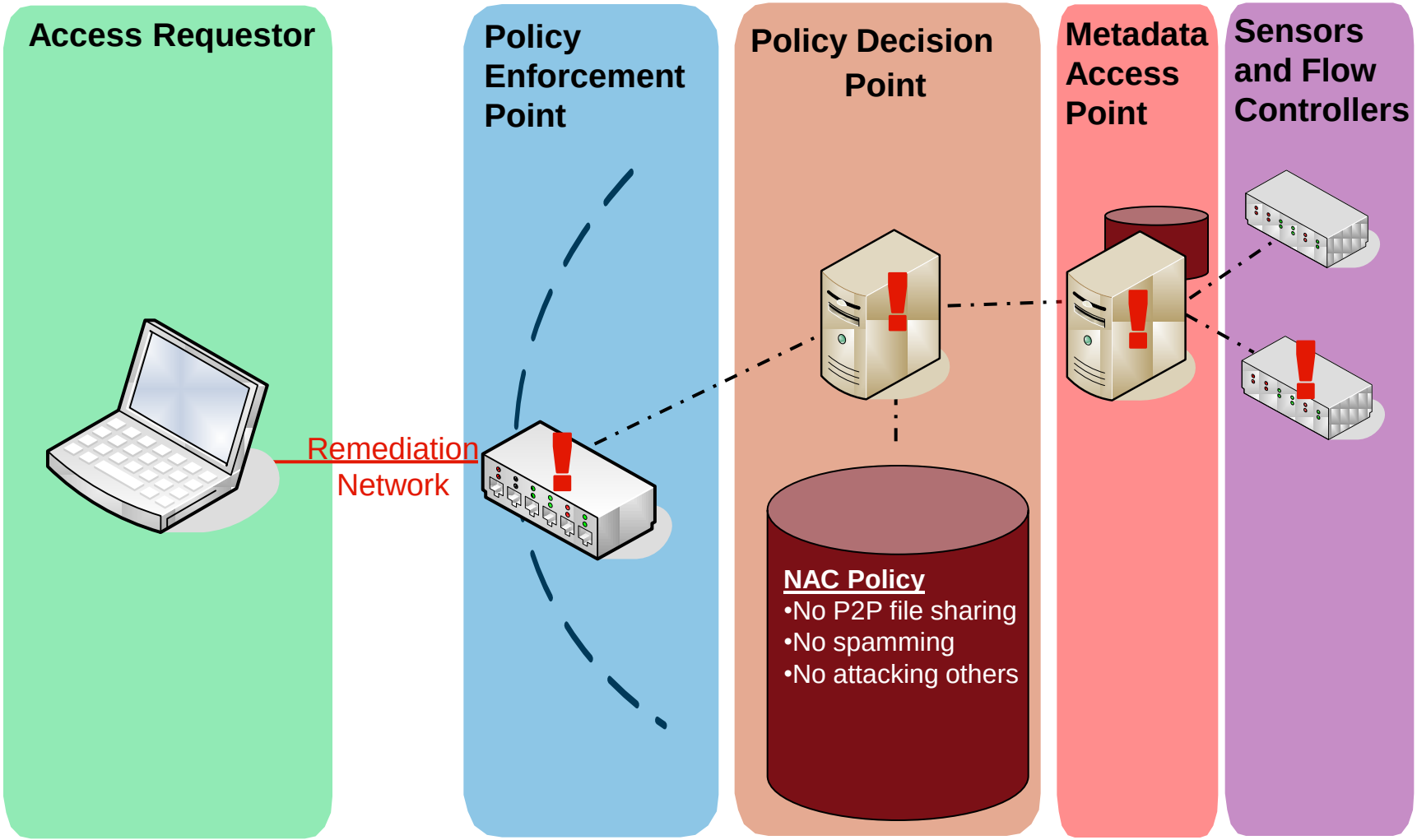
- Immediately Scan New Devices When They Connect

Cloud Security

- Share Security Information From Cloud Provider to Customer

Copyright© 2011 Trusted Computing Group

Automation Example



Copyright© 2011 Trusted Computing Group

TNC Advantages

Open standards

- Non-proprietary – Supports multi-vendor compatibility
- Interoperability
- Enables customer choice
- Allows thorough and open technical review

Leverages existing network infrastructure

- Excellent Return-on-Investment (ROI)

Roadmap for the future

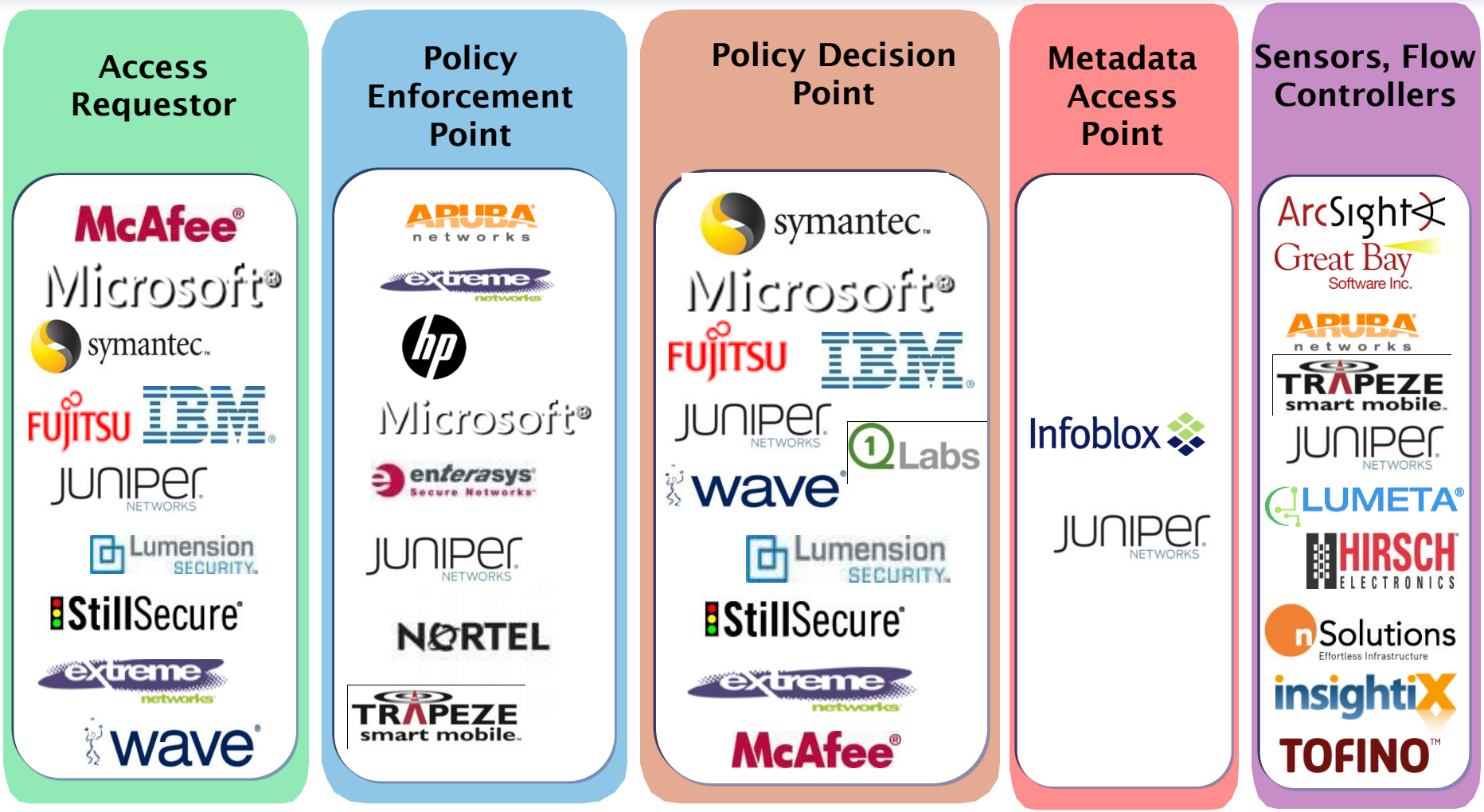
- Full suite of standards
- Supports Trusted Platform Module (TPM)

Products supporting TNC standards shipping today

TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group

TNC Adoption



Copyright© 2011 Trusted Computing Group

Summary

TNC solves today's security problems with growth for the future

- Flexible open architecture to accommodate rapid change
- Coordinated, automated security for lower costs and better security

TNC = open network security architecture and standards

- Enables multi-vendor interoperability
- Can reuse existing products to reduce costs and improve ROI
- Avoids vendor lock-in

TNC has strongest security

- Optional support for TPM to defeat rootkits
- Thorough and open technical review

Wide support for TNC standards

- Many vendors, open source, IETF

Copyright© 2011 Trusted Computing Group

Poll Question 3

3. How important is it in your company to restrict network access based on users, devices, their security posture, etc? (choose one)

- Extremely important
- Somewhat important
- Not important

BOEING

Engineering, Operations & Technology
Information Technology

Automate to Win: The Business Case

Steven Venema, PhD, ATF
Craig Dupler, TF
26 April 2011

TRUSTED COMPUTING GROUP™

Overview

- **Where IT Meets Industrial Controls**
- **A Standards-Based Solution using TNC's IF-MAP**
- **Broader Implications**
  - **Harnessing our Dark Matter**

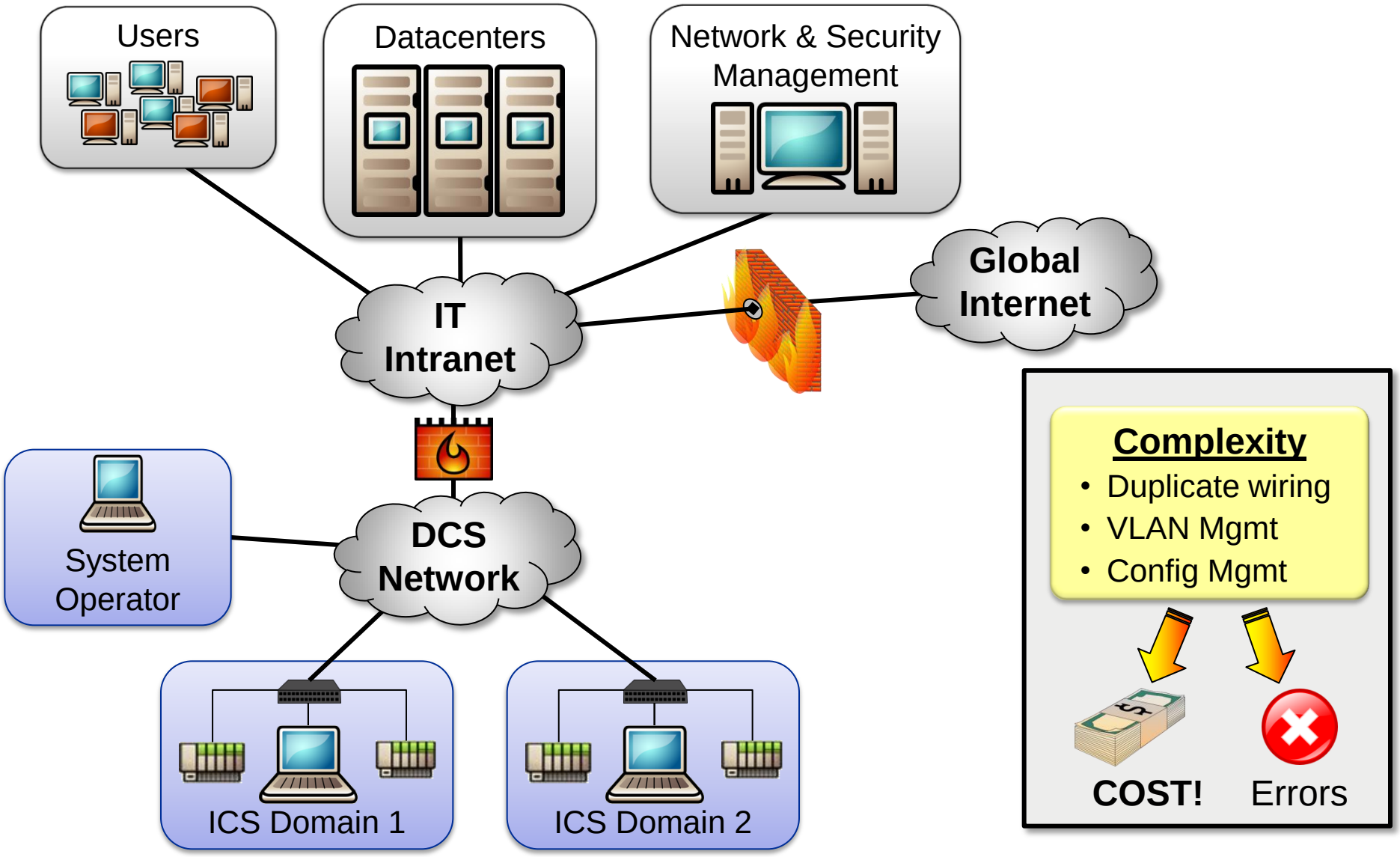
Industrial Control Systems (ICS/SCADA) and General IT Systems Don't Play Well Together



Why NAC Matters for ICS & SCADA

- **Controllers and Control Protocols have very weak authentication/authorization**
  - **“If you can Ping it, you can own it” (Eric Byres)**
  - **Need to be sure exactly what is on the control network**
  - **Need to be sure they are behaving well (Infected with Stuxnet anyone?)**
  - **How do we do that with existing technology?**

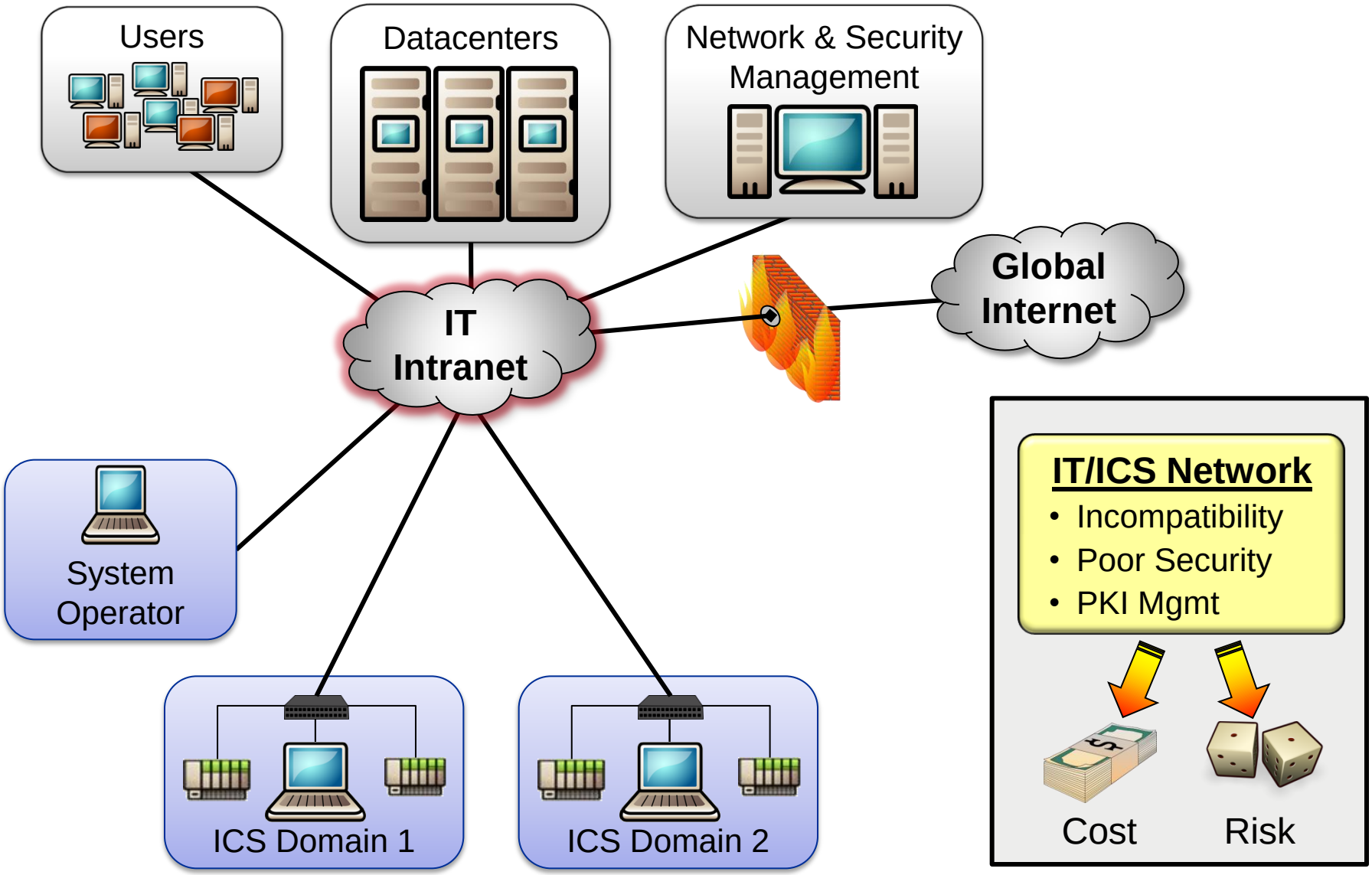
Typical ICS ⇔ IT Shared Network



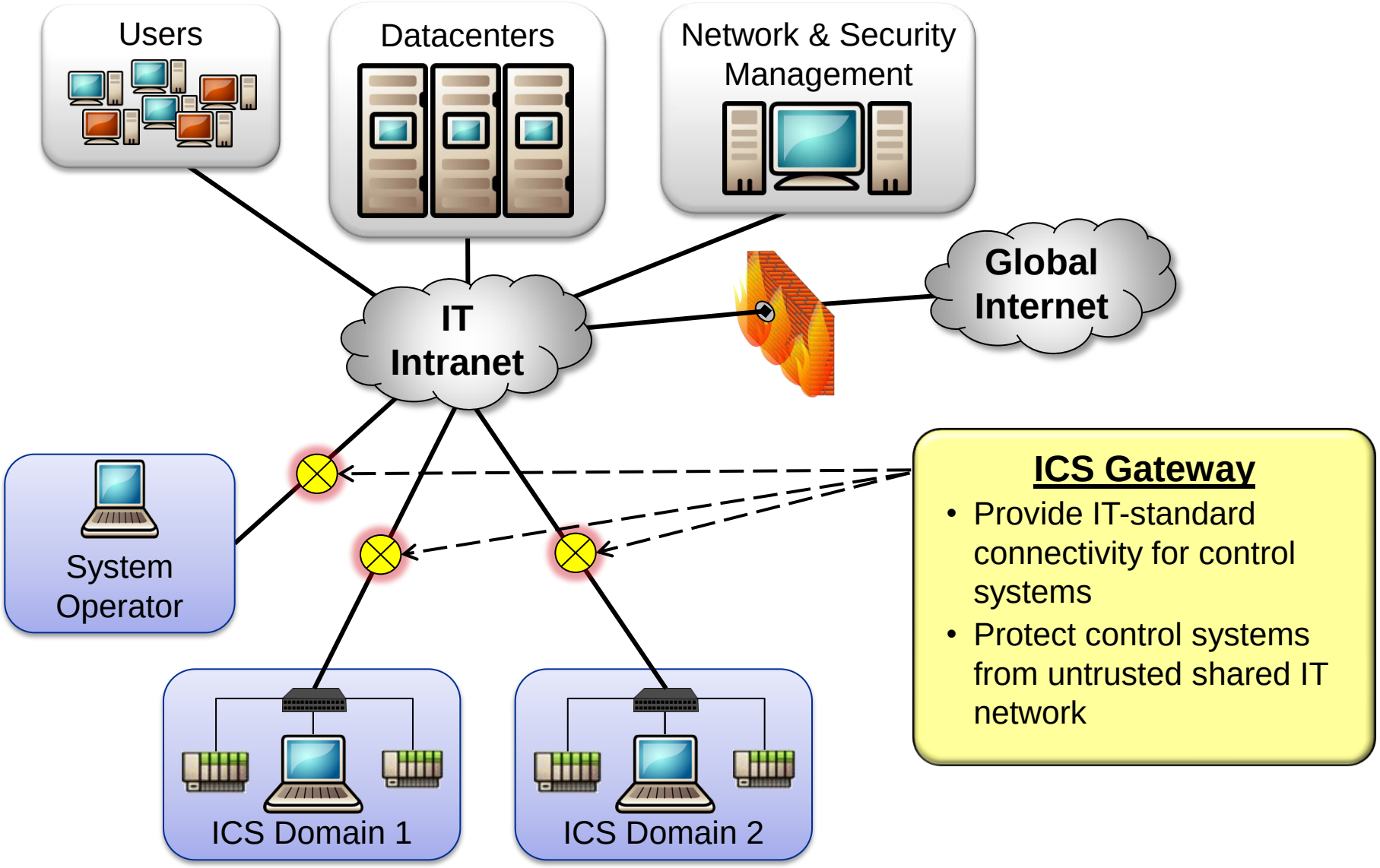
The Cost of Segregated Networks

- **Dual physical infrastructures.**
- **RF management conflicts for wireless.**
- **“Sneaker net” the touch points for**
  - **remote access for troubleshooting and updates**
  - **connectivity for performance data collection**
  - **integrated process visibility systems**
- **Odds are that they will end up touching anyway.**

Ideal ICS ⇔ IT Shared Network



The Solution: Provide a Virtual Secure ICS Network within an Untrusted IT Network

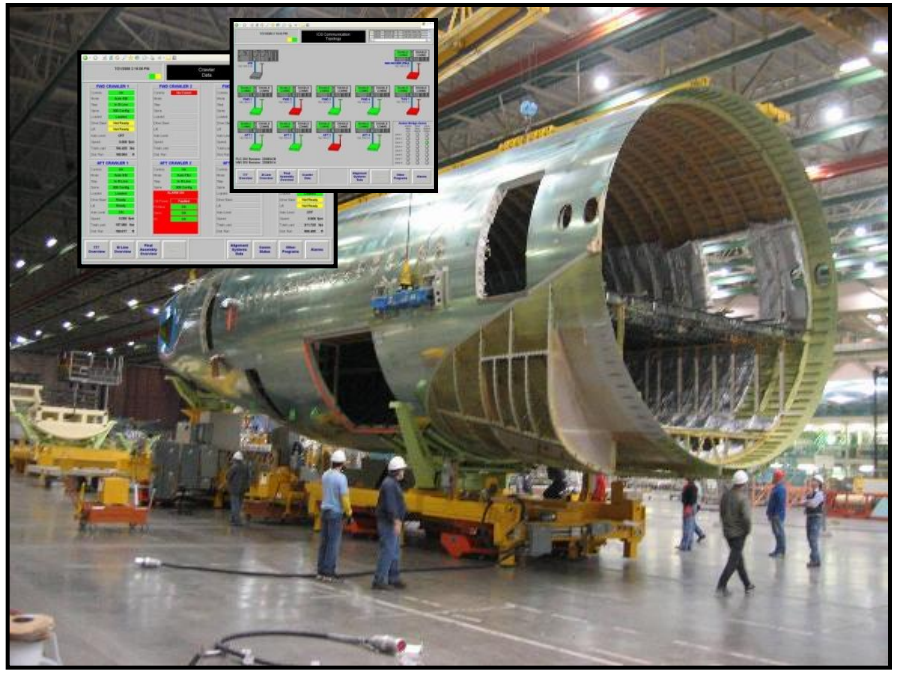


Real Life Example: Connectivity for Crawlers

- **Crawlers: Mobile manufacturing platforms full of PLCs & HMIs**
- **As they move they have different roles and access rights**

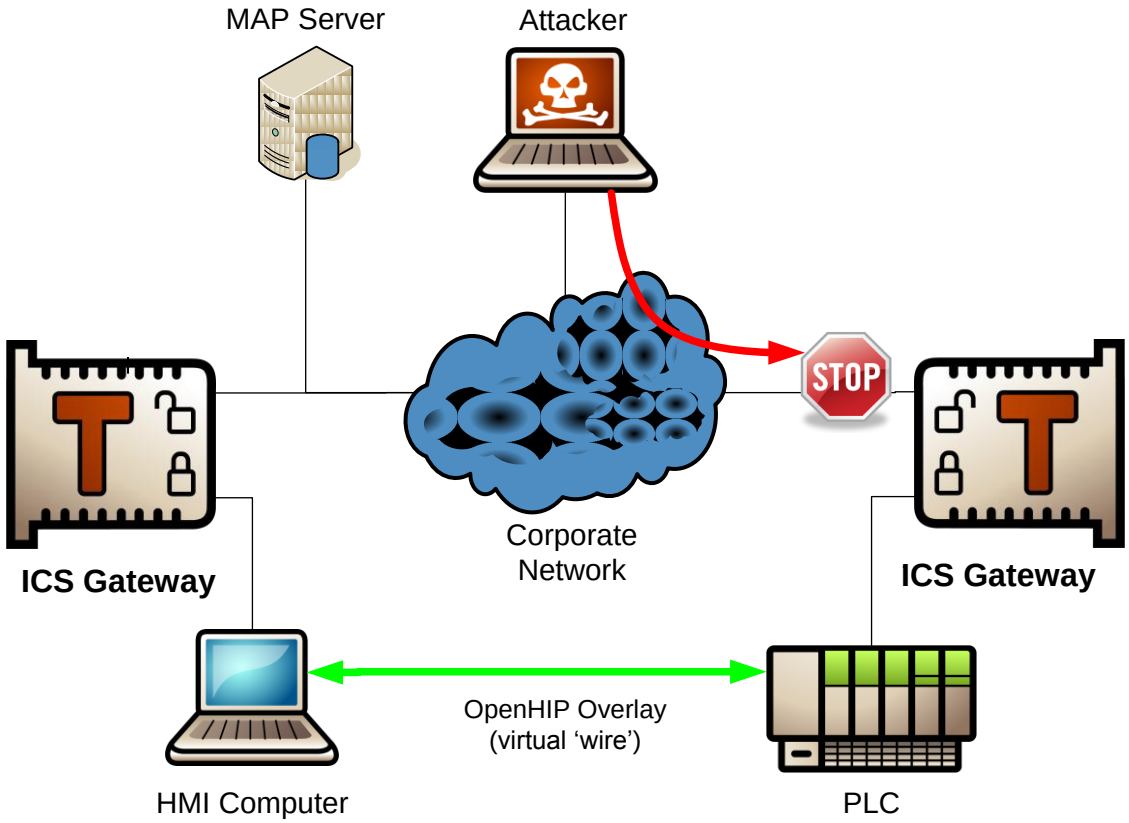
- **Relevant data include:**
  - Auth Tokens/Certificates
  - Crawler position
  - Activities
  - Network conditions
- **Needs to be dynamic, flexible, and highly automated**
  - Can't require IT technicians to constantly tweak config

TNC's Work Applied Here!



Implementing Dynamic, Automated Security

- IP-based industrial control traffic shares the general IT network in the factory
- ICS Gateways provide VPN/firewall security
- ICS Gateway configurations dynamically loaded from MAP server – based on user, location, etc.



Other Organizations See the Value in an Orchestration Standard for ICS/SCADA (ISA 100.15)

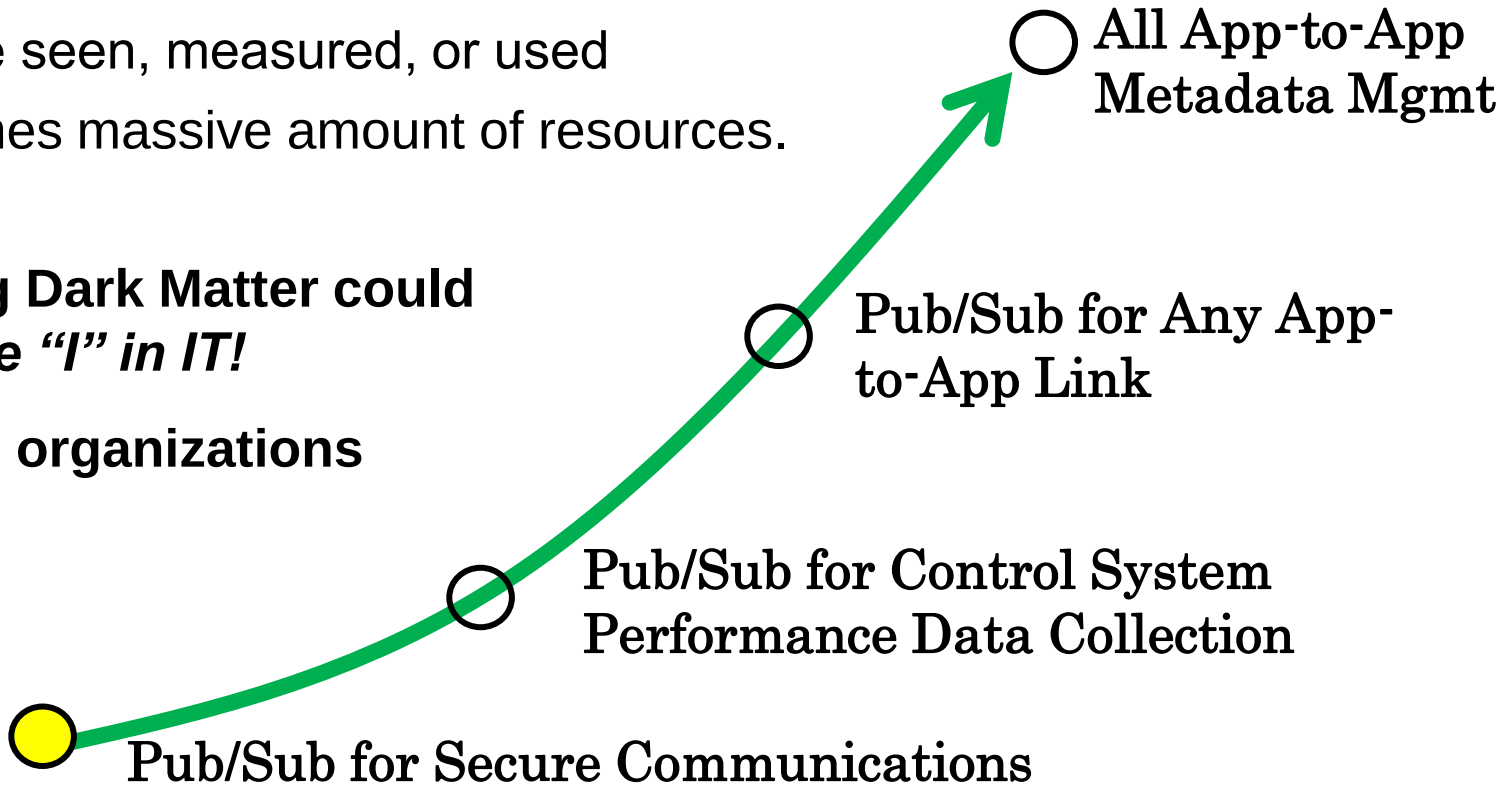
- **Goal: Implement secure over untrusted networks based on application-level constraints**
  - Working Group Title: “Wireless Backhaul”
- More flexible and easier to manage than VPNs, VLANs
- **Participants:**
  - ExxonMobile, Shell, GE, Boeing, etc.
  - Honeywell, Siemens, Yokogawa, Cisco, etc.
  - Cooperation activity with Fieldbus Foundation
  - Collaboration with Security & Embedded Systems Forums at The Open Group

Other Uses of Metadata & MAP

- **Extensions of the Security Use case:**
  - Combined physical security and SCADA cyber security
  - Convergence of IT networks/security and industrial controls security
- **Location Services:**
  - Coordination of supply chains and process flow across one or more Enterprises
- **Process/Event coordination:**
  - Too many business process today are coordinated synchronously or (worse yet) open loop
  - The asynchronous Pub/Sub notification capability built into the MAP database can give us a new coordination pattern for many business processes

The BIG Big Idea

- **Leverage Metadata Access Points for other IT Needs**
- **Much of the information within an enterprise is "Dark Matter" – unstructured data.**
  - Can't be seen, measured, or used
  - Consumes massive amount of resources.
- **Unleashing Dark Matter could *put the "I" in IT!***
- **Transform organizations**



Q&A

Please Submit Your Questions Now

Resources

To View This or Other Events On-Demand Please Visit:

http://www.netseminar.com

For more information please visit:

Technical

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

Business

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