
# TNC: Open Standards for Network Security Automation

# Agenda

## Introduce TNC and TCG

## Explanation of TNC

- What problems does TNC solve?
- How does TNC solve those problems?
- TNC Architecture and Standards
- TNC Adoption and Certification
- TNC Advantages
- Case Studies

## Summary

## For More Information

# Trusted Network Connect

## Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing

## Open Standards for Network Security

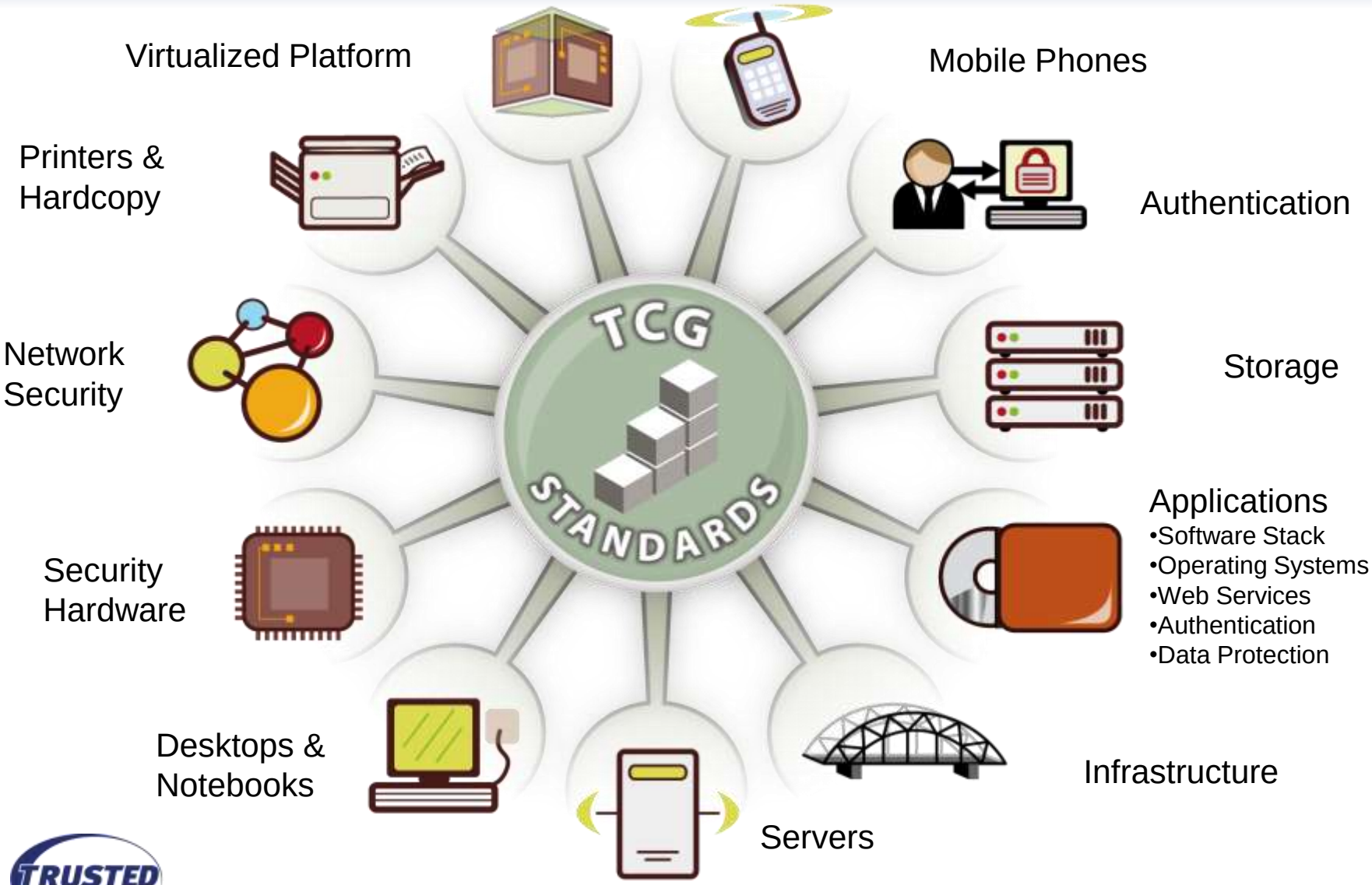
- Full set of specifications available to all
- Products shipping for almost five years

## Developed by Trusted Computing Group (TCG)

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

# TCG: Standards for Trusted Systems



# Trusted Platform Module (TPM)

Security hardware on motherboard

- Open specifications from TCG
- Resists tampering & software attacks

Now included in almost all enterprise PCs

- Off by default; opt in

Features

- Secure key storage
- Cryptographic functions
- Integrity checking & remote attestation

Applications

- Strong user and machine authentication
- Secure storage
- Trusted / secure boot

# 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 Enforcement

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

Network Access Control (NAC)

Device Remediation

- Quarantine and repair unhealthy devices

Security System Integration

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

Coordinated Security

# Sample Network Access Control Policy

To Access the Production Network…

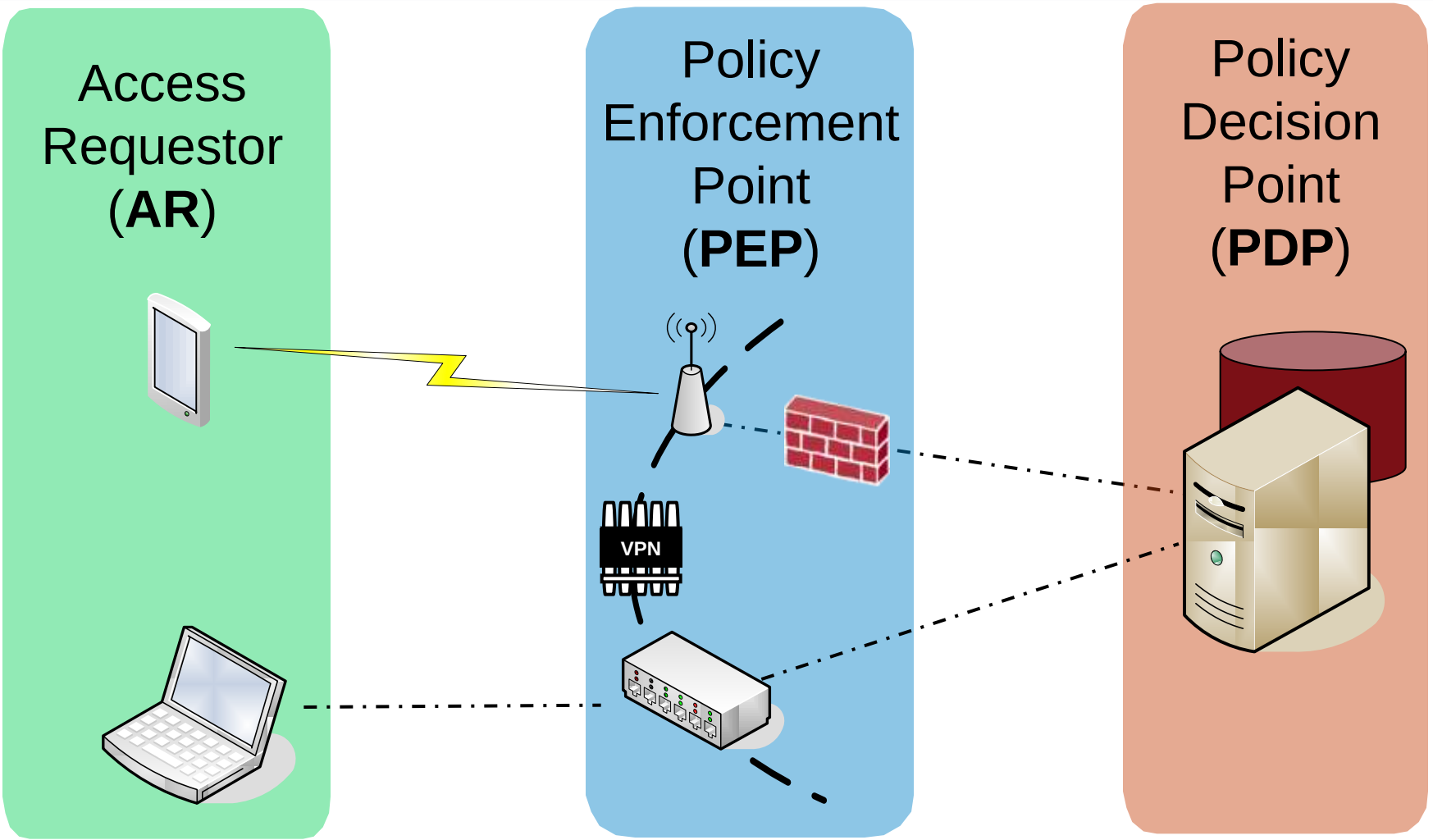
1. User Must Be Authenticated
   - With Identity Management System

2. Endpoint Must Be Healthy
   - Anti-Virus software running and properly configured
   - Recent scan shows no malware
   - Personal Firewall running and properly configured
   - Patches up-to-date

3. Behavior Must Be Acceptable
   - No port scanning, sending spam

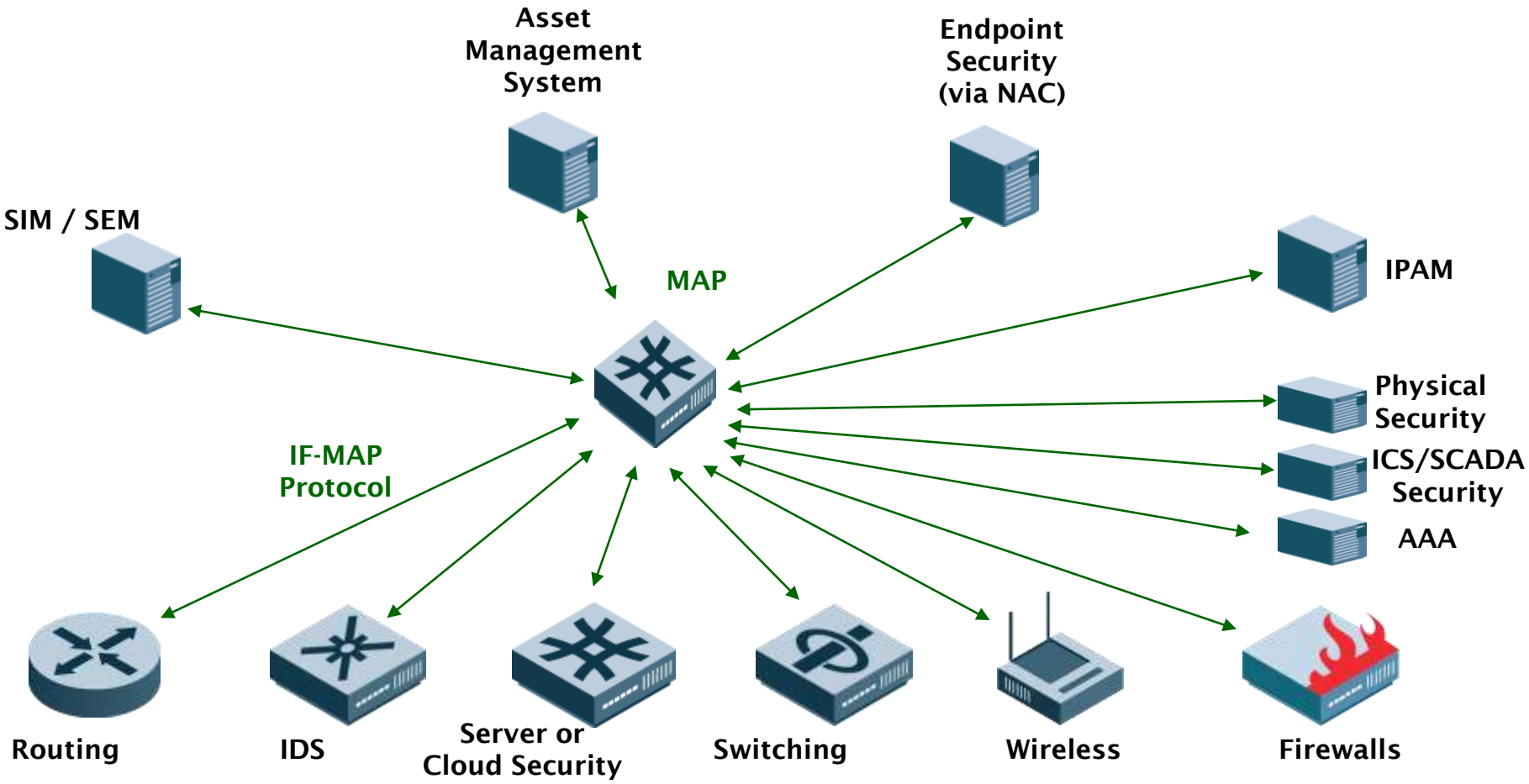
 

# NAC Architecture



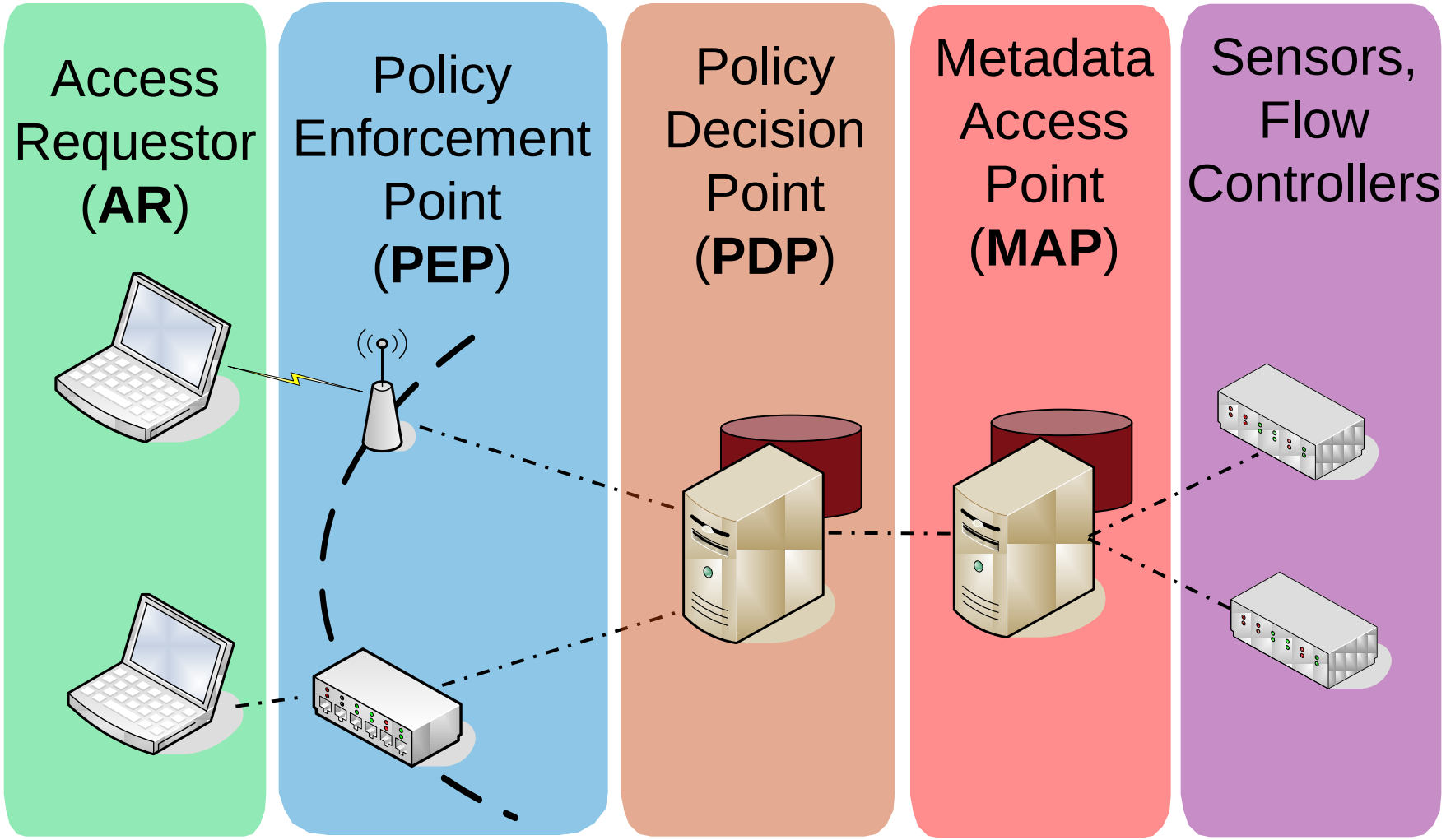

 

# Coordinated Security



# Coordinated Security & NAC Together



# Typical TNC Deployments

Health Check

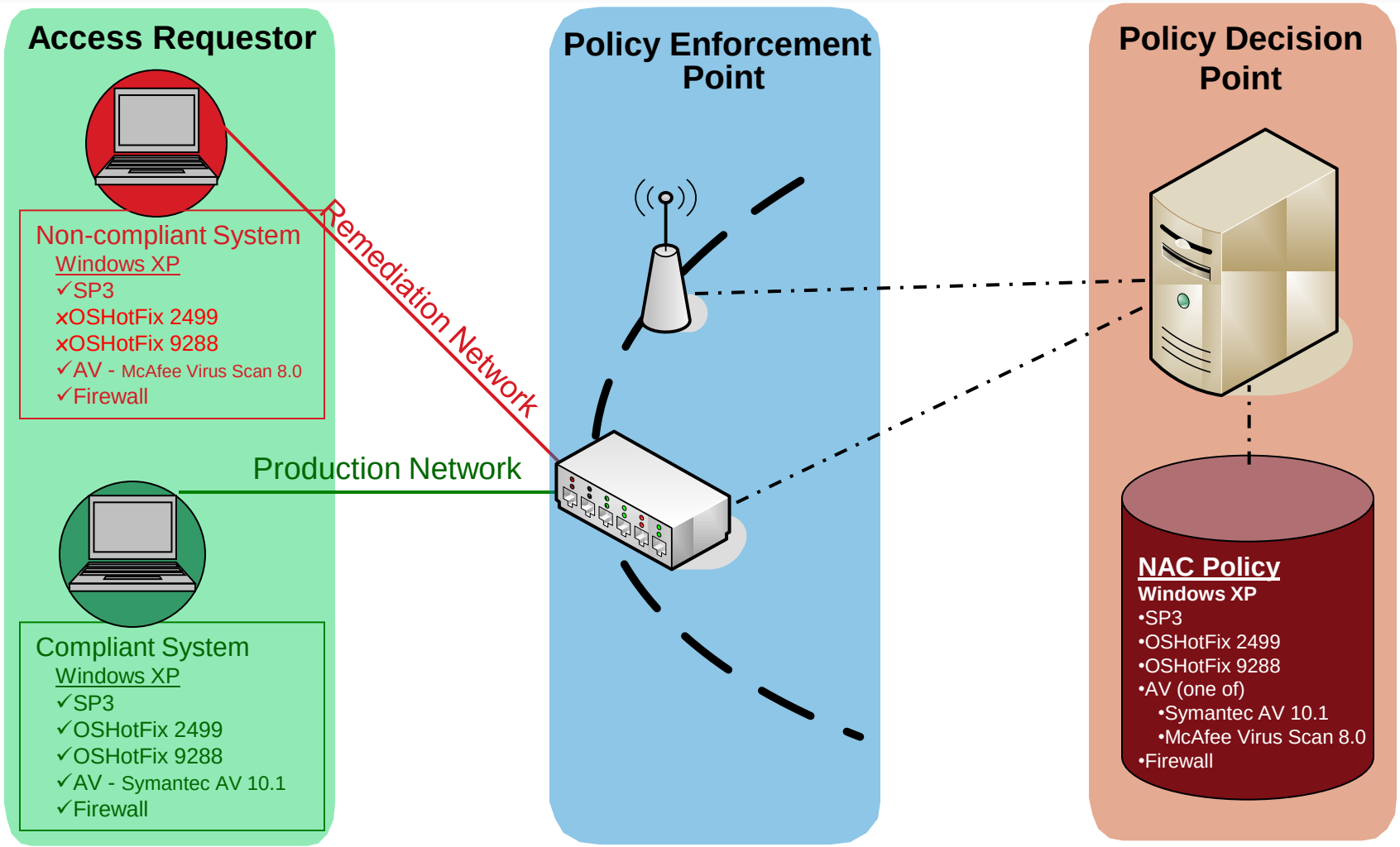
Behavior Check

User-Specific Policies

TPM-Based Integrity Check

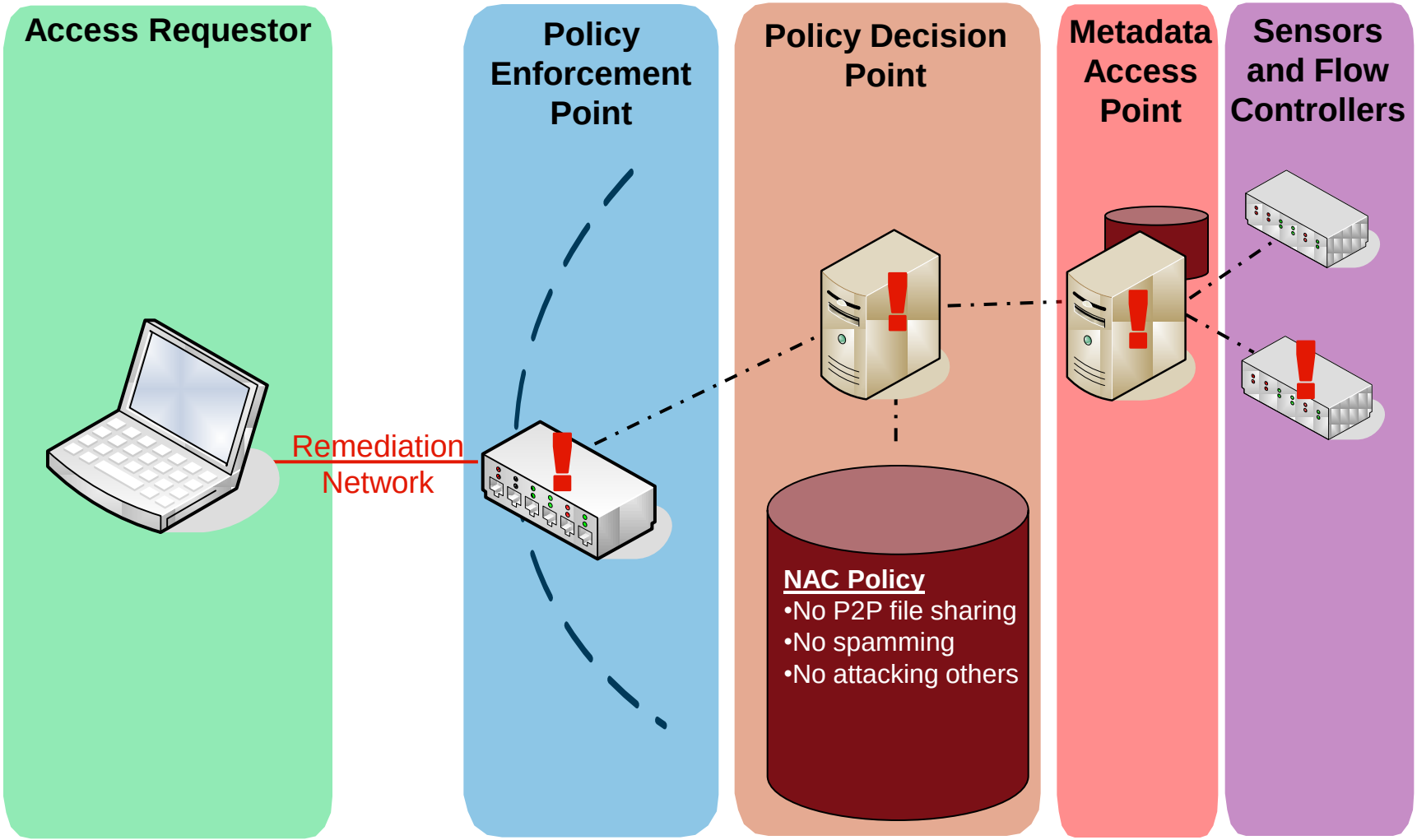
 

# Health Check



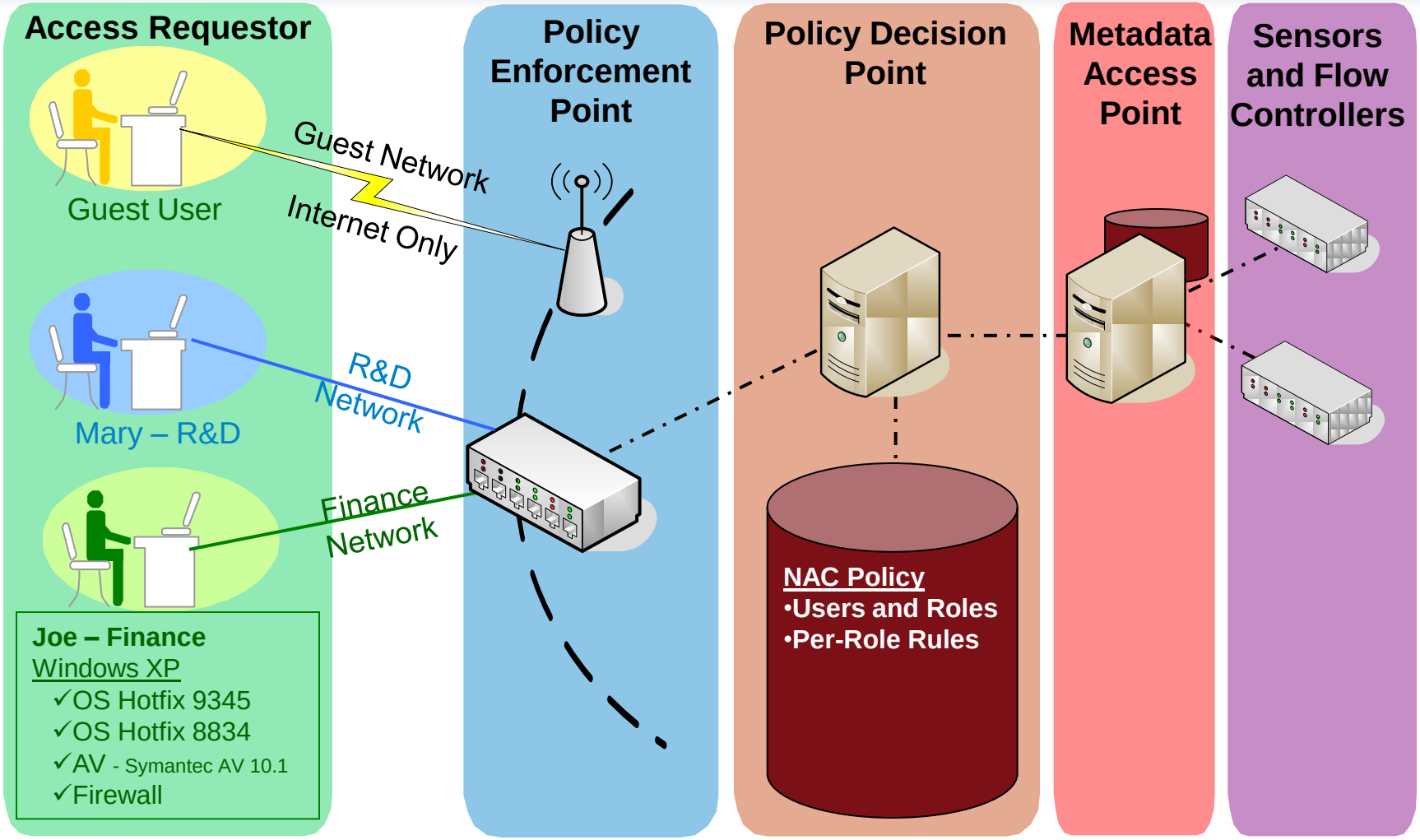

 

# Behavior Check



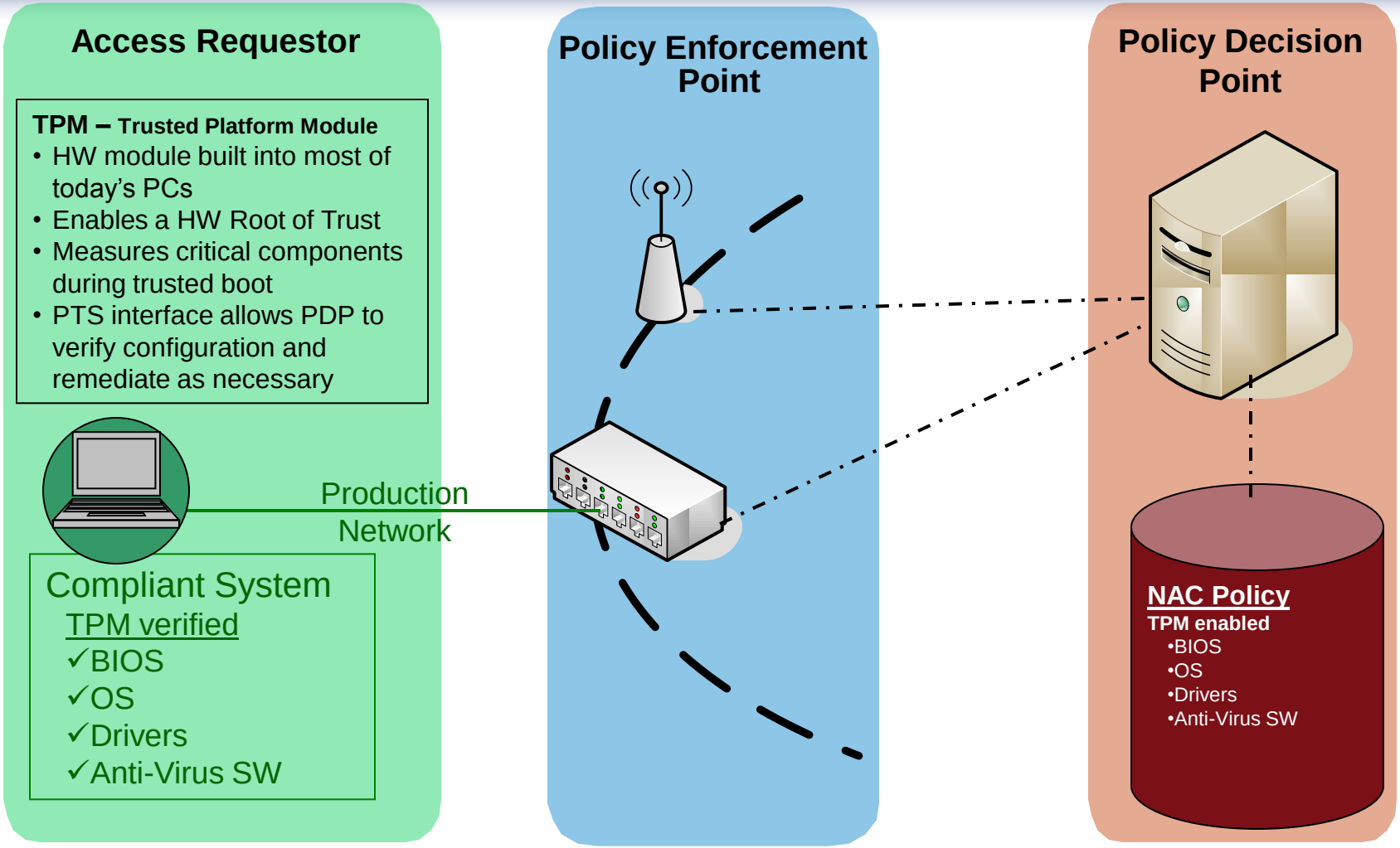

 

# User-Specific Policies



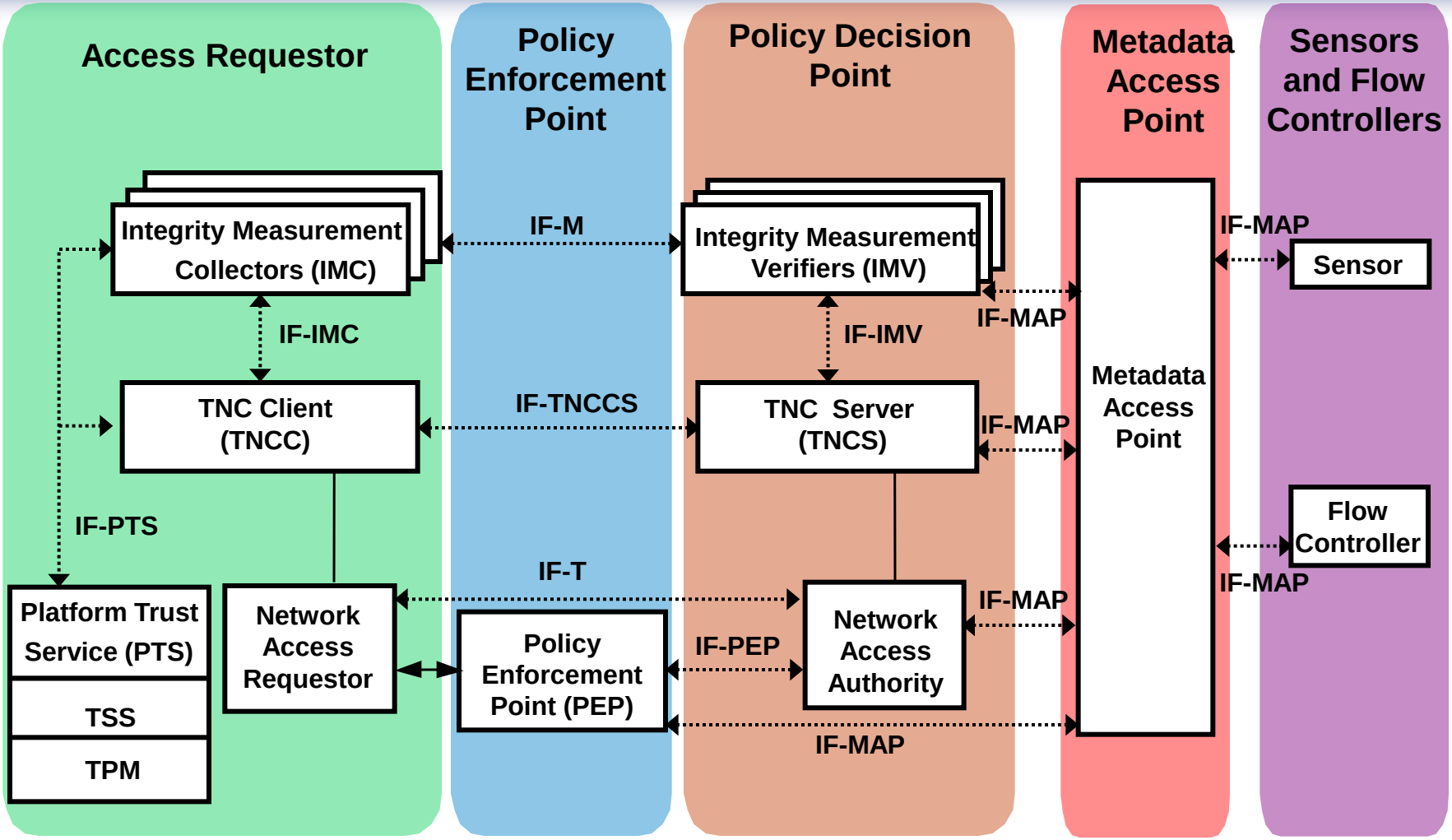

 

# TPM-Based Integrity Check



# TNC Architecture



# Foiling Root Kits with TPM and TNC

Solves the critical “lying endpoint problem”

TPM Measures Software in Boot Sequence

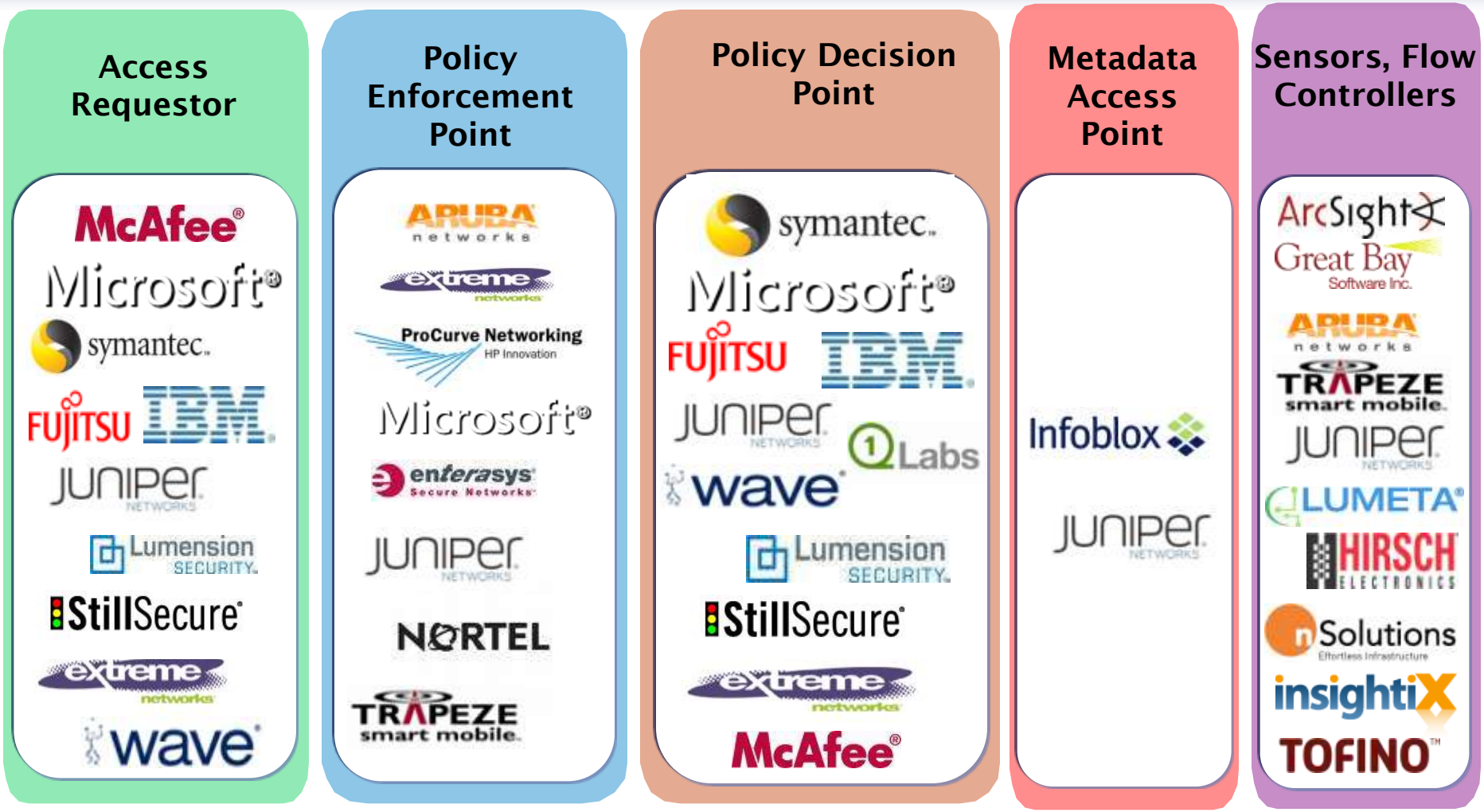
- Hash software into PCR before running it
- PCR value cannot be reset except via hard reboot

During TNC Handshake…

- PDP engages in crypto handshake with TPM
- TPM securely sends PCR value to PDP
- PDP compares to good configurations
- If not listed, endpoint is quarantined and remediated

# TNC 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
- libtnc
  http://sourceforge.net/projects/libtnc
- OpenSEA 802.1X supplicant
  http://www.openseaalliance.org
- FreeRADIUS
  http://www.freeradius.org
- omapd IF-MAP Server
  http://code.google.com/p/omapd
- IF-MAP Client Code
  http://ifmapdev.com/

# IETF and TNC

## IETF NEA WG

- Goal: Universal Agreement on NAC Client-Server Protocols
  - Co-Chaired by Cisco employee and TNC-WG Chair

## Published several TNC protocols as IETF RFCs

- PA-TNC (RFC 5792) and PB-TNC (RFC 5793)
- Equivalent to TCG's IF-M 1.0 and IF-TNCCS 2.0
- Co-Editors from Cisco, Intel, Juniper, Microsoft, Symantec

## Now working on getting IETF approval for IF-T

# TNC Certification Program

## Certifies Products that Properly Implement TNC Standards

## Certification Process

- Compliance testing using automated test suite from TCG
- Interoperability testing at Plugfest
- Add to list of certified products on TCG web site

## Customer Benefits

- Confidence that products interoperate
- Easy to cite in procurement documents



# TNC in the Real World

## Widely Deployed

- Millions of Seats
- Thousands of Customers
- Dozens of Products

## Across Many Sectors

- Government
- Finance
- Health Care
- Retail …

# 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)

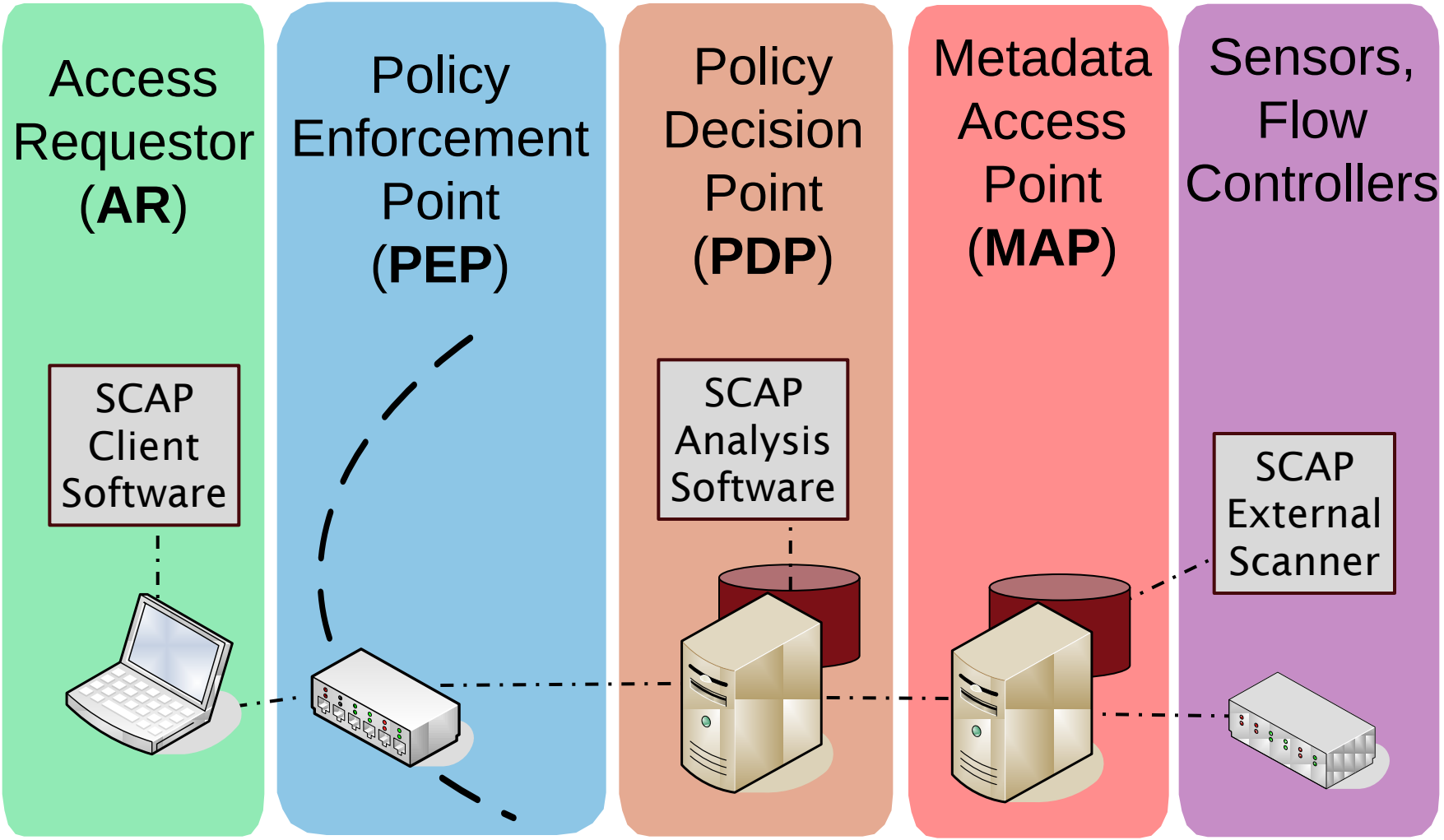
## Roadmap for the future

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

## Products supporting TNC standards shipping today

# TNC and SCAP Together



# Strengths of TNC and SCAP

## TNC Strengths

- Network and Endpoint Visibility
- Network Enforcement
- Device Remediation
- Security System Integration

## SCAP Strengths

- Device Assessment
- Compliance Management
- Deep, Consistent Content Libraries

## Both SCAP and TNC

- Open Standards
- Vendor Neutral
- Widely Implemented

# Benefits of TNC and SCAP Together

## Security automation

- At the desktop (SCAP)
- In the network (TNC)
- Across all security systems (TNC)

- … Leading to lower costs and stronger security

## Open standards throughout

- Completely vendor-neutral
- Enables multi-vendor interoperability
- Lower vendor integration costs – O(n) vs. $O(n^2)$
- Lower customer costs – develop content once, deploy widely

# 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

# Upcoming TNC-Related Sessions

## Security Coordination with IF-MAP

- Learn more about IF-MAP
- Hear about specific applications
- Next session in this room (Tuesday, 3:45-4:30 PM)

## 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)

# Questions? Discussion?

# 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