TCG TNC:
Automating End-to-end Trust

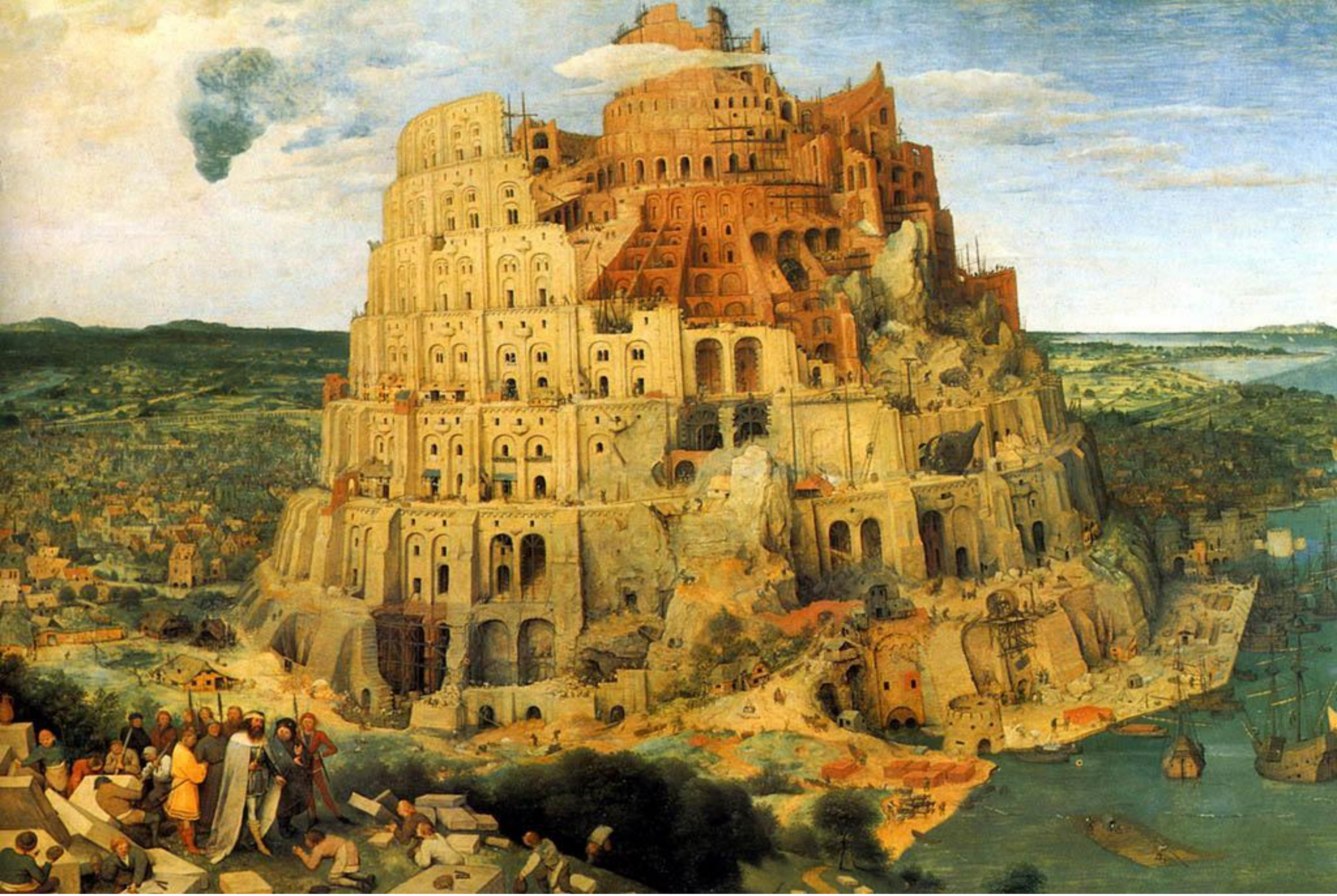
Lisa Lorenzin
Principal Solutions Architect
Pulse Secure

9/9/2015

R 208
R 188
R 216
R 28
RM58
1454

冨嶽三十六景
神奈川沖
浪裏
北斎改為一筆

DEPTH
GAUGE
90 ft.
CARL BARKS
© WALT DISNEY PRODUCTIONS

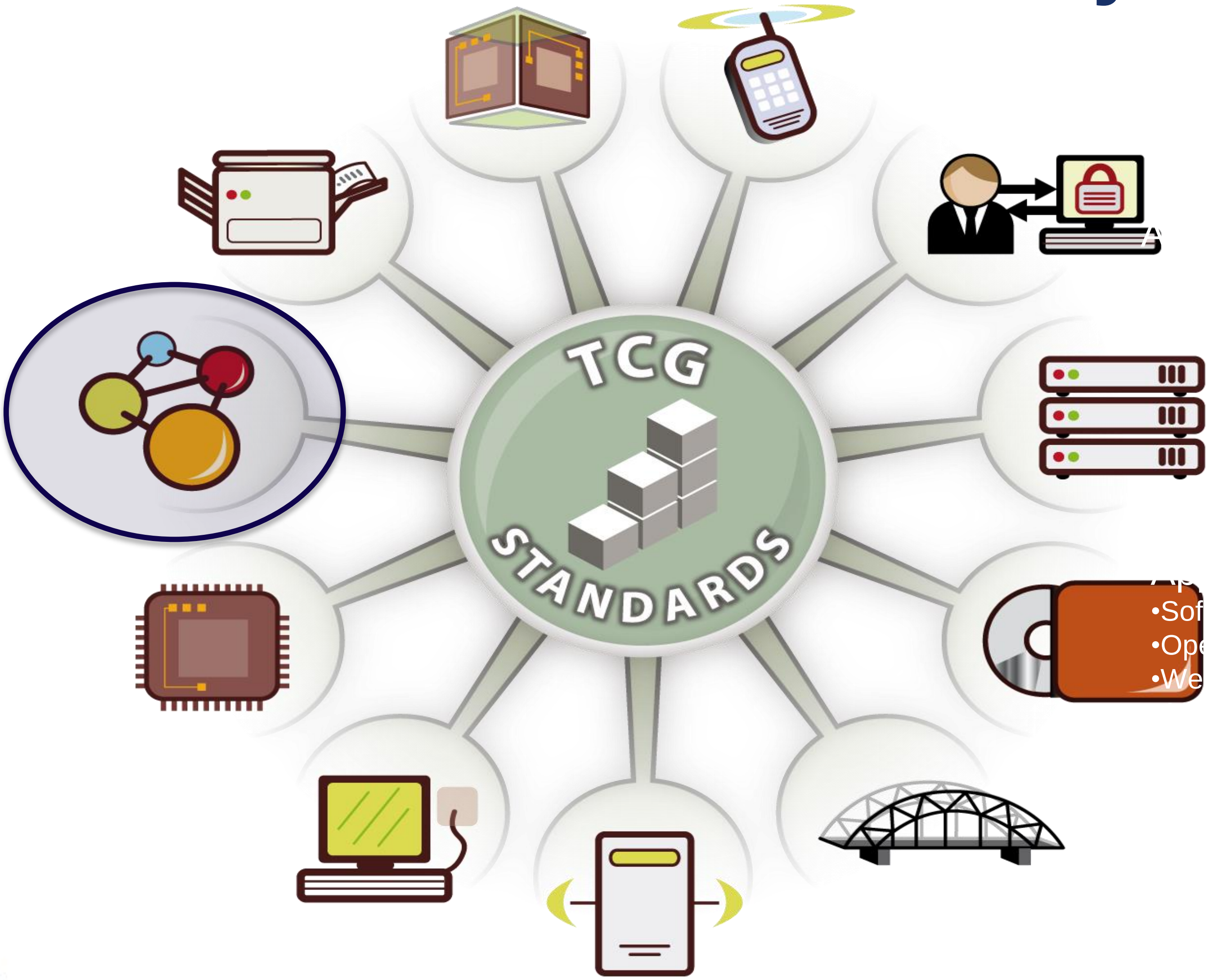


Trusted Network Communications

- Open Architecture for Network Security
  - Completely vendor-neutral
  - Strong security through trusted computing
  - Original focus on NAC; now expanded to also include Compliance and Orchestration

- Open Standards for Network Security
  - Full set of specifications available to all
  - Products shipping since 2005.

TCG: Standards for Trusted Systems



The Trusted Computing Group

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

Problems Solved by TNC

- Network and Endpoint Visibility
  - Who and what's on my network?

Compliance

- Endpoint Compliance
  - Are devices on my network secure?
  - Is user/device behavior appropriate?
- Network Enforcement
  - Block unauthorized users, devices, or behavior
  - Grant appropriate levels of access to authorized users/devices

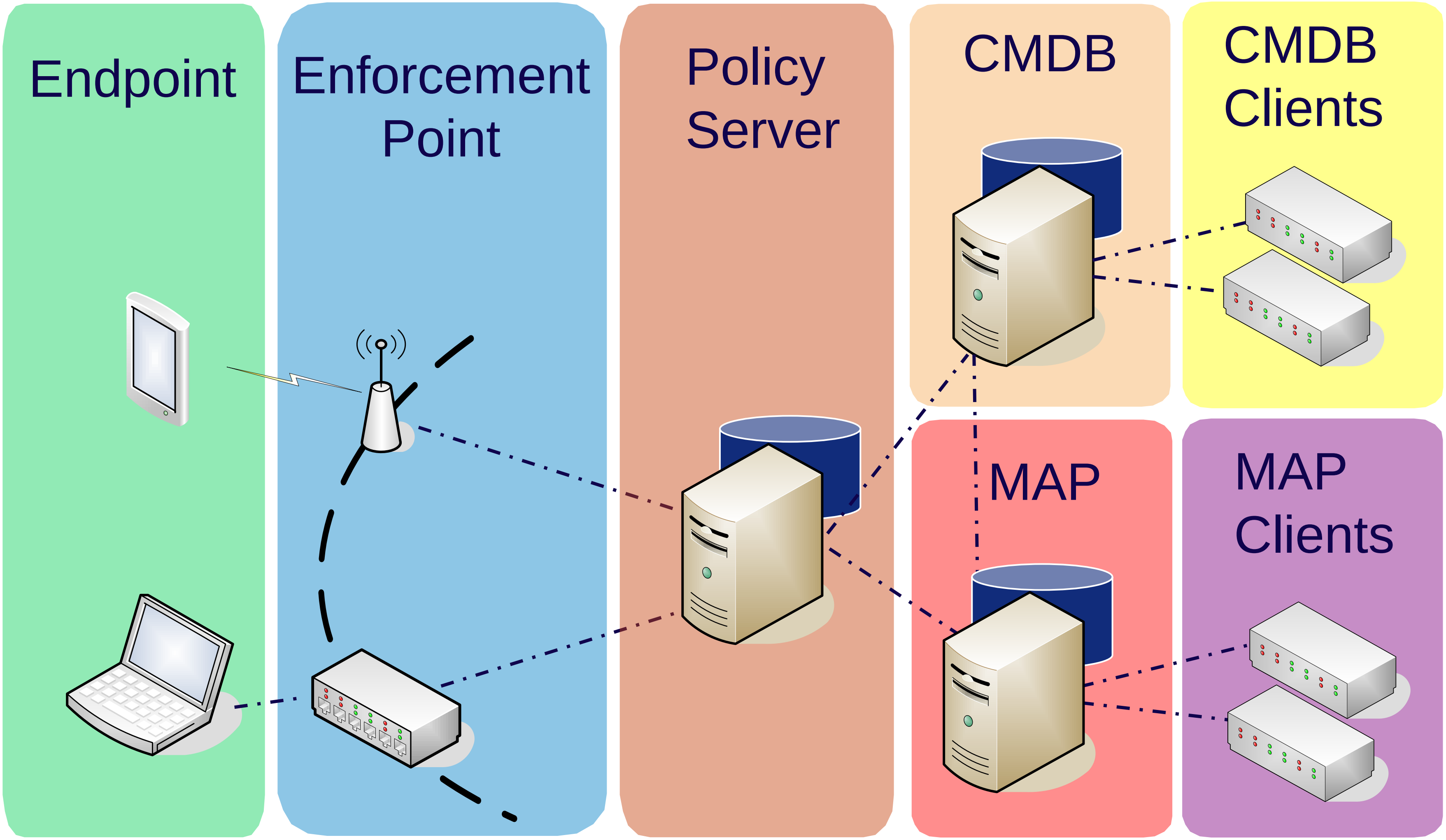
Access Control

Orchestration

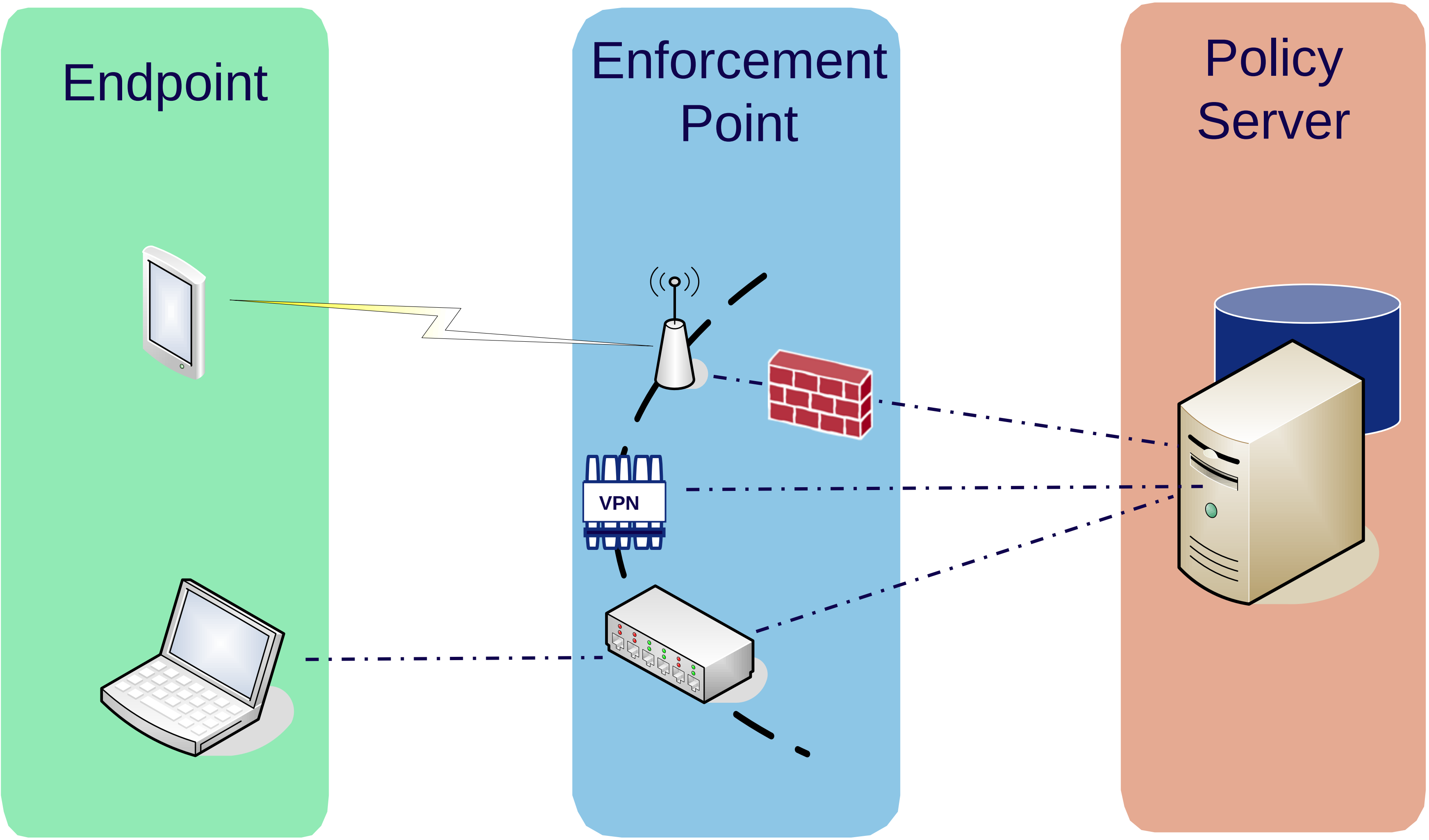
- Security System Integration
  - Share real-time information about users, devices, threats, etc.

TNC Solutions

TNC Capability – Access Control

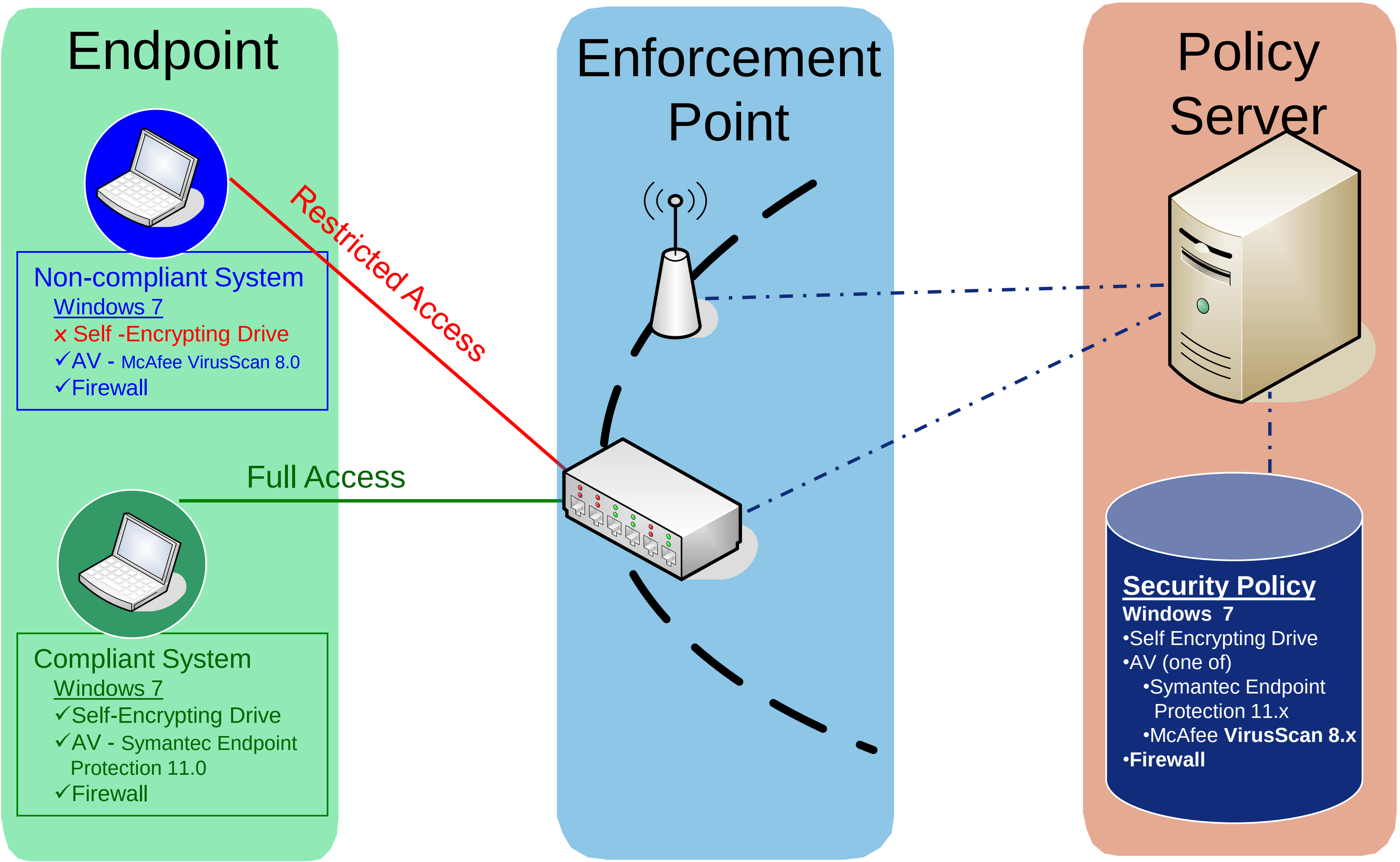


TNC Capability – Access Control



© 2015 Trusted Computing Group

TNC Solution – Health Check



Endpoint

Non-compliant System

Windows 7

✗ Self -Encrypting Drive

✓AV - McAfee VirusScan 8.0

✓Firewall

Compliant System

Windows 7

✓Self-Encrypting Drive

✓AV - Symantec Endpoint Protection 11.0

✓Firewall

Restricted Access

Full Access

Enforcement Point

Policy Server

Security Policy

Windows 7

•Self Encrypting Drive

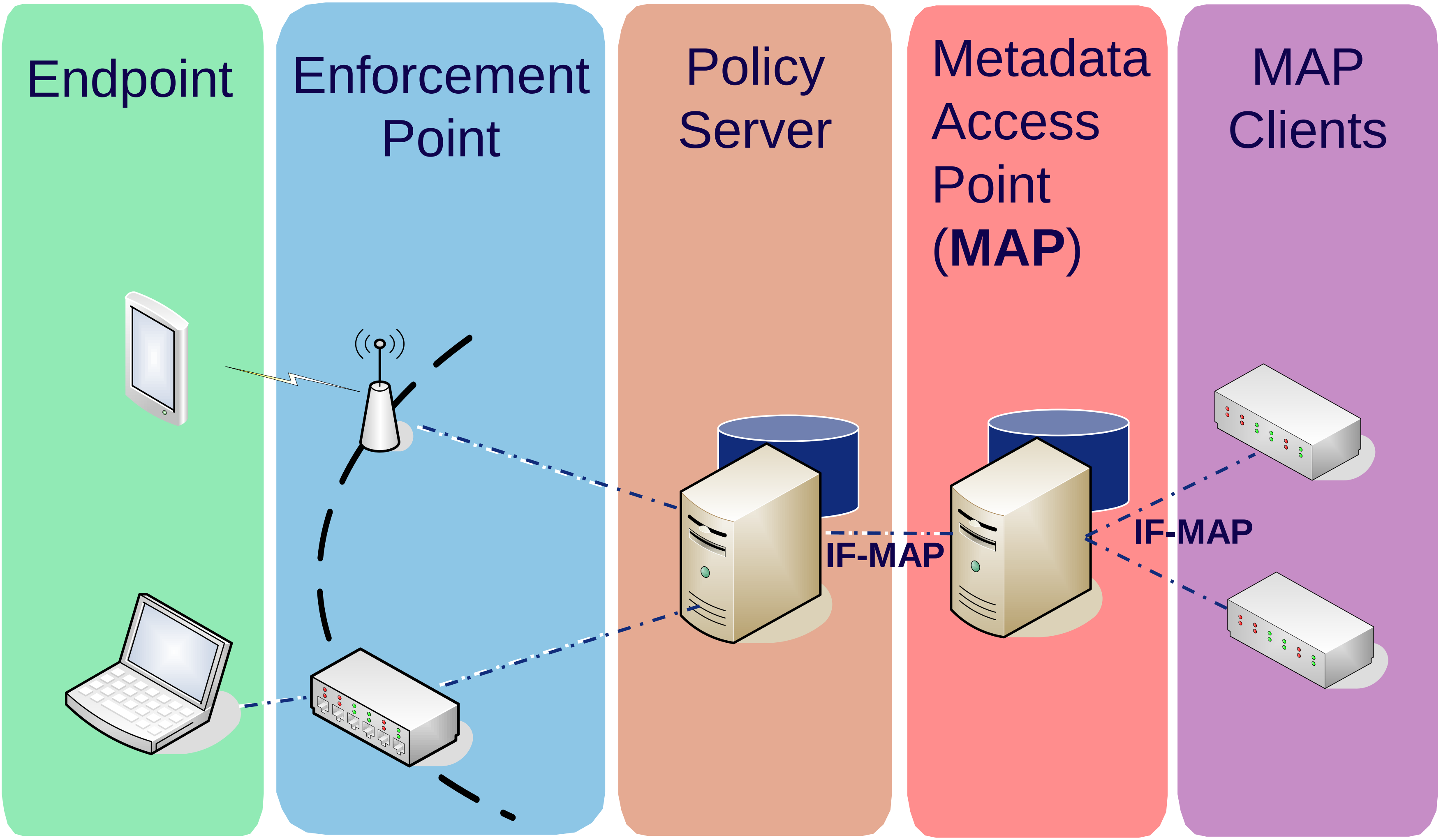
•AV (one of)

•Symantec Endpoint Protection 11.x

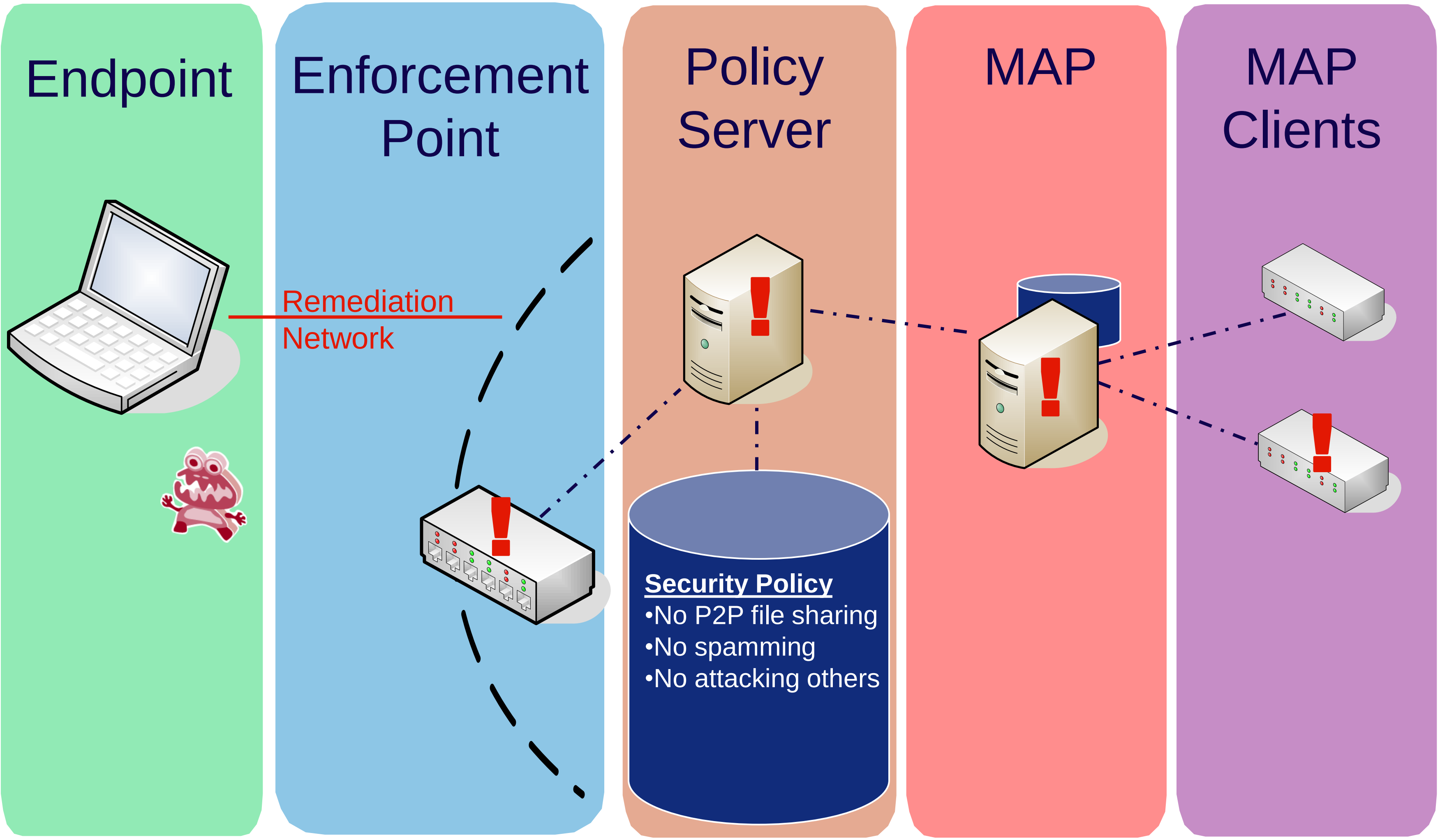
•McAfee **VirusScan 8.x**

•**Firewall**

TNC Capability – Security Automation



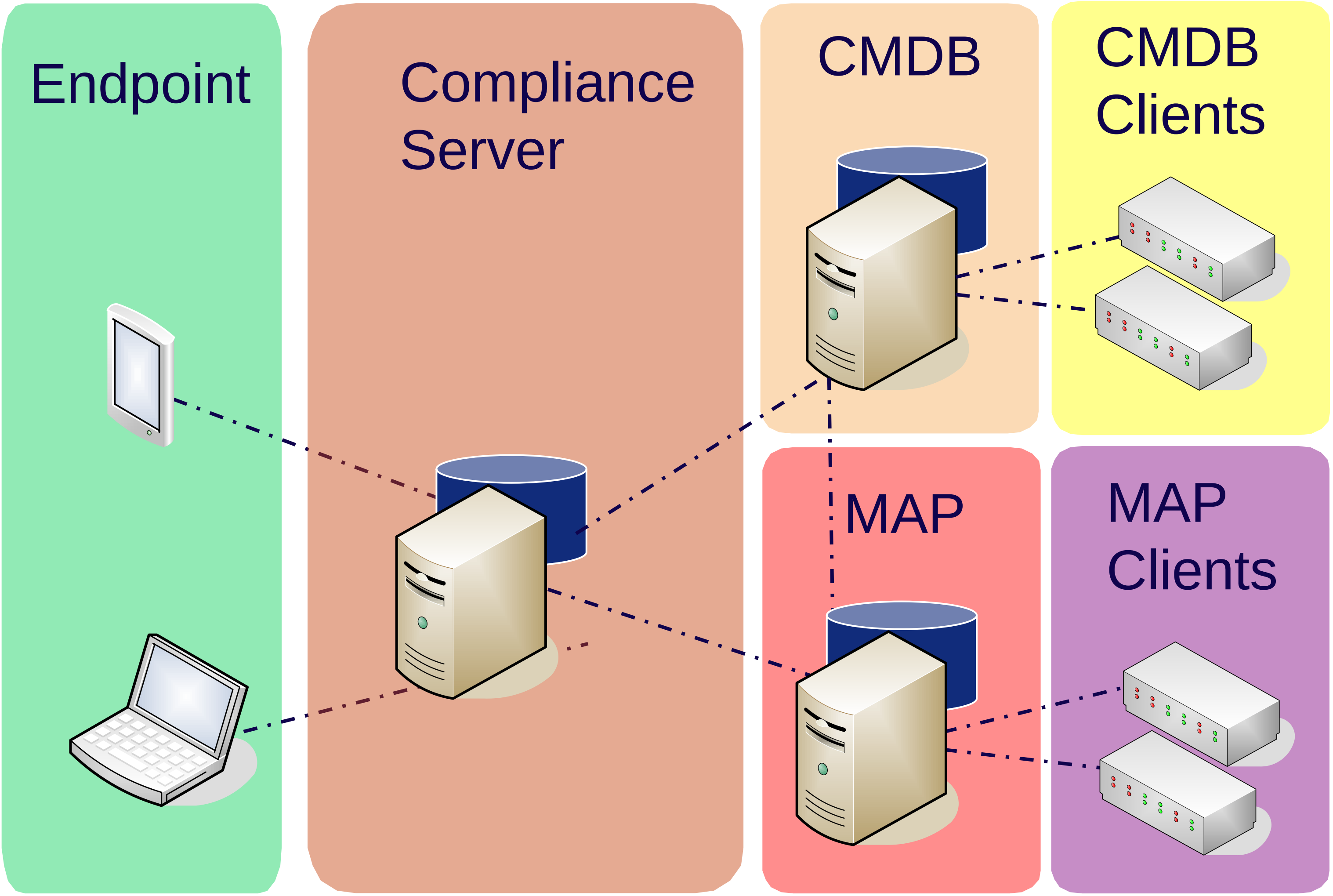
TNC Solution – Behavior Check



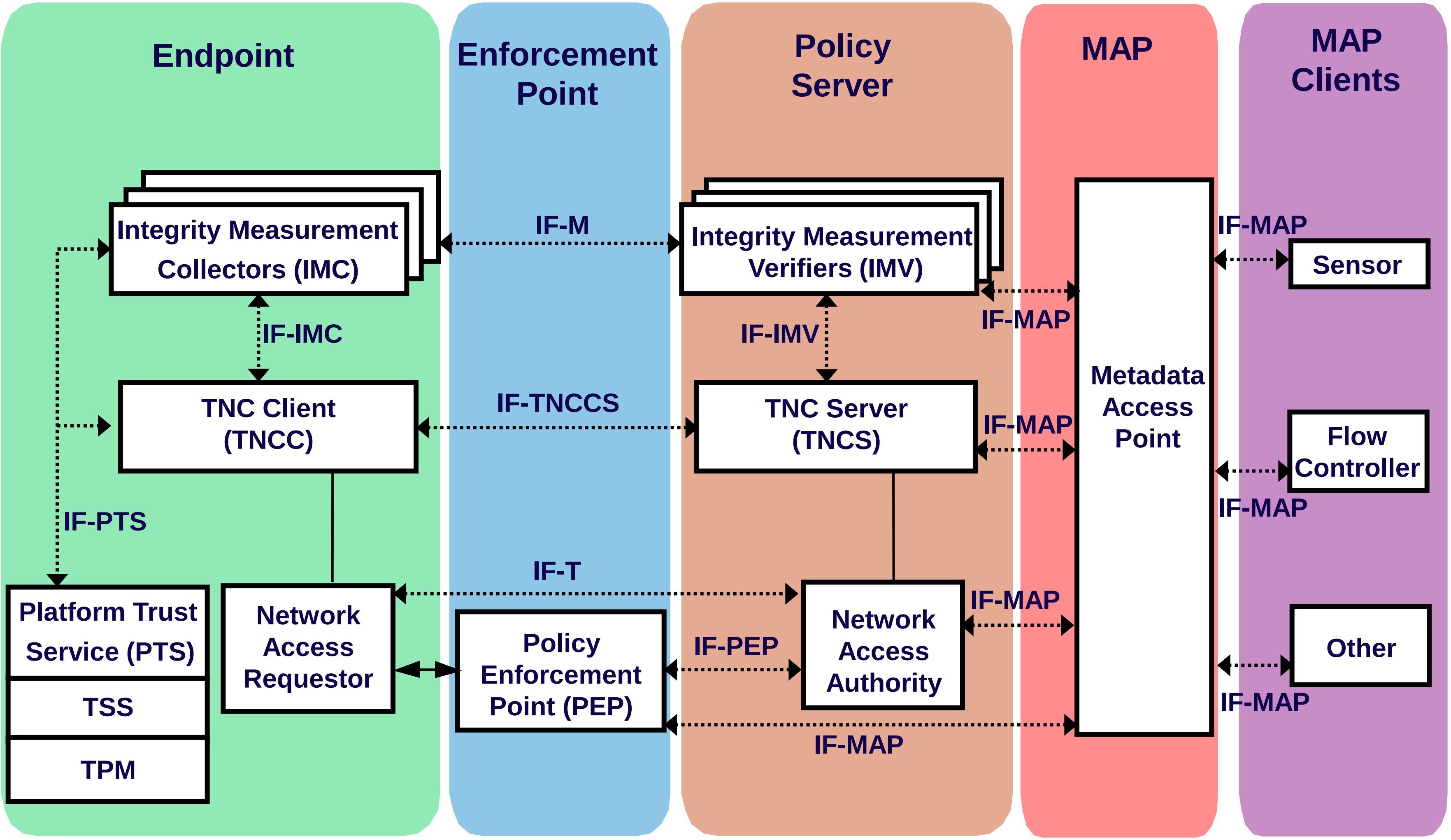
Security Policy

- No P2P file sharing
- No spamming
- No attacking others

TNC Capability – Compliance



TNC Interfaces



http://www.trustedcomputinggroup.org/developers/trusted_network_communications/specifications

SWID Messages and Attributes for IF-M

- **Latest TNC Specification**
  - http://www.trustedcomputinggroup.org/resources/tnc_swid_messages_and_attributes_for_ifm_specification
  - Specification and FAQ published August 2015

- **Standardizes the collection and exchange of SWID tag information**
  - Defines how IMCs monitor the endpoint for changes to its SWID tag collection
  - Defines the structure IMCs use to send SWID-related information to an IMV
  - Supports exchange of full inventory or deltas driven by change events
  - Supports targeted queries from an IMV (e.g., presence of specific SWID tags on an endpoint)

SWID Message and Attributes, cont.

- Inventory data sourced from multiple sources
  - XML files collected from an endpoint’s file system
  - Dynamically generated SWID tags from other software management systems (e.g., RPM)

- Inventory reports can consist of:
  - Full tags providing detail
  - The unique SWID tag identifier in a more concise representation

Endpoint Compliance Profile (ECP)

- Details the use of TNC protocols and interfaces supporting automated gathering of compliance information from endpoints on a network
  - http://www.trustedcomputinggroup.org/resources/tnc_endpoint_compliance_profile_specification
  - Requires that endpoints provide their SWID tag collection to a PDP where it is passed to the CMDB for long-term storage
  - Requires that endpoints monitor for and automatically report relevant changes in their configuration

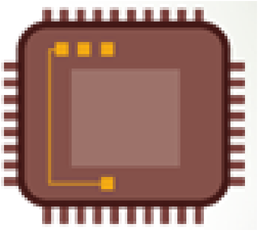
- Uses the SWID Message and Attributes for IF-M specification
  - Enables monitoring of the SWID tag collection on an endpoint
  - Supports spontaneously reporting any observed changes to the PDP

Beyond TNC

TCG 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

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

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), PB-TNC (RFC 5793), PT-TLS (RFC 6876), PT-EAP (RFC 7171)
  - Equivalent to TCG's IF-M 1.0, IF-TNCCS 2.0, and IF-T/TLS
  - Co-Editors from Cisco, Intel, Juniper, Microsoft, Symantec

- TNC members contributing to IETF SACM WG
  - Security Automation & Continuous Monitoring

Summary

- **TNC solves today's security problems, prepares 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
  - Open standards with thorough technical review

- **Wide support for TNC standards**
  - Many vendors, open source, IETF

For More Information

- **TNC Web Site**
  Solutions
  http://www.trustedcomputinggroup.org/solutions/endtoend_trust
  Standards
  http://www.trustedcomputinggroup.org/developers/trusted_network_communications
  Architects Guides
  http://www.trustedcomputinggroup.org/resources/tcg_architects_guides

- **TNC-WG Co-Chairs**

  - **Lisa Lorenzin**
  - Principal Solutions Architect, Pulse Secure
  - llorenzin@juniper.net

  - **Atul Shah**
  - Senior Security Strategist, Microsoft
  - atuls@microsoft.com

Questions?