# Trusted Network Communications and Security Automation

Charles Schmidt

November 17, 2015

# Cybersecurity Automation and/or Standards

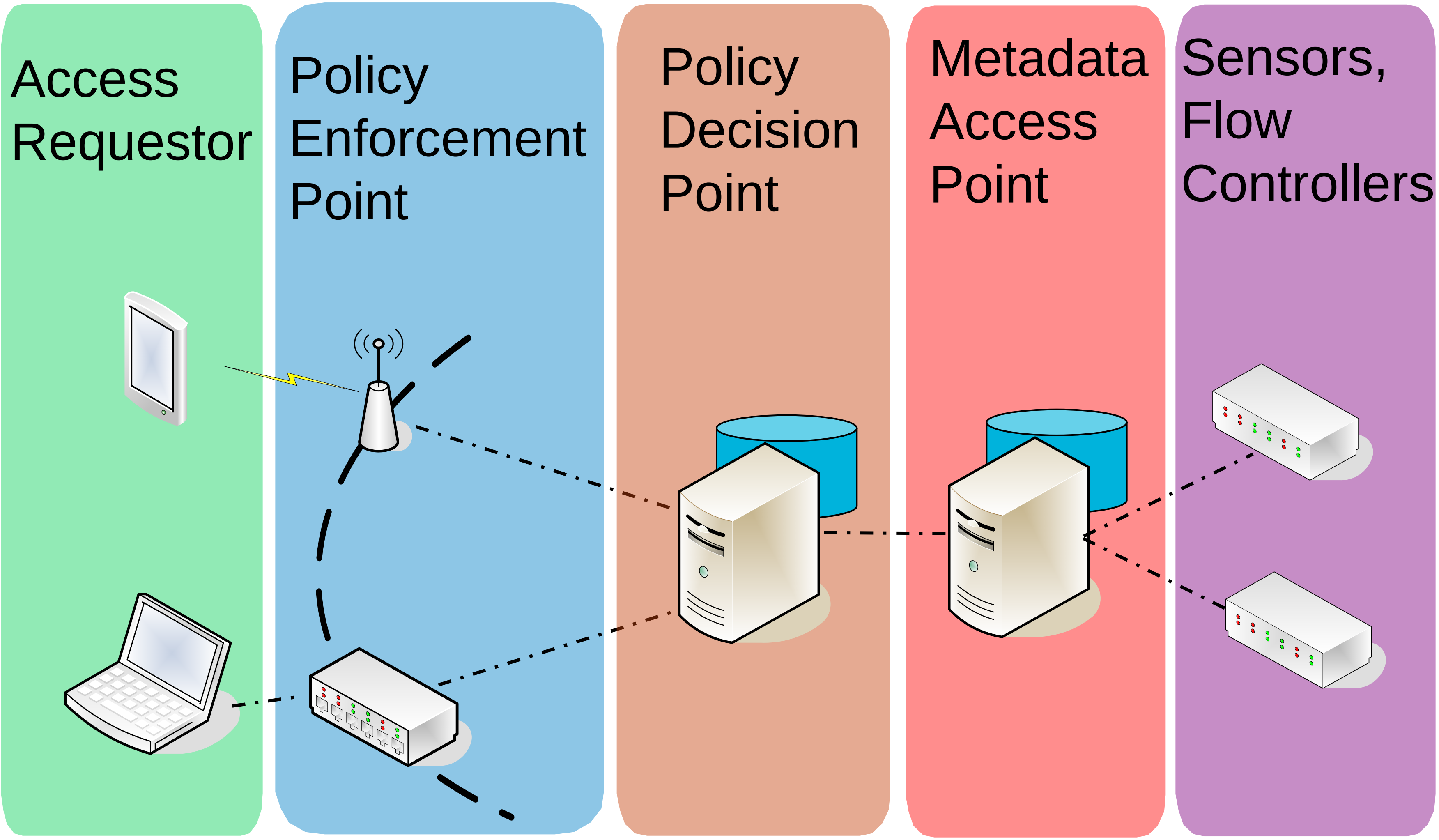
- **Security automation does not require standards**
  - Vendors can and do create proprietary security automation solutions
- **Security automation standards add:**
  - Flexibility
    - Standard extension points
    - Not dependent on one vendor for new capabilities
  - Reduce single-vendor dependency
    - Interchangeable commercial components are a myth, but…
    - Add new components to an enterprise's security automation solution more easily by using standards as capability interfaces
  - Improved transparency
    - See the logic and controls used by tools to collect/analyze/act on data

# What is Trusted Network Communications

- **Supports automation of**
  - Endpoint health/state/compliance monitoring
  - Responses to policy violations
  - Controlled sharing of enterprise state information
    - Enables additional automation in other tools

- **A standardized architecture to support endpoint assessment, network access control, and controlled sharing of network state information**
- **Architecture is supported by a collection of standards for individual components and/or interfaces**
  - Implementers can use parts of the architecture separately
  - Individual standards all support vendor extensions

# The TNC Architecture Overview



Access Requestor

Policy Enforcement Point

Policy Decision Point

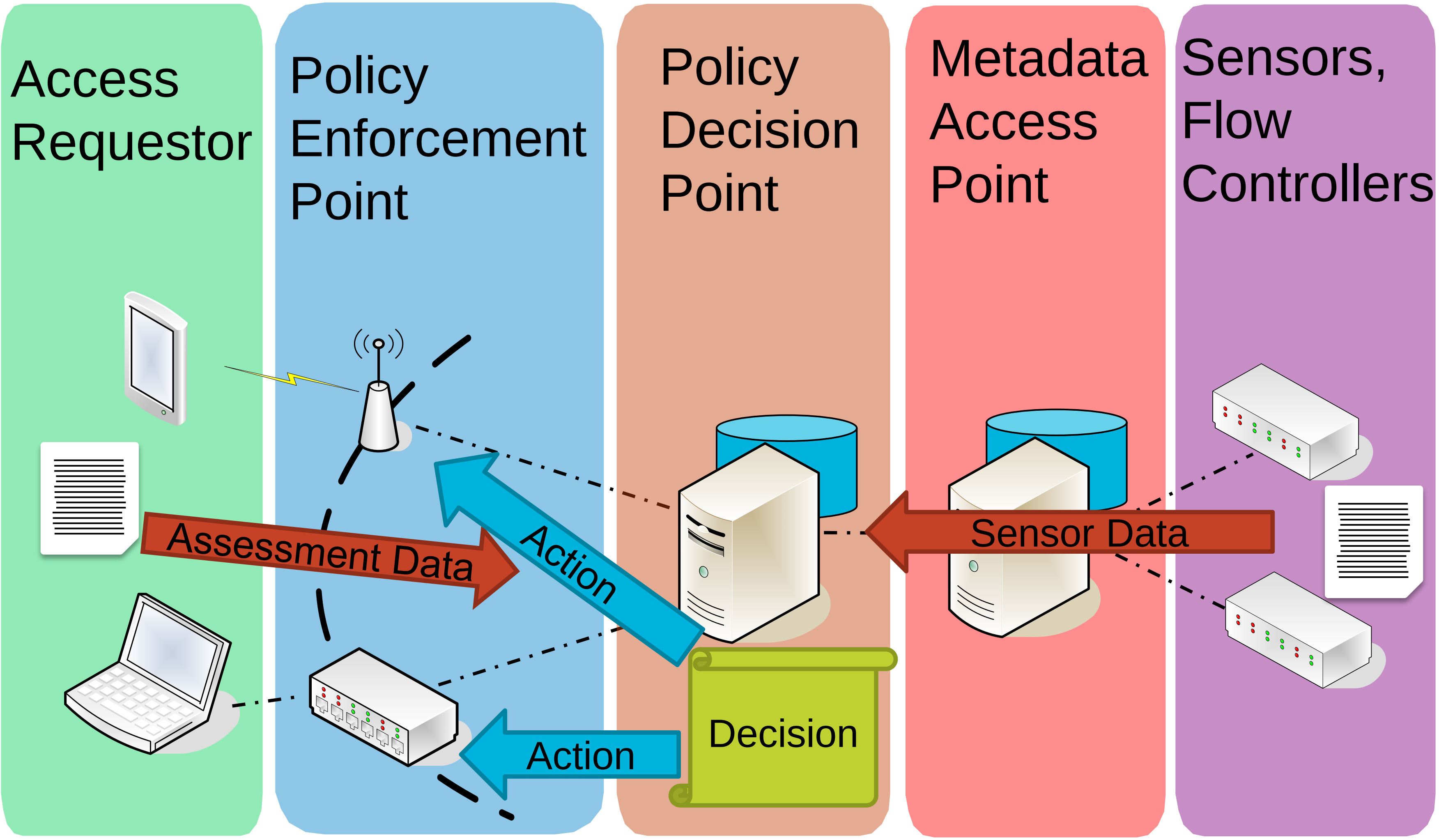
Metadata Access Point

Sensors, Flow Controllers

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Approved for Public Release; Distribution Unlimited. Case Number 15-3479

# TNC for Access Control



Access Requestor

Policy Enforcement Point

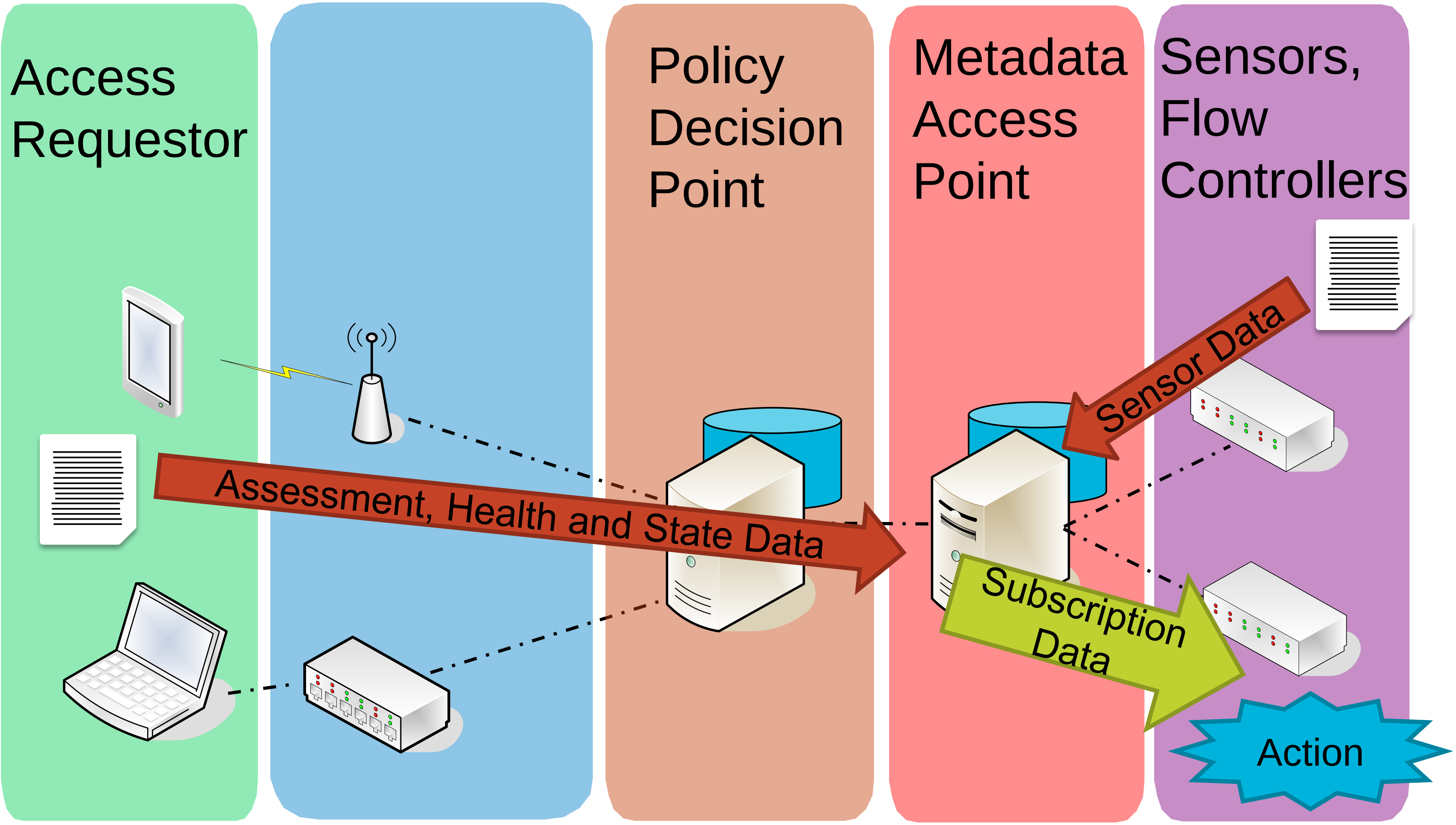
Policy Decision Point

Metadata Access Point

Sensors, Flow Controllers

Approved for Public Release; Distribution Unlimited. Case Number 15-3479

# TNC for Data Orchestration

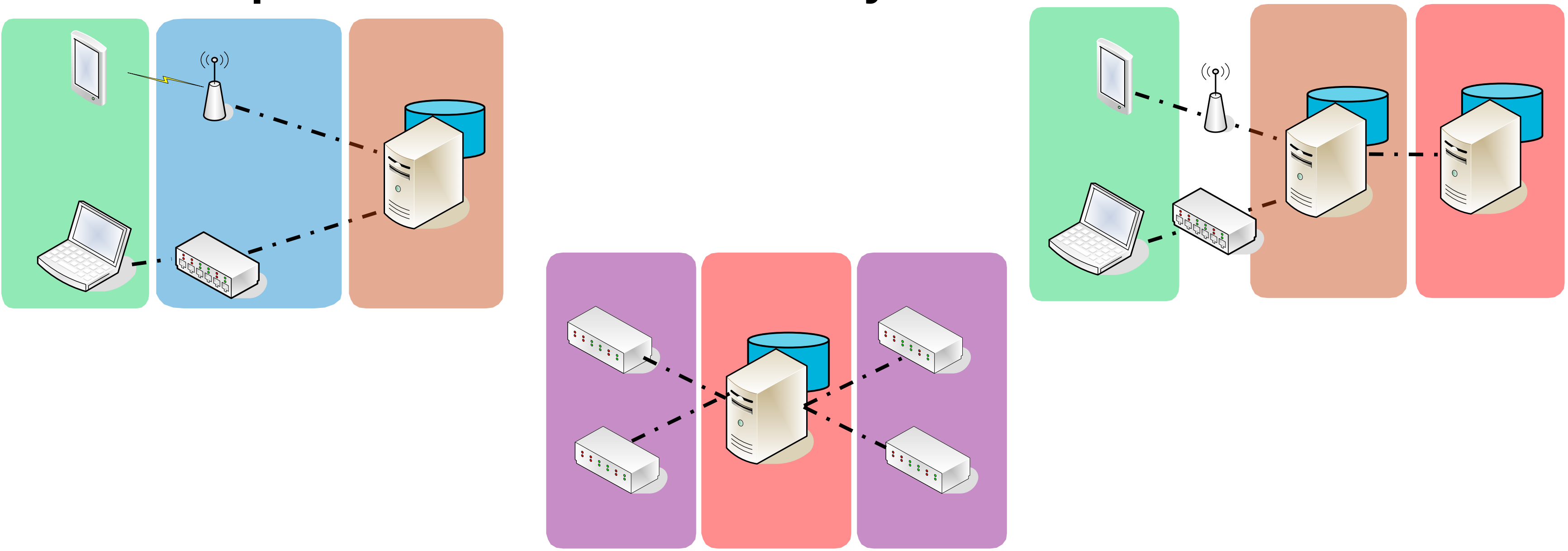


Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Approved for Public Release; Distribution Unlimited. Case Number 15-3479

# TNC for Local Enterprise Needs

- **One framework for any type of information**
  - Create a collection capability; create an evaluation capability
  - TNC securely moves collected data to where it can be used
  - Easy to drop in new collection/evaluation components
    - Because of standardized interfaces
- **Use the portion of the architecture you need**



Approved for Public Release; Distribution Unlimited. Case Number 15-3479

# TNC Adoption

- **TCG claims over a half-dozen companies implementing products that use TNC**
  - That’s good, but not great
- **Reasons and responses**
  - TCG is not the biggest name in standards
    - TNC has been cloned in the IETF where it is called Network Endpoint Assessment (NEA) - RFCs 5792, 5793, 6876, and 7171
  - Perception of a limited scope: “a comply to connect solution”
    - TNC undergoing a major push to expand both perception and reality of its scope
  - Architectures are not as attractive to vendors as more narrowly scoped standards – architectures are bigger investments/risk
    - Revising architecture to emphasize modularity – reduce investment/risk
  - Built with traditional networks in mind
    - Reaching out to TCG cloud/mobile/network device/etc. teams

# Food for Thought

- **Structured data about endpoint/network/software/etc. state is important**
  - TNC defines a few such formats
  - Equally important is getting that information to where it can inform decisions that lead to actions
- **TNC gets this information to Policy Decision Points**
  - Decisions can control network/application access
  - Can be used to assign endpoint/user attributes for Attribute Based Access Control
- **TNC gets this information to the Metadata Access Point**
  - Controlled exposure to a vast array of client devices/applications
- **TNC does this in a modular, extensible way**
  - Define your own data types, set your own evaluation criteria – TNC can get this information where it needs to be

**Approved for Public Release; Distribution Unlimited. Case Number 15-3479**

# TNC as a Solution Enabler

- **Vendors**
  - Consider support of TNC interfaces
  - Allow collected data to be shared with other tools via TNC
  - Enhance your tool value to consumers by bridging information islands
- **Customers**
  - Use TNC-enabled products to create a more complete security solution
  - Drop in new products/custom tools into your security architecture

- **TCG hopes that you will consider the use of TNC as a way to create a more holistic, connected, and automated enterprise security capability**

# References

- **Trusted Network Communications information**

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

- **Trusted Network Communications Architecture for Interoperability (currently undergoing revision)**

**http://www.trustedcomputinggroup.org/resources/tnc_architecture_for_interoperability_specification**

- **IETF Network Endpoint Assessment**

**https://datatracker.ietf.org/wg/nea/documents/**

# Questions?