RSAConference2016

Singapore | 20-22 July | Marina Bay Sands

Connect to Protect

SESSION ID: CMI1-F04

Identify, Contain, and Prevent Threats in Smart Cities and Smart Grids

David M Dufour

Head of Security Architecture
Webroot, Inc.

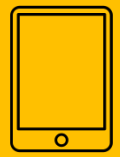
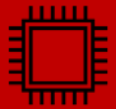
Chairman, Security Landscapes,
IoT Security Foundation

@davidmdufour

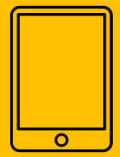
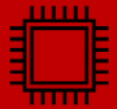
#RSAC

Cybersecurity: Current State

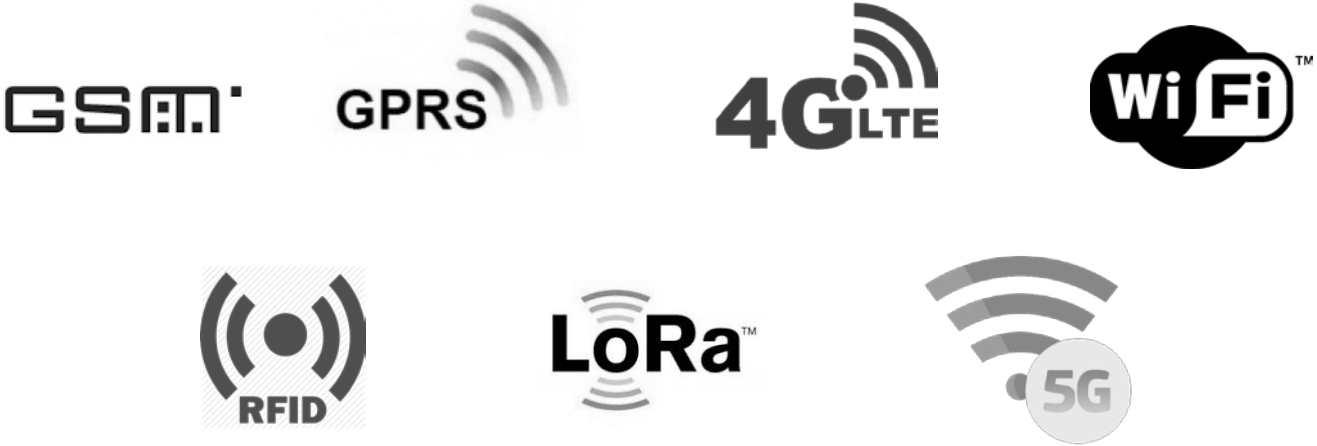
Device Categories

High Resource	Resource Constrained	Static
		
• Endpoint capable • Updatable • Common OS	• Minimal endpoint capability • Updatable w/ limits	• Not endpoint capable • Not updatable • Closed command set

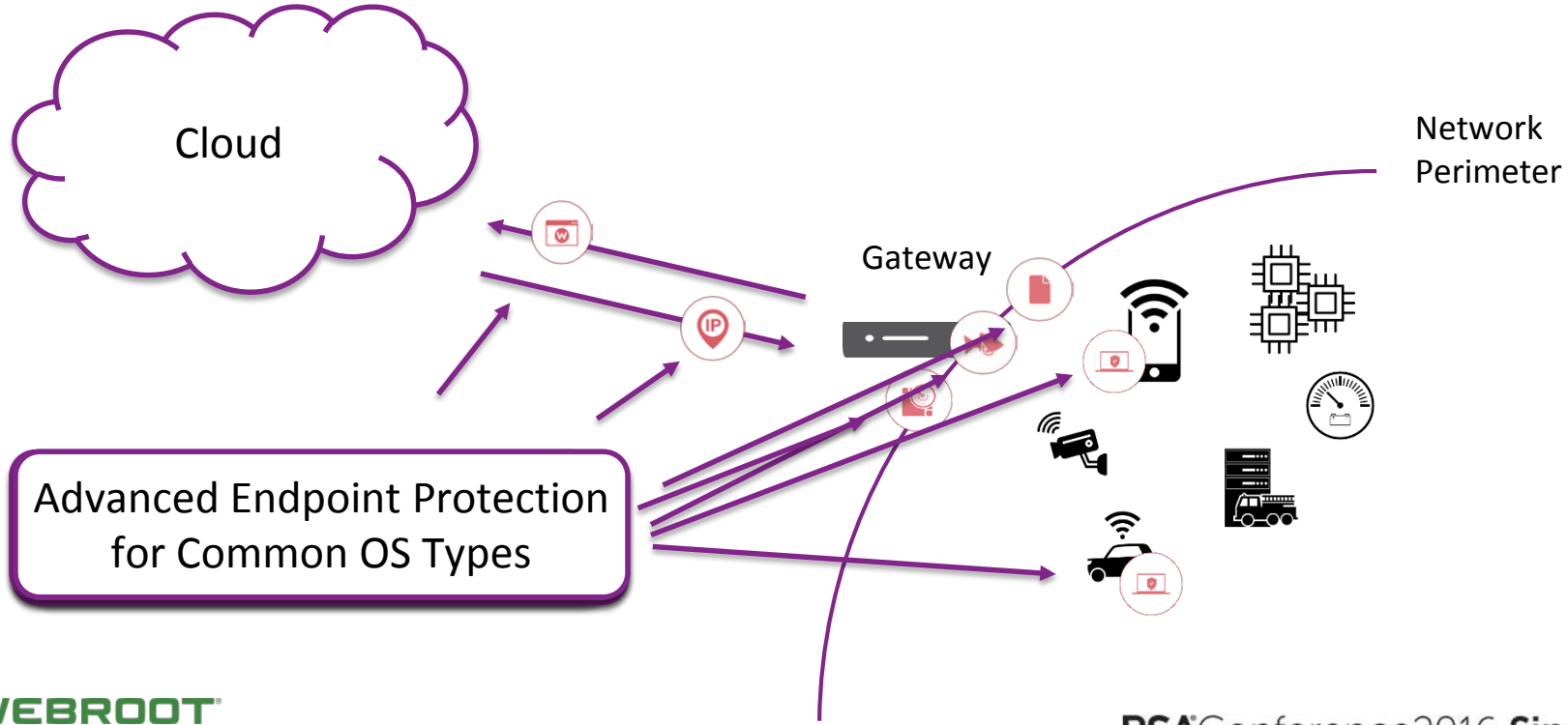
Device Categories: Security

High Resource	Resource Constrained	Static
		
• Identify & remediate • Behavioral modeling • Logging & rollback	• Auditing • Chain of trust	• Possible chain of trust • No auditing

Network: Types



Network: Security



Cybersecurity: Future State

Future State: The Problem

Static endpoint and network security cannot keep up with the threat landscape

Endpoint solutions cannot protect transient devices

Endpoint solutions cannot run on resource constrained devices

Future State: The Problem

Move security focus off the endpoint into the network

Use device ID to develop solutions that create dynamic sensors in the network and on resource capable endpoints

Develop ecosystem machine models to protect the unique aspects of each network

Future State: Device Identification

Manufacturers submit devices

Devices are analyzed for:
Unique performance features
Unique hardware configurations

Fingerprint is used for device detection and device specific machine modeling

Analysis is stored as a unique device type fingerprint

Future State: Machine Modeling

Devices are identified and analyzed

Machine model is created for defined standard performance parameters

Machine model is created for anomaly detection

Machine model is tuned for given ecosystem

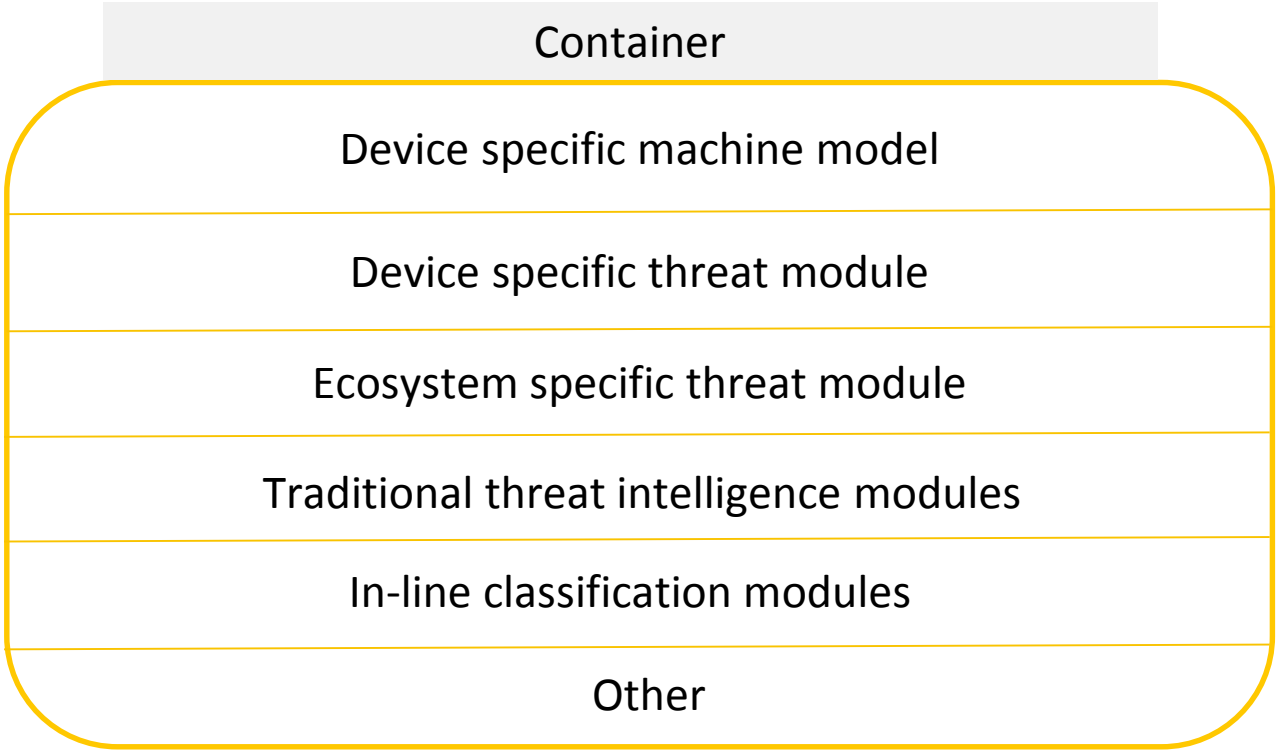
Dynamic Sensors: Structure

Container
(OS or network specific)

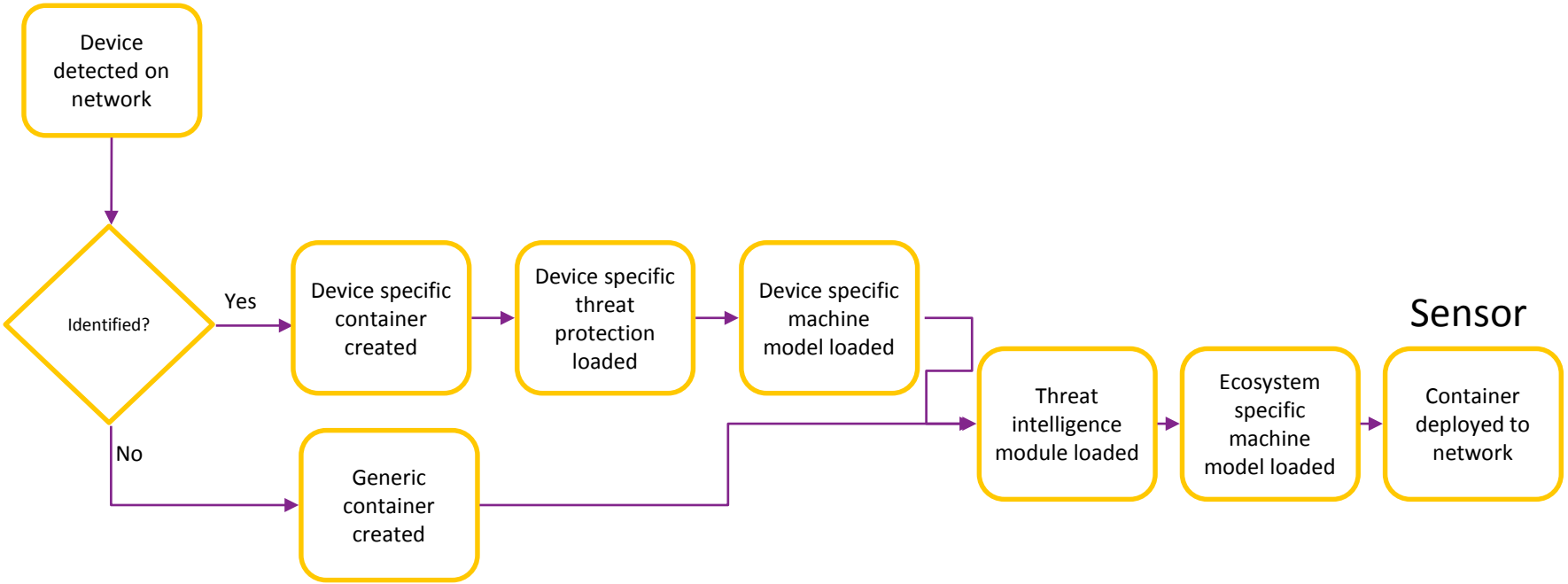
Security
modules

Environment / device unique
machine models

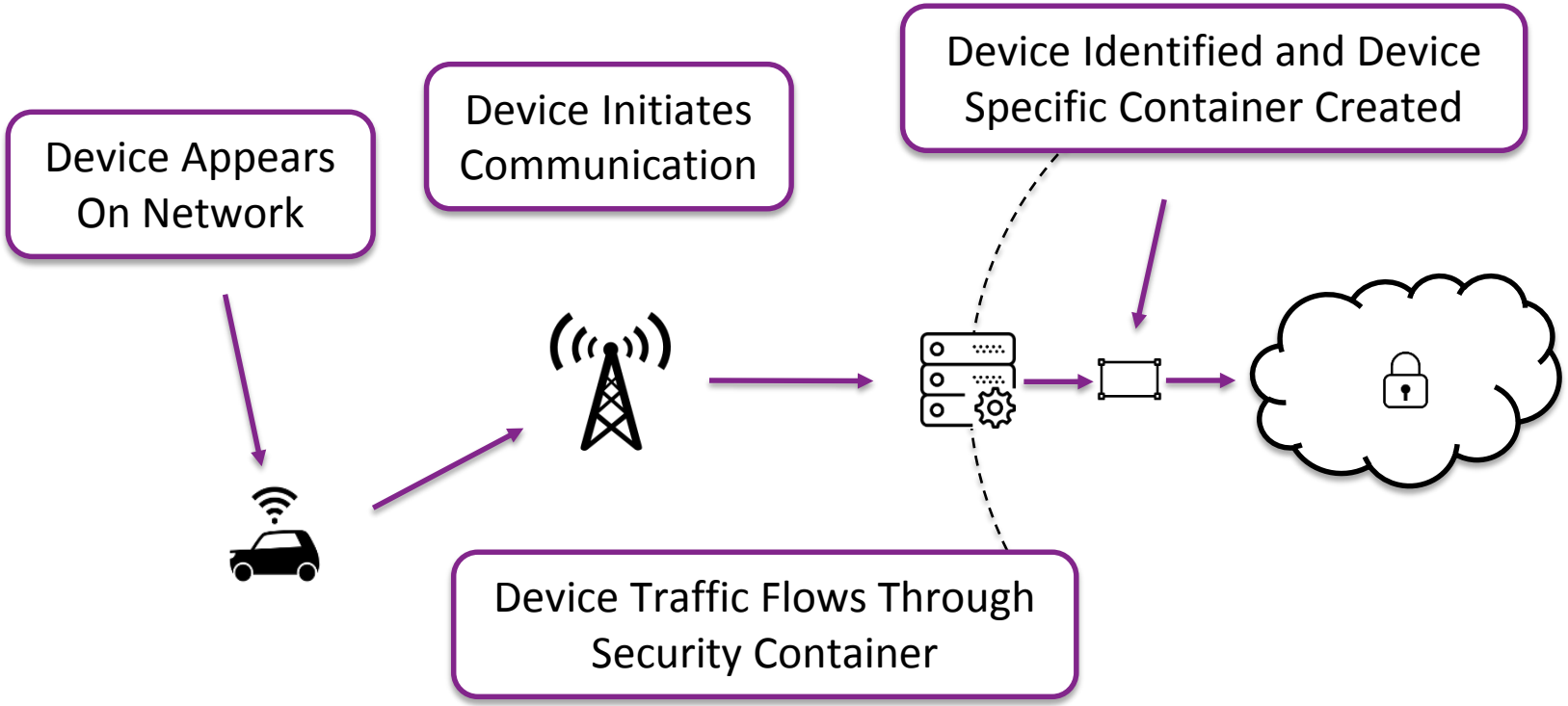
Sensor Detail



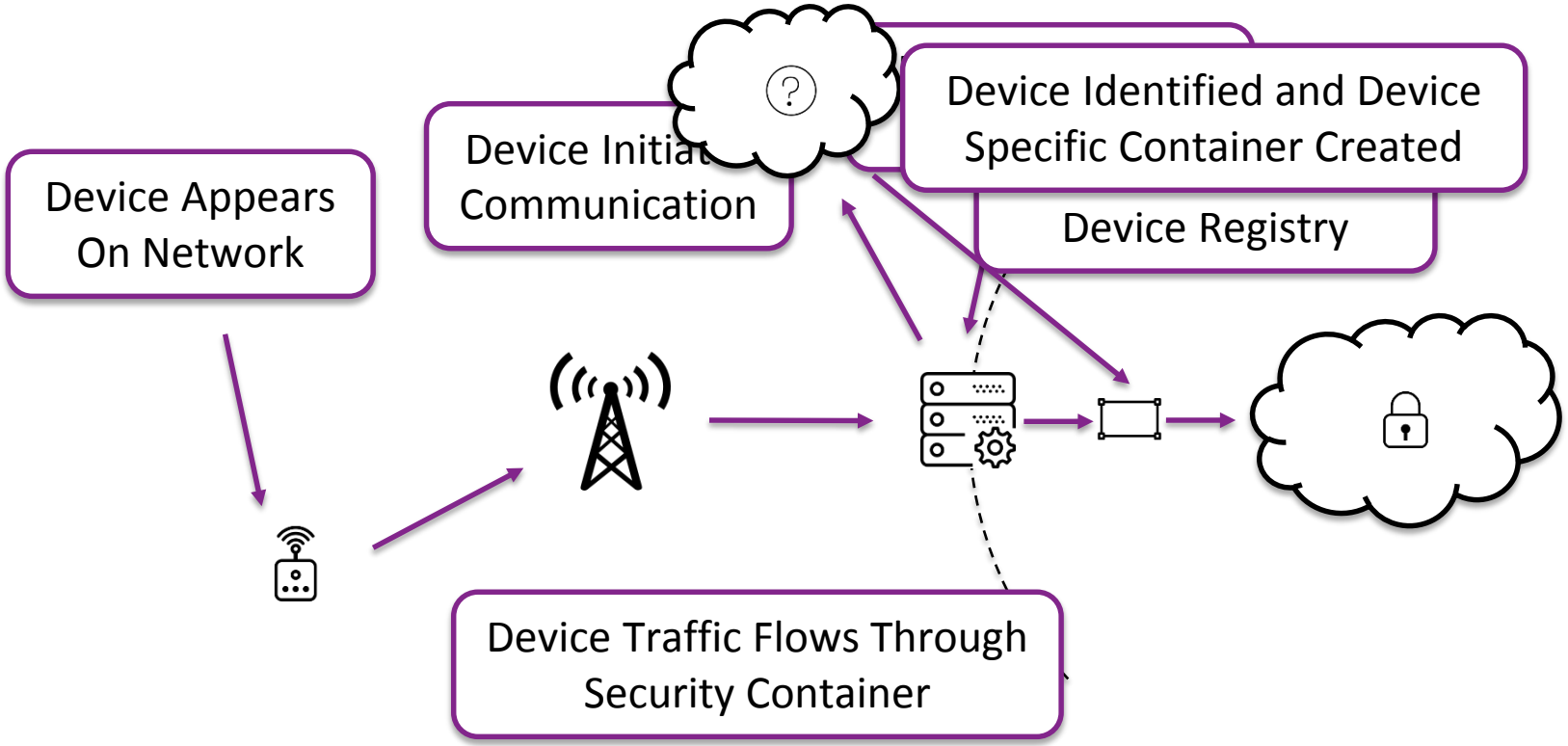
Typical Flow



Known Device



Unknown Device



Application

Now What? Apply It!

Implement traditional cybersecurity solutions into smart meter and smart city ecosystems, including:

- Implement traditional threat intelligence solutions
- Endpoint solutions, where available
- SIEM and other monitoring systems

Identify promising new technologies and partner with organizations building these solutions, such as:

- Network anomaly detection
- Dynamic agent generation
- Closed system machine modeling

Questions?

David M. Dufour
@davidmdufour