RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: MBS-TS09

Achieving Operational Security Excellence in Connected IoT Solutions

Michele D. Guel

Distinguished Engineer, IoT Security Strategist
Cisco Systems
@MicheleDGuel

RSA®Conference2019

By 2020, an estimated 30 billion "things" will be connected.

What’s Your Viewpoint Today?

Consumer/Personal Market

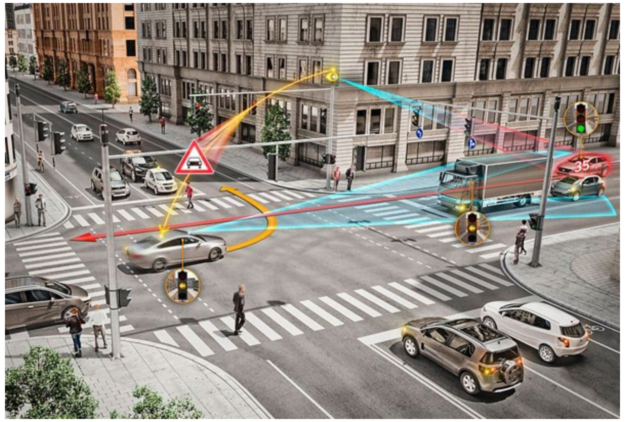
- Smart home owner?
- Autonomous vehicle owner?
- IoT Wearable Enthusiast?
- Connect health patient?
- Connected commuter?

Industry

- Smart City Manager?
- Building Planner?
- Shipping company?
- Department of transportation?
- Healthcare professional

The Internet of Things impacts us all, even if we don’t think it does…

Maturing Industry IoT Vertical Solutions



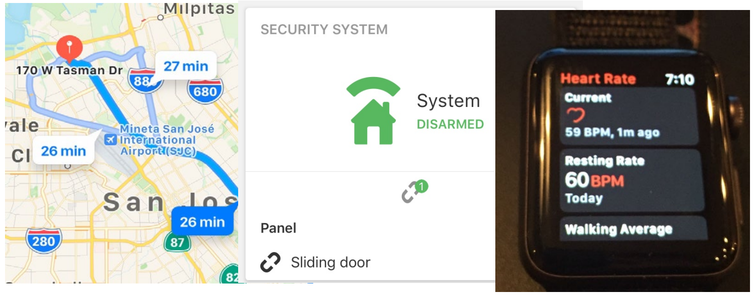
Connected Transportation

Smart Cities & Communities

Connected Healthcare

Connected Retail

Connected Manufacturing

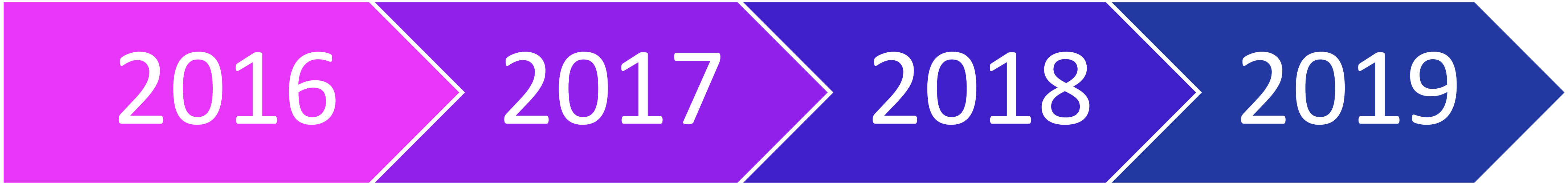


Consumer IoT

RSA®Conference2019

Attacks & Threat Actors

Biggest IoT Attacks



2016

- Mirai
- Hajime
- Nyadrop

2017

- Hajime
- IoT Reaper
- BrikerBot

2018

- VPN Filter
- Hide-n-Seek
- Mirai Okiru

2019

- Adversarial AI
- Fake Apps
- Modular IoT Malware

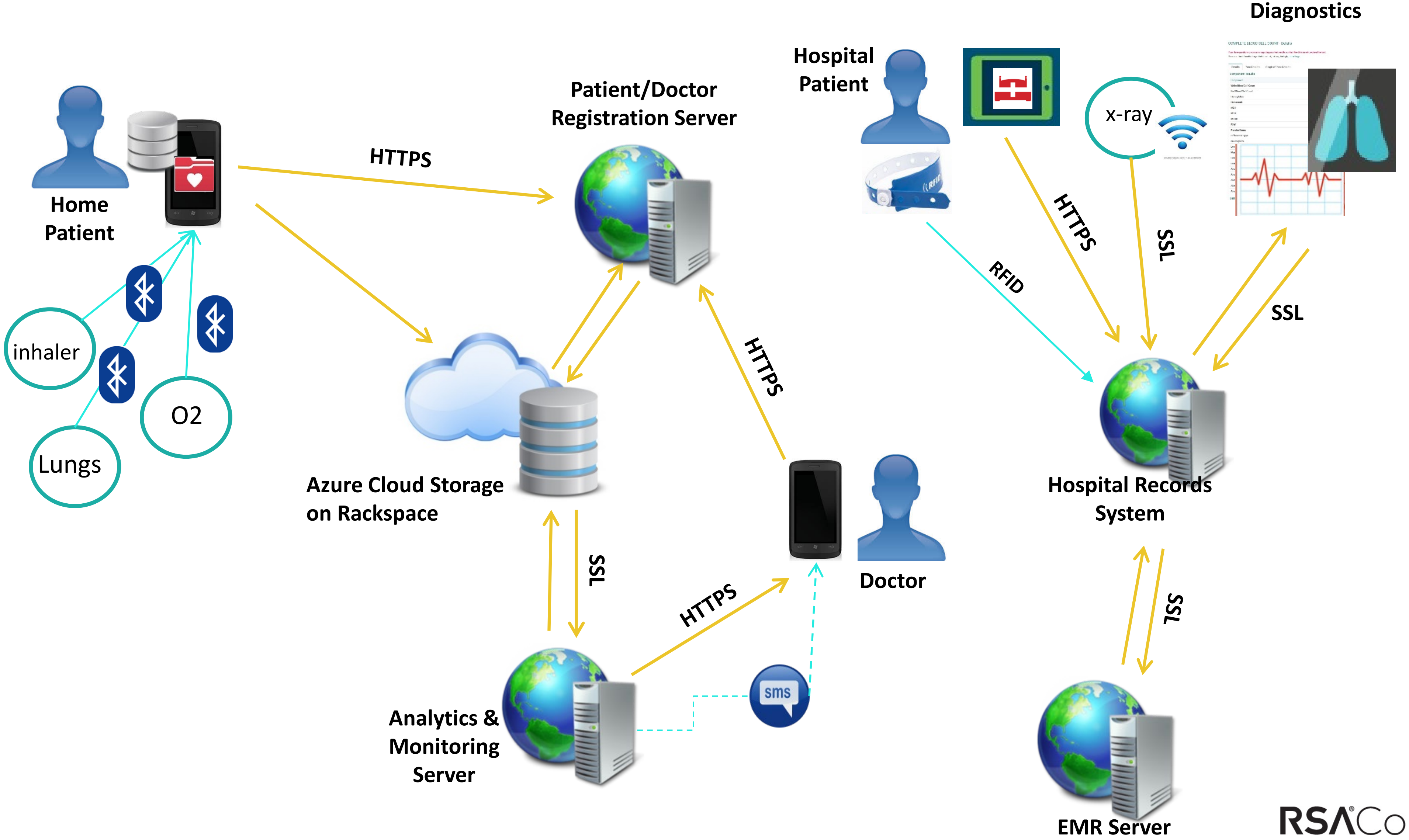
Common and Repeated Attacks

- Known default credentials
- Denial of Service
- Web/Cloud service vulnerabilities
- Trojaned firmware
- Physical tampering
- Pivot

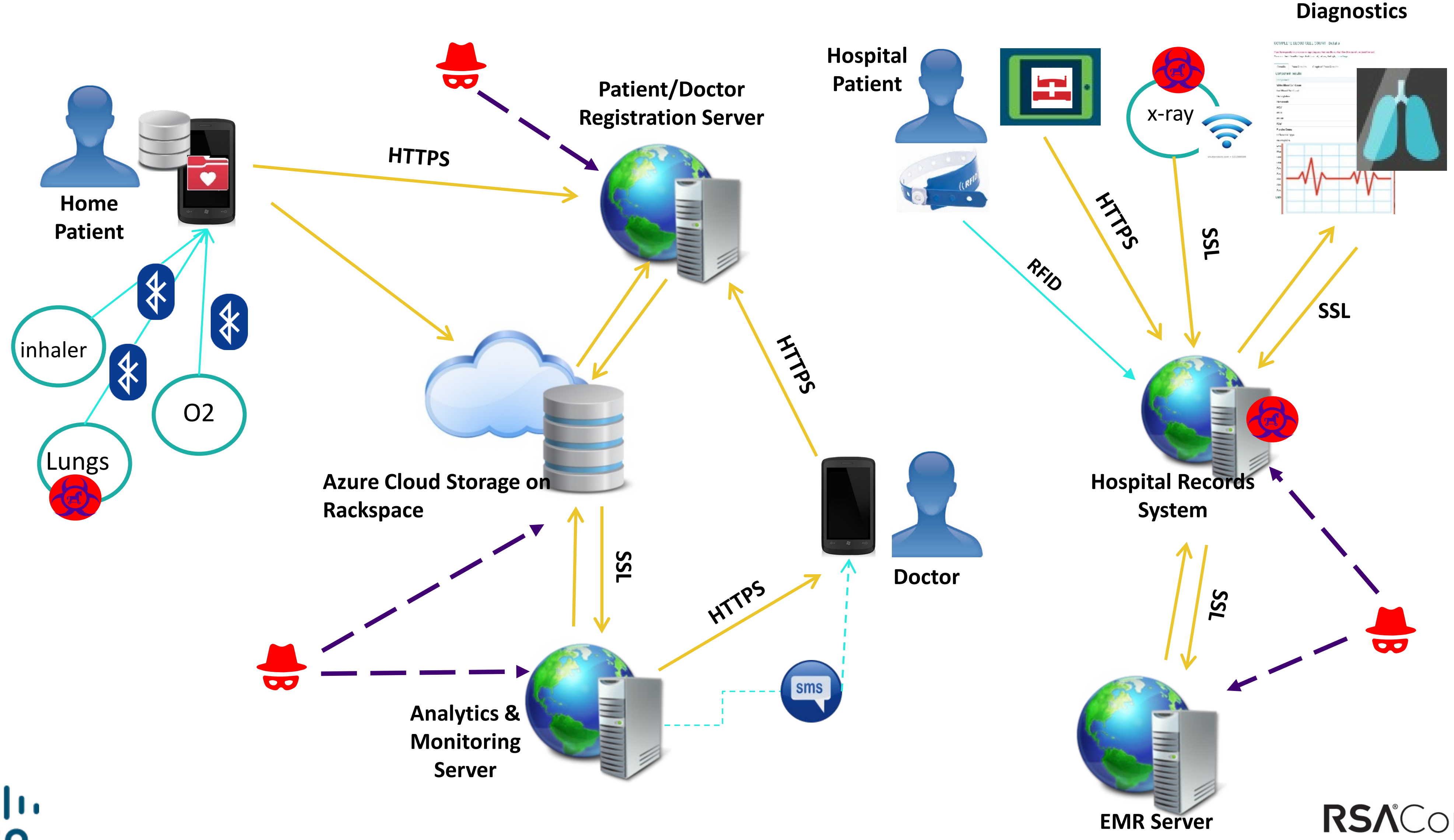
Why are the threat actors gaining ground?

- More IoT devices
  - larger attack surface
  - always connected, always on
- Variations on a theme
- Vendors continue to use old and vulnerable versions of O/S
- Consumers are still buying
- IT organizations are ill equipped to manage lots of “things”

Architecture Complexity Poses Challenges



Architecture Complexity Poses Challenges



Intersection of IT & OT – Fusion or Parallel Universe?

IT Network		OT Network
Protecting Intellectual Property and Company Assets	Focus	24/7 Operations, High OEE, Safety, and Ease of Use
Confidentiality, Integrity, Availability	Priority	Availability, Integrity, Confidentiality
Converged Network of Data, Voice and Video (Hierarchical)	Types of Data Traffic	Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical)
Strict Network Authentication and Access Policies	Access Control	Strict Physical Access and Simple Network Device Access
Continues to Operate	Implications of Device Failure	Could Stop Processes, Impact Markets, Physical Harm
Shut Down Access to Detected Threat and Remediate	Threat Protection	Potentially Keep Operating with a Detected Threat
ASAP, during uptime	Upgrades & Patch Management	Scheduled, during downtime

RSAConference2019

Promising Practices

Waiting for the “best” to emerge…

Two Paths for IoT Solutions

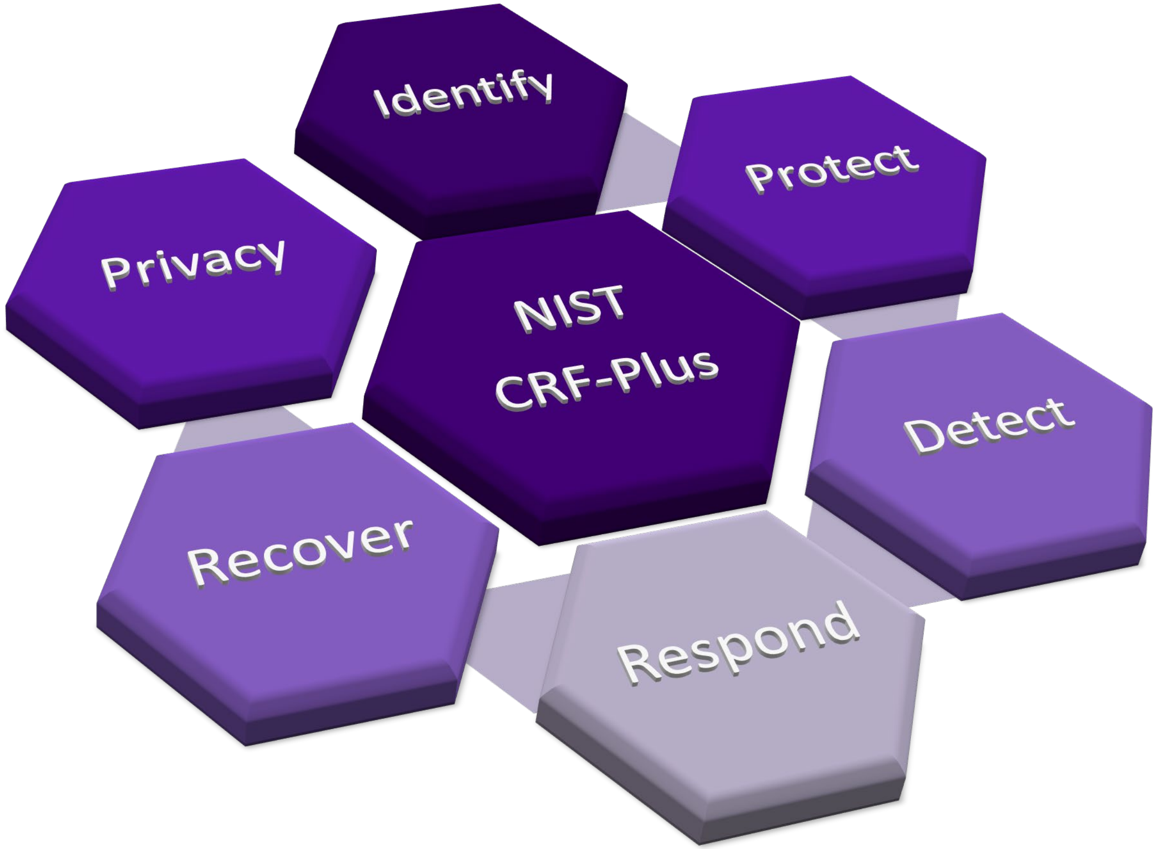
Brown Field

- Legacy Infrastructure
- Incremental changes
- Understand risks
- Outline long term architecture
- Migrate when possible

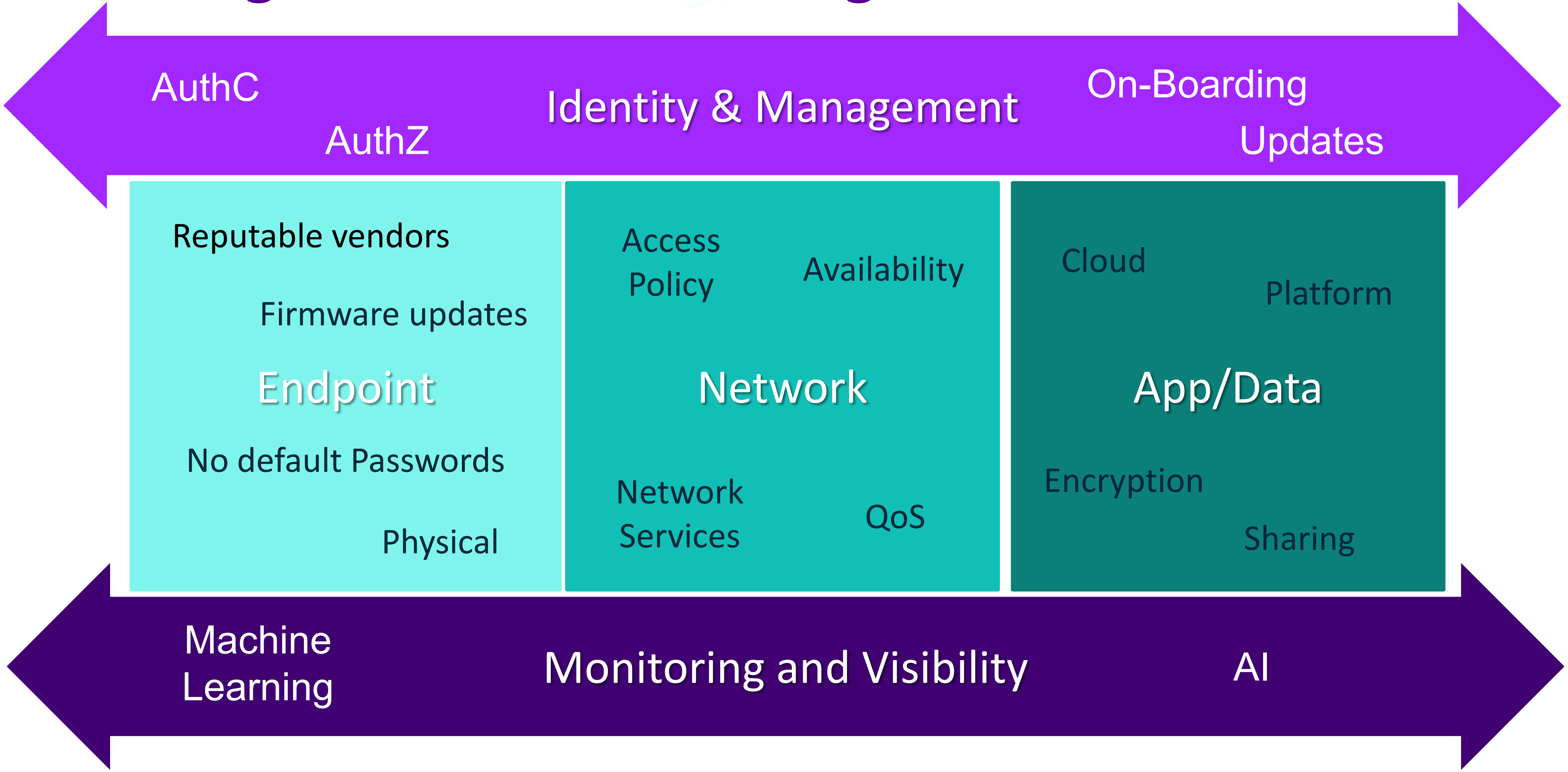
Green Field

- New technologies
  - Open protocols
  - Distributed workflows
  - Fog Computing
  - Machine learning
- Industry Mindshare Forums
- Transformational IoT

What Defines Operational Security Excellence?



Promising Practices for Securing IoT



Identity & Management

AuthC

AuthZ

On-Boarding

Updates

Endpoint

Reputable vendors

Firmware updates

No default Passwords

Physical

Network

Access Policy

Availability

Network Services

QoS

App/Data

Cloud

Platform

Encryption

Sharing

Monitoring and Visibility

Machine Learning

AI

Download full worksheet

How Business Leaders can Shape Their IoT Solution Strategy

- What is the expected business benefit of your IoT solution?
- Which verticals does your IoT solution involve?
- Does the IoT solution involve collection, use or processing of PII?
- Have the specific technologies been implemented before?
- What is the potential impact if all or parts of the IoT solution were attacked?
- What is the acceptable amount of financial loss due to system or data breach?
- Are there known security risks with the IoT solution chosen?
- What is the expected timeline for the entire program?
- What % of the total program has committed funding?
- Have you identified a designated owner(s) of the solution?

Download full worksheet

How IT Leaders Can Shape Their IoT Solution Strategy

- What type of data will be collected, used or processed?
- What is the current state of IoT management in your infrastructure?
- What is the expected scale of the solution in terms of endpoints?
- Do the vendor products meet the Critical IoT requirements?
- What government regulations may apply?

- What is the vendor viability and product maturity?
- What is the complexity of solution architecture?
- What is the experience level with the implementation team?
- Does the solution involve any safety requirements or regulations?
- Is the current IT infrastructure capable of supporting the IoT solution?

Download full worksheet

Apply What You Have Learned Today

Within 3 Months

- Within two weeks you should:
  - Identify your personal/home attack surface.
  - Identify your organization’s attack surface.
- Within three months you should:
  - Use included worksheets to plan IoT implementations.
  - Improve your knowledge of IoT space.

Within 9 Months

- Within six months you should:
  - Develop IoT operational security strategy.
  - Keep abreast of IoT threat, attacks and mitigations.
  - Investigate IoT security alliances
- Within nine months you should:
  - Share successful practices back to community.

RSA®Conference2019

THANK YOU

Questions?

RSA®Conference2019

Resource Materials

Web Resources

- Cisco IoT Resources - https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
- Cisco Cybersecurity Report Series - https://www.cisco.com/c/en/us/products/security/security-reports.html
- Take a Leap into the 21 Century of IoT - https://blogs.cisco.com/innovation/take-a-leap-into-the-21st-century-of-iot
- IoT Predictions for 2019 - https://betanews.com/2018/12/21/iot-predictions-2019/
- 2018 Trends in IoT Threats - https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/
- Vigilante IoT Malware - https://resources.infosecinstitute.com/the-vigilante-malware-do-we-need-a-cyber-vigilante/#gref

Web Resources

- Trusted IoT Alliance – https://www.trusted-iot.org/
- Online Trust Alliance IoT Resources - https://otalliance.org/resources/iot-resources
- Internet of Things Consortium - https://iofthings.org/
- IoT Cybersecurity Alliance - https://www.iotca.org/

RSAConference2019

Promising Practices

Identity and Access Management Controls

- All devices must require authentication with strong passwords or multi-factor prior to user or administrative access.
- Endpoint devices must not contain default user/password combinations (e.g. “admin/admin”) that are easily guessed or accessible.
- All devices must be on boarded in a secure manner.
- Principe of least access should be used for all administrative functions.

Baseline Security Requirements for IoT Endpoints

- Secure boot & system integrity
- Hardened and secure system
- Secure communications
- Ensure data privacy
- Network identity

- Secure web interfaces
- Minimize threat surface
- Log critical events
- Minimal security operations
- Secure Firmware/OS updates

Baseline Security Requirements for a Secure IoT Network

- Authenticate devices allowing them to join to network
- Limit network access
- Provide network telemetry
- Provide threat detection and mitigation
- Provide authenticated time distribution (NTP)
- Provide audit capability
- Limit unnecessary services

Application Layer Security Controls

- Strong Cryptographic Support
- Strong Authentication & Authorization
- Ensure Data Privacy
- Ensure Data Separation
- Hosted Services Hardening
- Log Critical Events
- Basic Operational Processes
- Strong Session Management
- Strong Web Security
- Strong Supply Chain Security

Monitoring and Visibility Controls

- Visibility of endpoints in the echo systems
  - Understanding of their baseline expected behavior
  - Identify compromise endpoints
- System Event Logging
  - Read/write endpoint state, update firmware
  - excessive unauthorized access attempts
  - excessive or inappropriate use of the Endpoint
- Declarative and heuristic mechanisms to detect attacks on the infrastructure
- Automated mitigation through policy updates

RSAConference2019

End of Resource Section