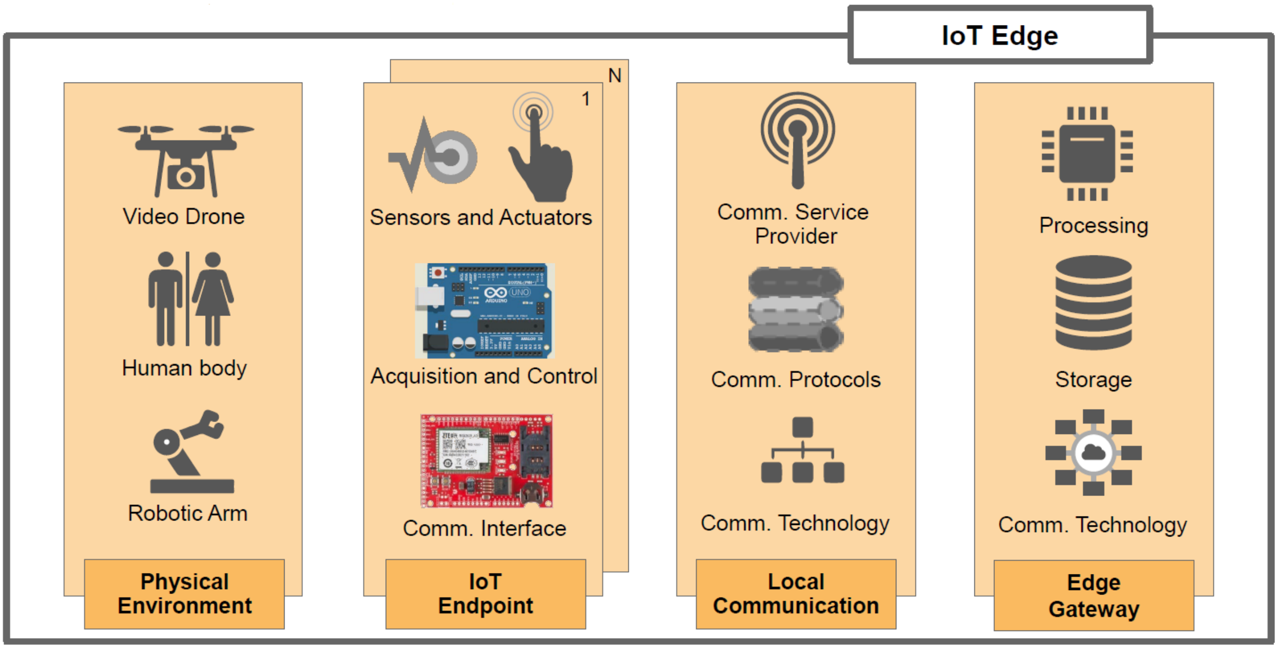
Securing the IoT

Darryl Ng

darryl.ng@nus.edu.sg

Objectives

- Employ IoT implementation patterns to identify security risks and possible matching security controls, accounting for legacy IT, OT and physical system architectures
- Identify and use specific patterns found in IoT projects to assign proper security controls for those IoT patterns
- Create a periodic end-to-end security pattern review process to track updates to IoT implementations to ensure chosen patterns still address risks to overall business objectives of IoT-infused projects

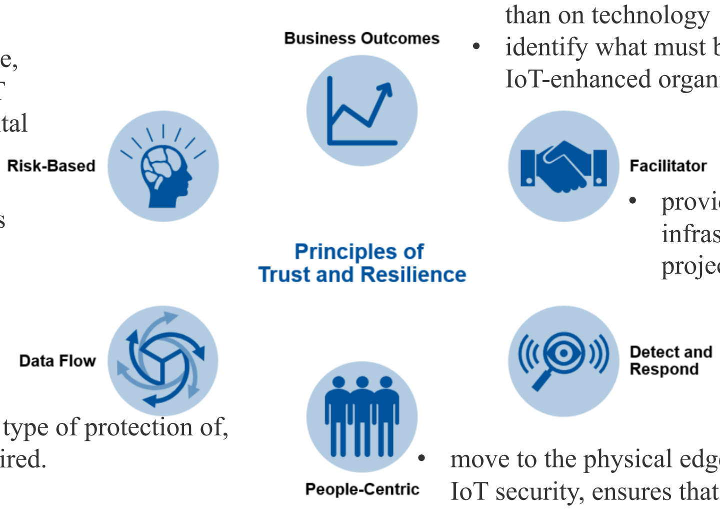


IoT Edge

Physical Environment	IoT Endpoint	Local Communication	Edge Gateway
Video Drone	Sensors and Actuators	Comm. Service Provider	Processing
Human body	Acquisition and Control	Comm. Protocols	Storage
Robotic Arm	Comm. Interface	Comm. Technology	Comm. Technology

Trust and Resilience in Digital Security

- dramatic increase in the scale, diversity and function of IoT devices in the pervasive digital presence
- ensures that a prioritization method for digital security is risk-driven to use available resources in the most cost-effective manner



Source: Gartner (May 2016)

- determine the level and type of protection of, and access to, data required.

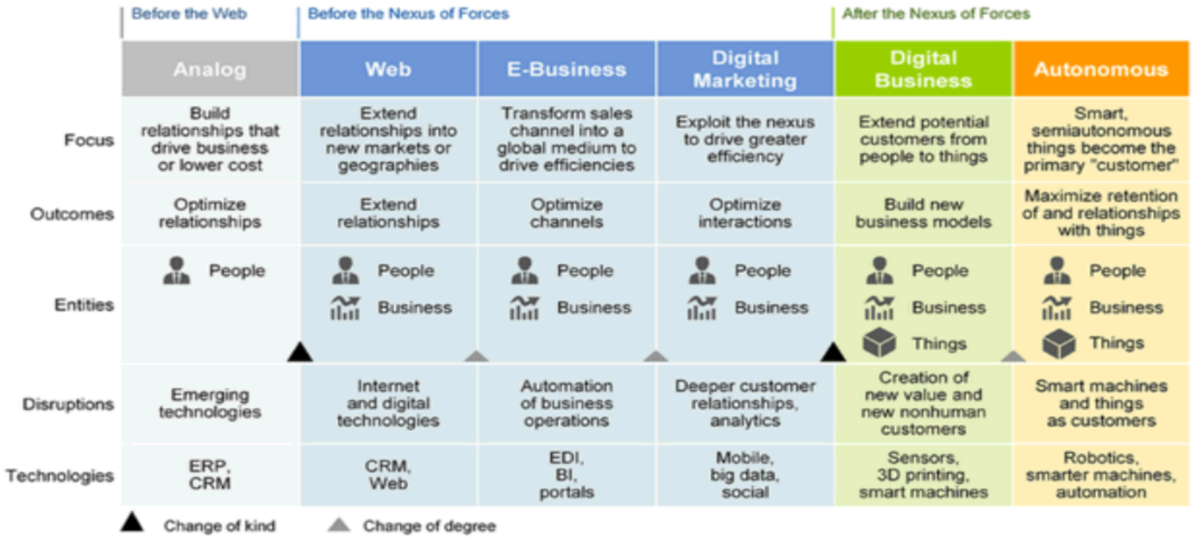
- focus on business outcomes, rather than on technology
- identify what must be secured in an IoT-enhanced organization

- provide long-lasting resilient infrastructure and services for IoT projects

- focus in digital security projects is moving toward detection and response

- move to the physical edge, especially in consumer-based IoT security, ensures that the decisions related to privacy and safety are people-centric.
- ensure that networks and devices are properly configured.

Nexus of Forces



	Before the Web	Before the Nexus of Forces			After the Nexus of Forces	
	Analog	Web	E-Business	Digital Marketing	Digital Business	Autonomous
Focus	Build relationships that drive business or lower cost	Extend relationships into new markets or geographies	Transform sales channel into a global medium to drive efficiencies	Exploit the nexus to drive greater efficiency	Extend potential customers from people to things	Smart, semiautonomous things become the primary "customer"
Outcomes	Optimize relationships	Extend relationships	Optimize channels	Optimize interactions	Build new business models	Maximize retention of and relationships with things
Entities	People	People Business	People Business	People Business	People Business Things	People Business Things
Disruptions	Emerging technologies	Internet and digital technologies	Automation of business operations	Deeper customer relationships, analytics	Creation of new value and new nonhuman customers	Smart machines and things as customers
Technologies	ERP, CRM	CRM, Web	EDI, BI, portals	Mobile, big data, social	Sensors, 3D printing, smart machines	Robotics, smarter machines, automation

▲ Change of kind ▲ Change of degree

Source: Gartner (December 2014)

What it meant for security professionals

Impact	Recommendations
In addition to generating information, the power of an Internet of Things (IoT) object to change the state of environments will need to redefine the scope of their security efforts beyond present responsibilities.	- current principles of IT security in the enterprise — the "information" mold and context of IT are too limiting. - expand technology security planning and architecture to include new (and old) technology and service delivery platforms and patterns.
Most IoT devices and services may be Nexus of Forces-driven. There is a need to deal simultaneously with all past eras of technology to secure the necessary scale and complexity that an IoT world demands.	- evaluate incoming IoT security requirements that account for possible combinations of mainframe, client/server, Web, cloud and mobile security needs, which are impacted by operational technology (OT) and physical security in specific use cases.
IoT security needs will be driven by specific business use cases that are resistant to categorization, increaing the need to prioritize initial implementations of IoT scenarios by tactical risk.	- Do not underestimate/underlook IoT security planning. - Develop initial IoT security projects based on specific, even tactical, business risk profiles, then build on those experiences to develop common security deployment scenarios, core architectural foundations and responsibilities.
The requirements for securing the IoT will be complex, and need to use a blend of approaches from mobile and cloud architectures, combined with industrial control, automation and physical security.	- Leverage current bring your own device (BYOD), mobile, cloud, OT, and physical security governance, management and operations for IoT use cases. - Monitor adoption of key IoT-specific wireless-communication-, hardware-, connected-device- and cloud-based platforms.

Security Key Challenges

- IoT product and service vendors are paying little attention to scenario- or vertical-specific requirements for IoT security
- Common security patterns for vertical-focused IoT deployments do not exist
- Organizations acquired the skills to adjust to extended digital security impacts caused by IoT
- Regulatory and market pressures to address specific vertical needs for IoT security are growing
- Technical standards and frameworks for IoT security are almost nonexistent or beta editions, as is security testing and certification

Develop Methods for Matching Vendor and Service Providers to IoT Security Scenarios and Vertical Requirements

- Embedded security functions within the device
  - e.g., application execution environments, encryption
- Securing cloud-based applications in IoT through expanded uses of cloud access security brokers (CASBs)
- Security implications of expanded wireless network types in existing end-to-end IoT networks
  - e.g., Z-Wave, ZigBee

Likely impact:

- Increases in scale of data amounts and device counts
- Diversity of systems across engineering and information-centric requirements
- Fit-for-purpose functions of devices
- Type of data and data flows generated

Recognize and Use Common Security Patterns to Address IoT Security Needs

Build a security pattern that addresses the IT portion of an end-to-end IoT initiative as a starting point.

- business outcome desired
- device type used and its limitations
- data flow generates and receives for modifications required

Other considerations:

- physically exposed to the public and the
- stay secure for a decade or more
- accessible power, connections and even places to stick things in
- Contractor/vendor back doors

Train for Skill Sets in Digital Security Management and Support In-House

- An information-centric culture that uses IT security
- An engineering culture that uses some IT security
  - asset-intensive industries such as utilities, transportation and manufacturing

Adopt Security Testing and Certification Services for Required or Recommended Certifications

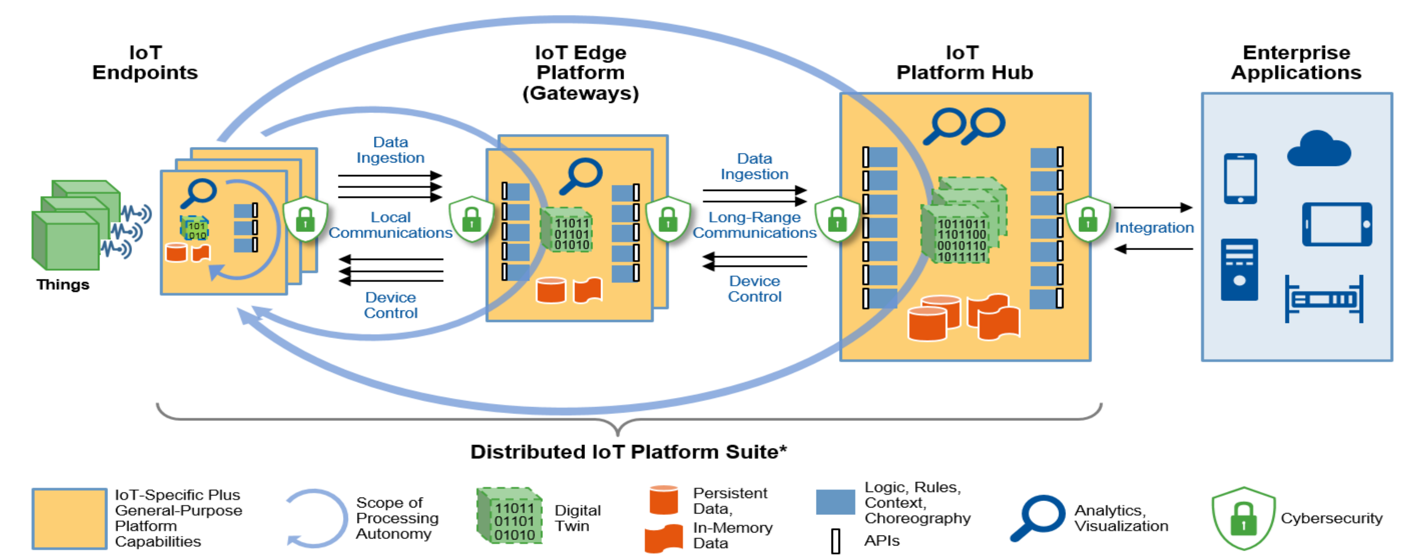
Regulatory concerns regarding the impact of IoT on industrial, commercial and consumer environments

- Address specific vertical needs for IoT security
- Provide some level of standardization for different industries, though this still remains voluntary as of this date

Prepare to Rearchitect as Standards Change, Considering Your Dependence on the Immaturity of Those Standards and Compensating With Existing Standards

- evolving IoT technical standards and protocols
- different IoT industry verticals
- broader vendor ecosystems that drive proprietary security for those environments
- Organizations Defining IoT Standards
  - Industrial Internet Consortium (IIC)
  - Institute for Electrical and Electronics Engineers (IEEE)
  - International Standards Organization/International Electrotechnical Commission (ISO/IEC)
  - Internet Engineering Task Force (IETF)
  - IoT Cybersecurity Alliance
  - IoT Security Foundation
  - Open Web Application Security Project (OWASP)

Reference Model for IoT



* Not all architectural elements — e.g., IoT edge platform, digital twin and visualization — are offered by all vendors. Also, not all architectural elements are always required for a particular IoT project.
For details, see "Use the IoT Platform Reference Model to Plan Your IoT Business Solutions" (G00311536).

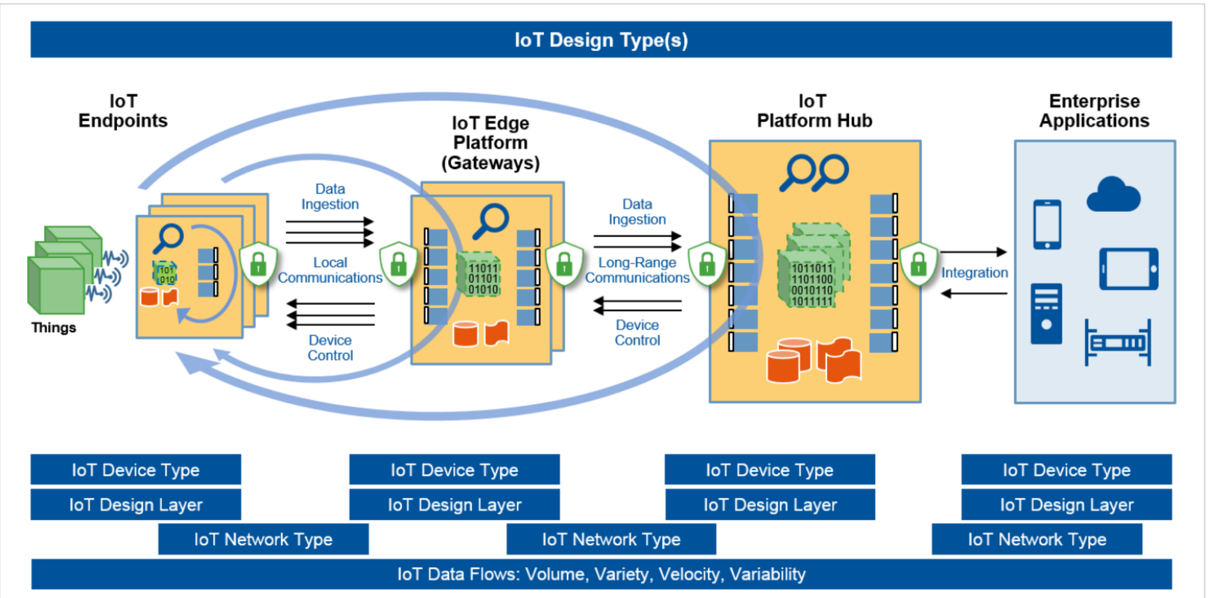
Three key steps in addressing IoT security patterns

1. Identify the essential IoT architectural patterns exhibited by most IoT projects using simple pattern components
2. Identify the matching security characteristics that map to each pattern, creating a matching security pattern
3. Apply risk assessment principles to IoT patterns to determine matching security controls from that assessment

Identify the essential IoT architectural patterns exhibited by most IoT projects using simple pattern components (Step 1)

IoT Design Types	IoT Design Layers	IoT Data Flow Types	IoT Data Flow Designs	IoT Device Types	IoT Network Types
Centralized Distributed Hybrid	Process (Physical) Control (Basic, Site, Operation) Boundary (IoT to OT, IT Gateway) Process (Application, Service)	Sense Only Sense and Act	Edge to Core Distributed Mesh Hybrid	Class 1 – Sensor or Actuator Class 2 – Edge Platform Class 3 – Platform Hub Class 4 – Enterprise Platform	Machine or Internal Area Personal Area Local Area Campus or Plant Area Metropolitan Area Wide Area Hybrid Area (System of Systems)

Component Areas for an IoT Design

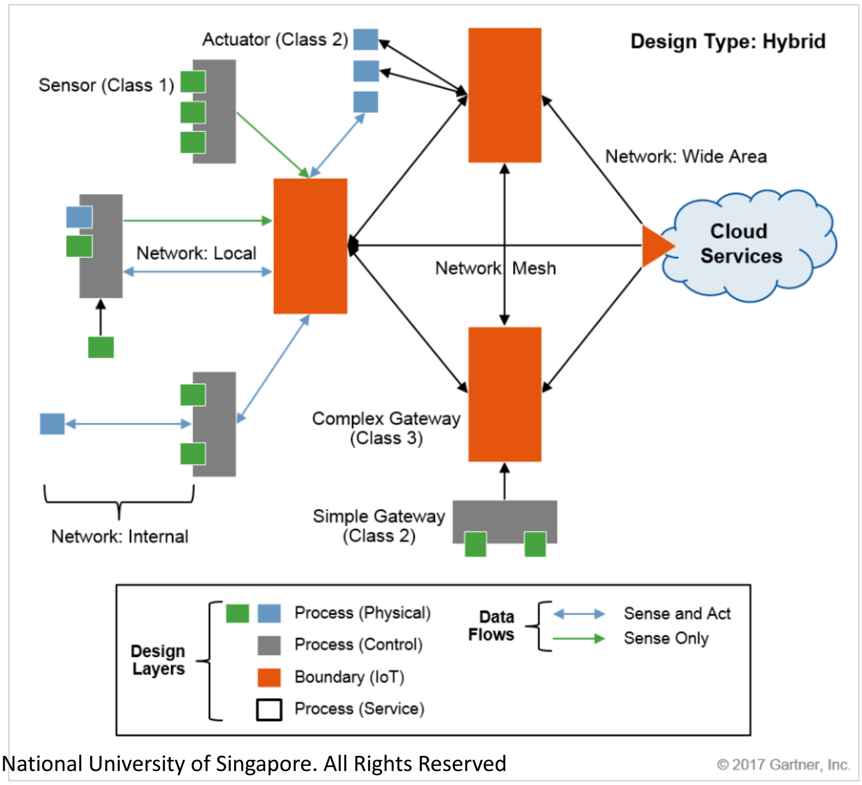


© 2017 Gartner, Inc.

Different Classes/Classifications of IoT Devices

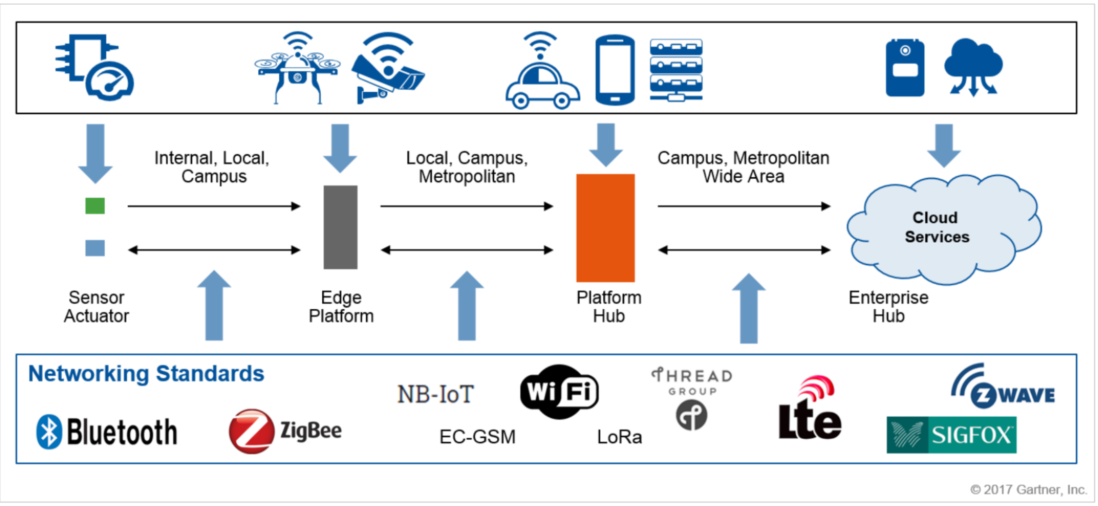
- **Class 1**
  - simple mechanisms such as sensors or actuators that provide the physical control capabilities at the extreme edges of projects.
  - physical and cyber capabilities of IoT are manifested
- **Class 2**
  - simple or complex gateways that aggregate or preprocess information from Class 1 devices and deliver it to other devices, gateways or services
- **Class 3**
  - complex gateways, often in the form of IoT platforms, which perform extensive processing
  - complete IoT applications distributed into the networks for efficiency, performing that process as close to the edge as necessary for the process
- **Class 4**
  - connections to be made to cloud services that may require separated functions from the complex gateway

IoT Hybrid Design Example

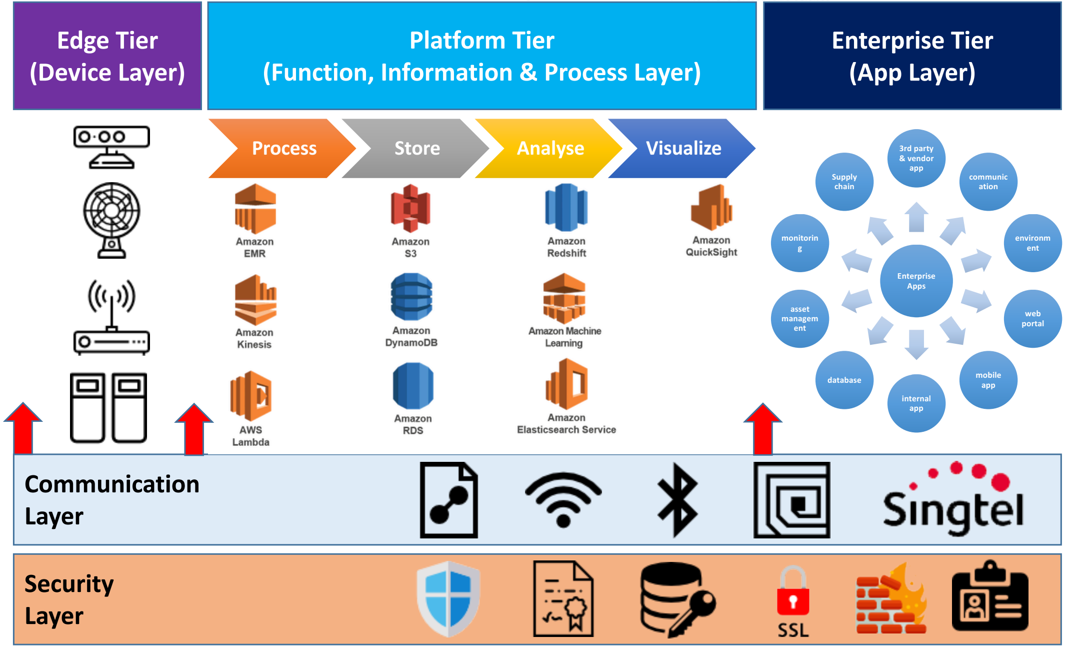


© 2017 Gartner, Inc.

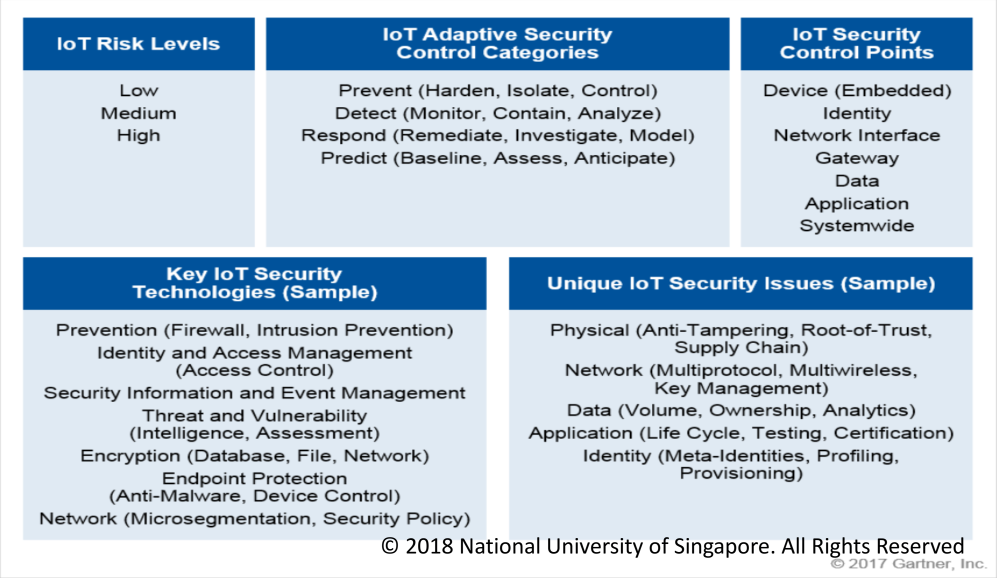
Gartner Reference to Layered Model



Layered Solution Model



Identify the matching security characteristics that map to each pattern, creating a matching security pattern (Step 2)



IoT Risk Levels

Low
Medium
High

IoT Adaptive Security Control Categories

Prevent (Harden, Isolate, Control)
Detect (Monitor, Contain, Analyze)
Respond (Remediate, Investigate, Model)
Predict (Baseline, Assess, Anticipate)

IoT Security Control Points

Device (Embedded)
Identity
Network Interface
Gateway
Data
Application
Systemwide

Key IoT Security Technologies (Sample)

Prevention (Firewall, Intrusion Prevention)
Identity and Access Management (Access Control)
Security Information and Event Management
Threat and Vulnerability (Intelligence, Assessment)
Encryption (Database, File, Network)
Endpoint Protection (Anti-Malware, Device Control)
Network (Microsegmentation, Security Policy)

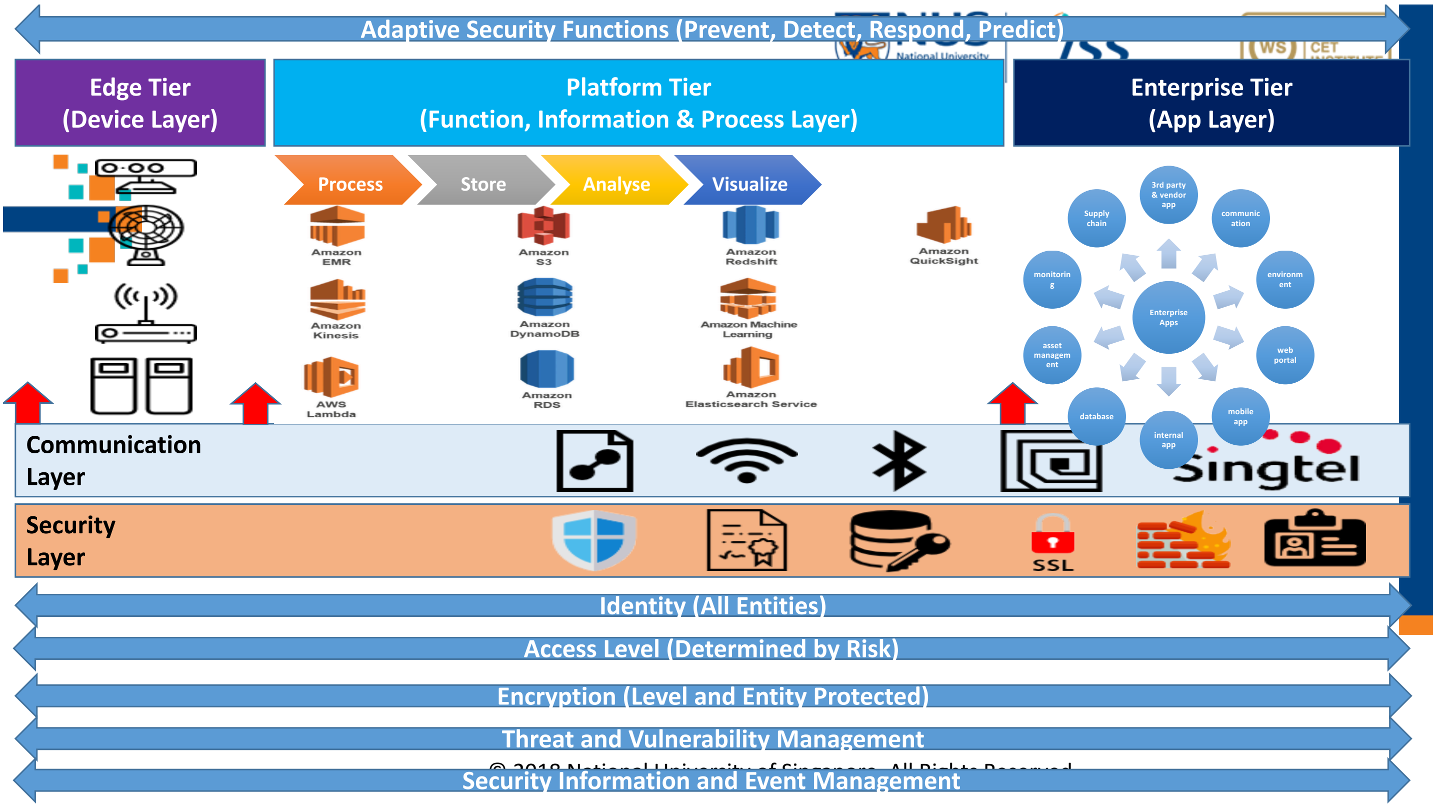
Unique IoT Security Issues (Sample)

Physical (Anti-Tampering, Root-of-Trust, Supply Chain)
Network (Multiprotocol, Multiwireless, Key Management)
Data (Volume, Ownership, Analytics)
Application (Life Cycle, Testing, Certification)
Identity (Meta-Identities, Profiling, Provisioning)

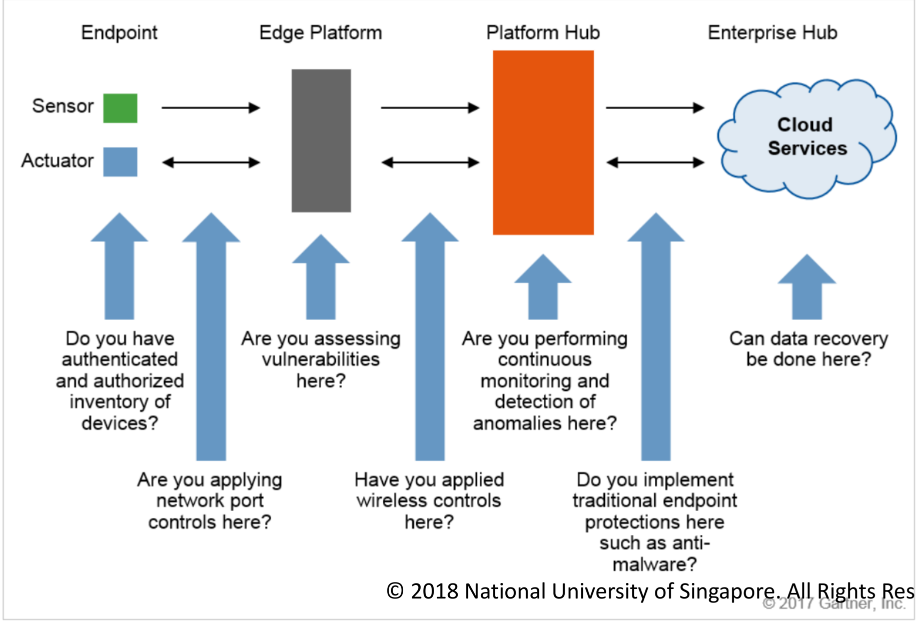
© 2017 Gartner, Inc.

Apply risk assessment principles to IoT patterns to determine matching security controls from that assessment (Step 3)

- Create a Periodic IoT Pattern Review Process to Track Updates to IoT Implementations
  - Using a requirements list to select a combination of design types, design layers, data flow designs and types, device types, and network types to determine the basic pattern of the IoT system
    - Distributed IoT design type
    - Physical, boundary and service process layers
    - Distributed data flow design
    - Sense-only data flow type
    - Class 1, Class 3 and Class 4 device types
    - Use of machine, local-area network and wide-area network types



Security Control Mapping


Endpoint
Edge Platform
Platform Hub
Enterprise Hub
Sensor
Actuator
Cloud Services
Do you have authenticated and authorized inventory of devices?
Are you assessing vulnerabilities here?
Are you performing continuous monitoring and detection of anomalies here?
Can data recovery be done here?
Are you applying network port controls here?
Have you applied wireless controls here?
Do you implement traditional endpoint protections here such as anti-malware?
© 2017 Gartner, Inc.