# Connected Products ioTrust Security Solution

Ranjeet Khanna

*Director, IoT & Embedded Security*

*Entrust Datacard*

**Entrust Datacard**™

# Digital Economy
# and
# Trust Foundation

# IoT Underlying Trends Impact Every Industry

**Digital business** is the creation of new business designs by blurring the digital and physical worlds. ... Digital business promises to usher in an unprecedented convergence of people, business, and things that disrupts existing business models

Objectives

- **Optimize current business model**

- **Transformative growth**

*The **Internet of Things (IoT)** is the network of physical objects that contain embedded technology to communicate and **sense** or **interact** with their internal states or the external environment - Gartner*
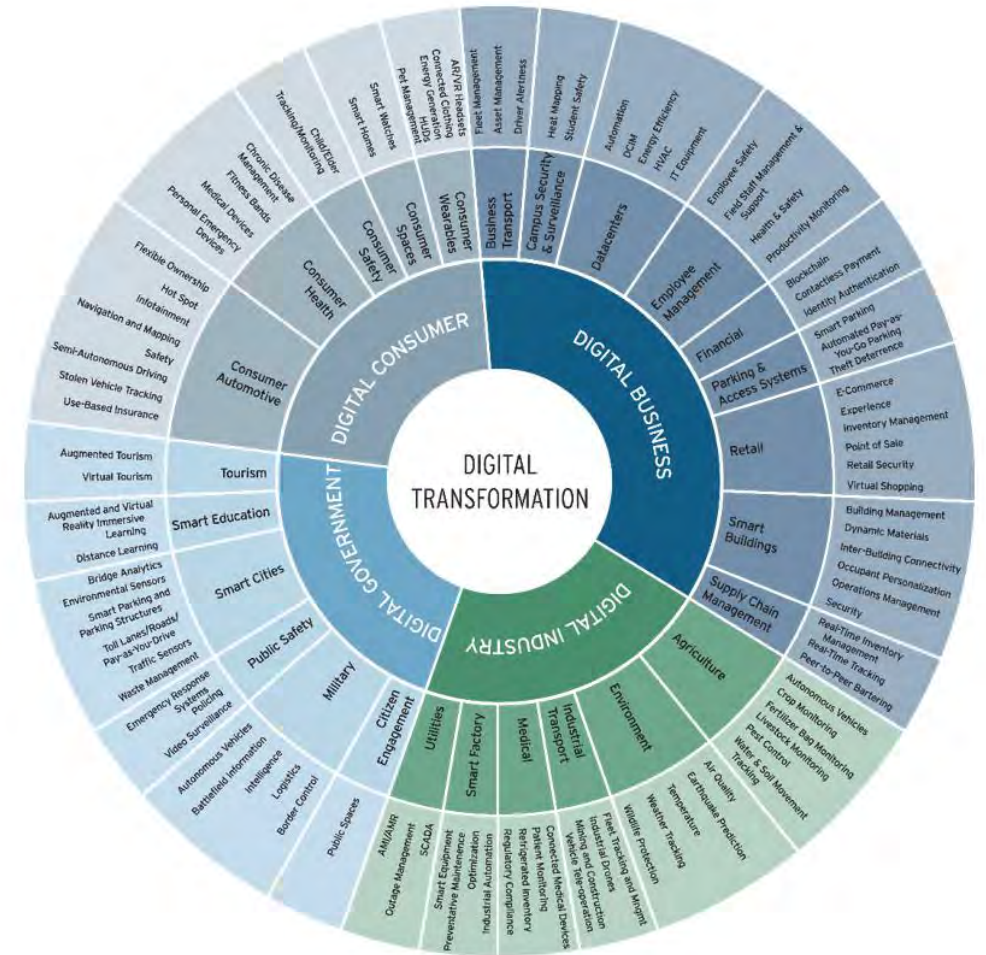


By 2020, IoT technology will be in 95% of electronics for new product designs.

# IoT Unlocks The Growth Opportunities

**26B+**
**Connected Devices**
by 2020

**10x**
**Actionable Data**
by 2020

New Business Models

Diversification of Revenue Streams

Global Visibility

24/7 Real-time information on mission-critical systems

Efficient, Intelligent Operations

## CONVERGENCE OF PHYSICAL AND DIGITAL ASSETS
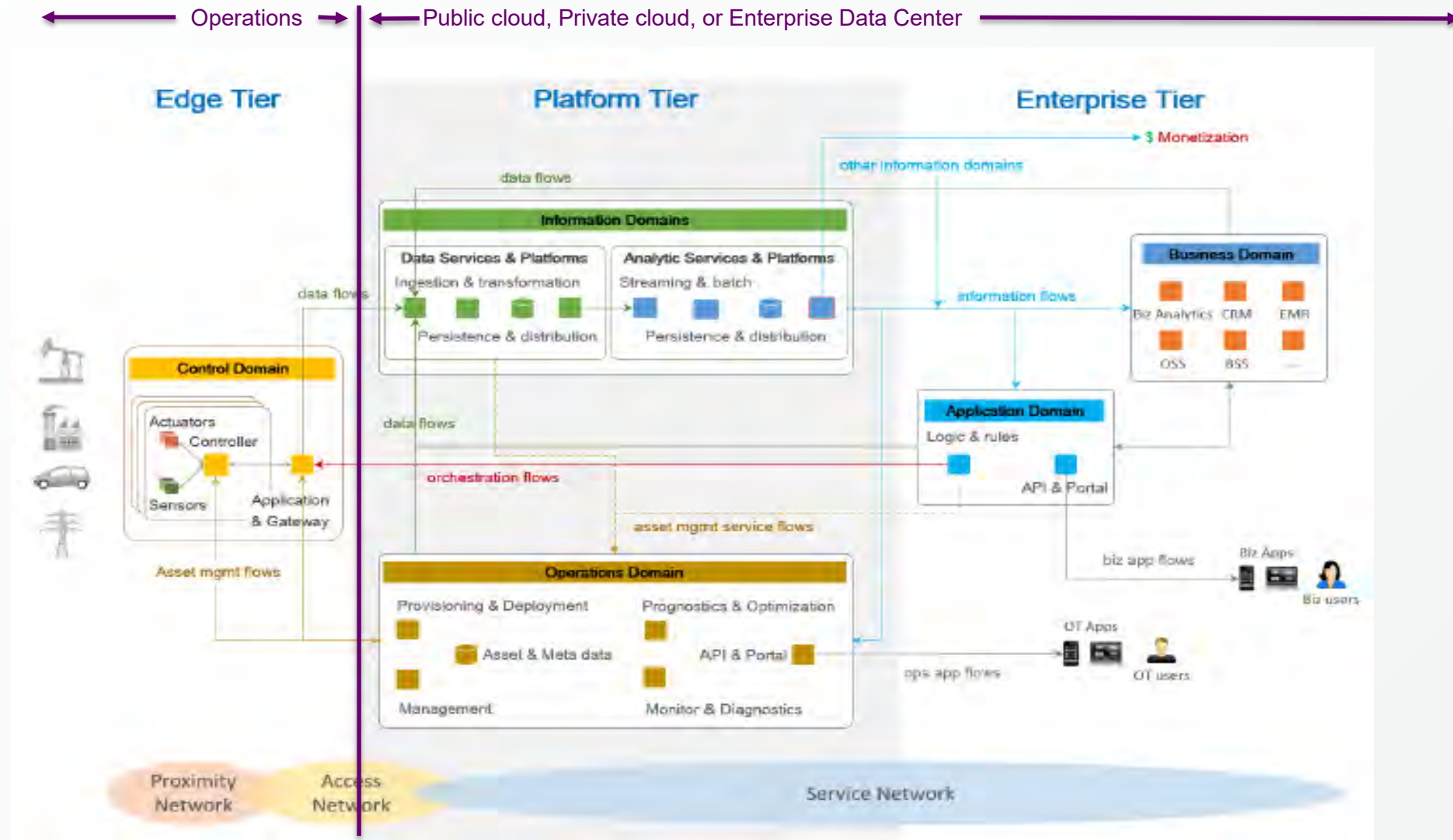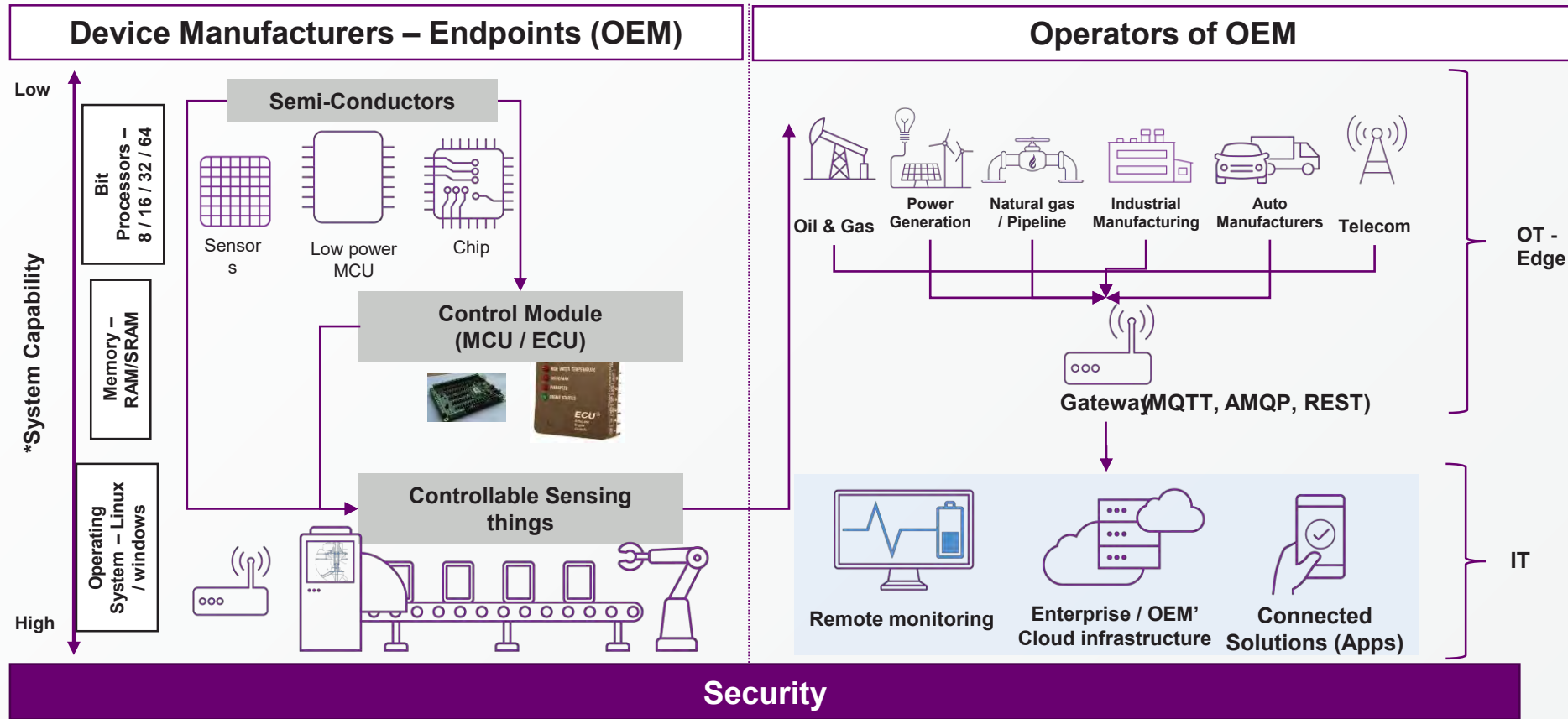
# Digital Enterprise and Connected Ecosystem



CONNECTED
**USERS**

CONNECTED
**SYSTEMS**

CONNECTED
**THINGS**

# IoT Platform: IIC Reference Architecture



Platforms (can be multiple) can be bought or built

# Key Considerations: Device Lifecycle in IoT



## Device Manufacturers – Endpoints (OEM)

*System Capability

- Low
- High

Bit Processors – 8 / 16 / 32 / 64

Memory – RAM/SRAM

Operating System – Linux / windows

**Semi-Conductors**

Sensors | Low power MCU | Chip

**Control Module (MCU / ECU)**

**Controllable Sensing things**

## Operators of OEM

Oil & Gas | Power Generation | Natural gas / Pipeline | Industrial Manufacturing | Auto Manufacturers | Telecom

OT - Edge

**Gateway (MQTT, AMQP, REST)**

Remote monitoring | Enterprise / OEM' Cloud infrastructure | Connected Solutions (Apps)

IT

## Security

| Identity Set up | Secure Identity | Identity Provisioning | Lifecycle Mgmt. |
|---|---|---|---|
| • Establishing Root-of-Trust<br><br>• Addition of Device attributes & bootstrap certificate / token | • HSM, TPM, E-Sim, SE, TEE<br>• Key Management<br>• Ownership transfer | • Discovery<br>• Device Authentication<br>• Provisioning & Authorization | • Secure Data & Identity<br>• Identity & Security Updates<br>• Activate / Suspend / Terminate<br>• Device Update – Firmware, Cert |

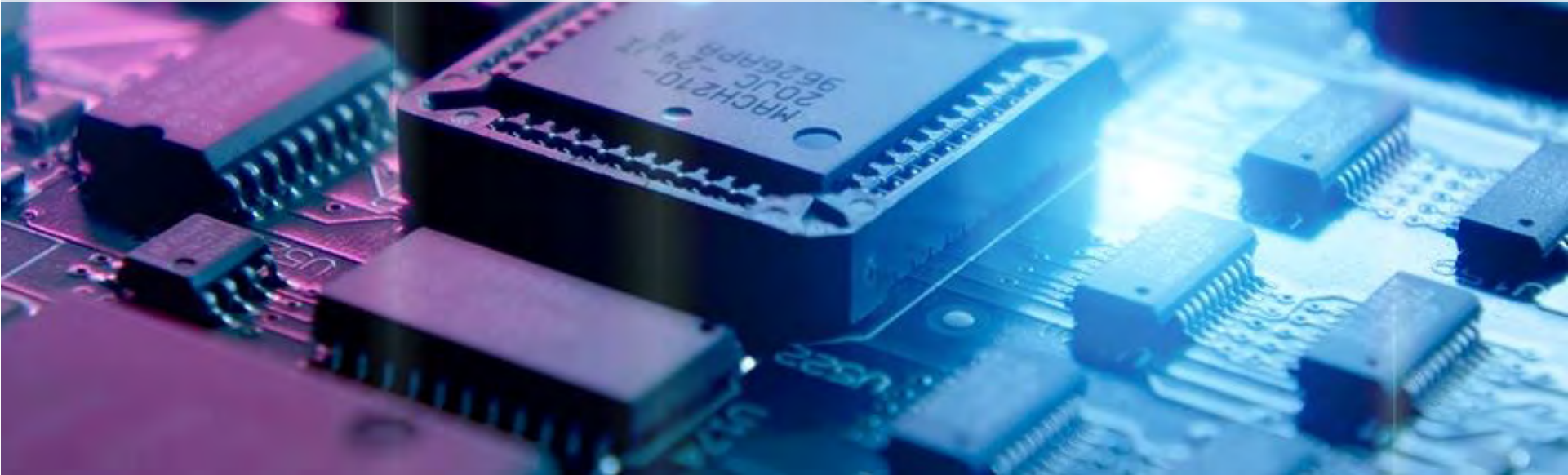# Device Manufacture's Opportunity and Responsibility

# Manufacturing Opportunity

Chip and component manufacturers are in a unique position to enable end-to-end IoT security by securely producing product with root of trust.

**Secured-by-Design**     **Trusted Identity**     **Integrity**

# Manufacturing Challenges

Geographic separation and contract manufacturing

Verification of software authenticity

Secure updates post manufacture

Secure enrollment services post manufacture

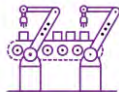Secure storage and generation of private keys

# Leading Use-Cases

TOP USE CASES

## Device Manufacturing

Unique Device Identity

Geo Separation & Contract Mfg.

Firmware Signing

Key Management

## Device Operations

Device Provisioning

Identity Lifecycle Management

Secure Communications

Over the Air Updates

Ownership Transfer

Endpoint Monitoring

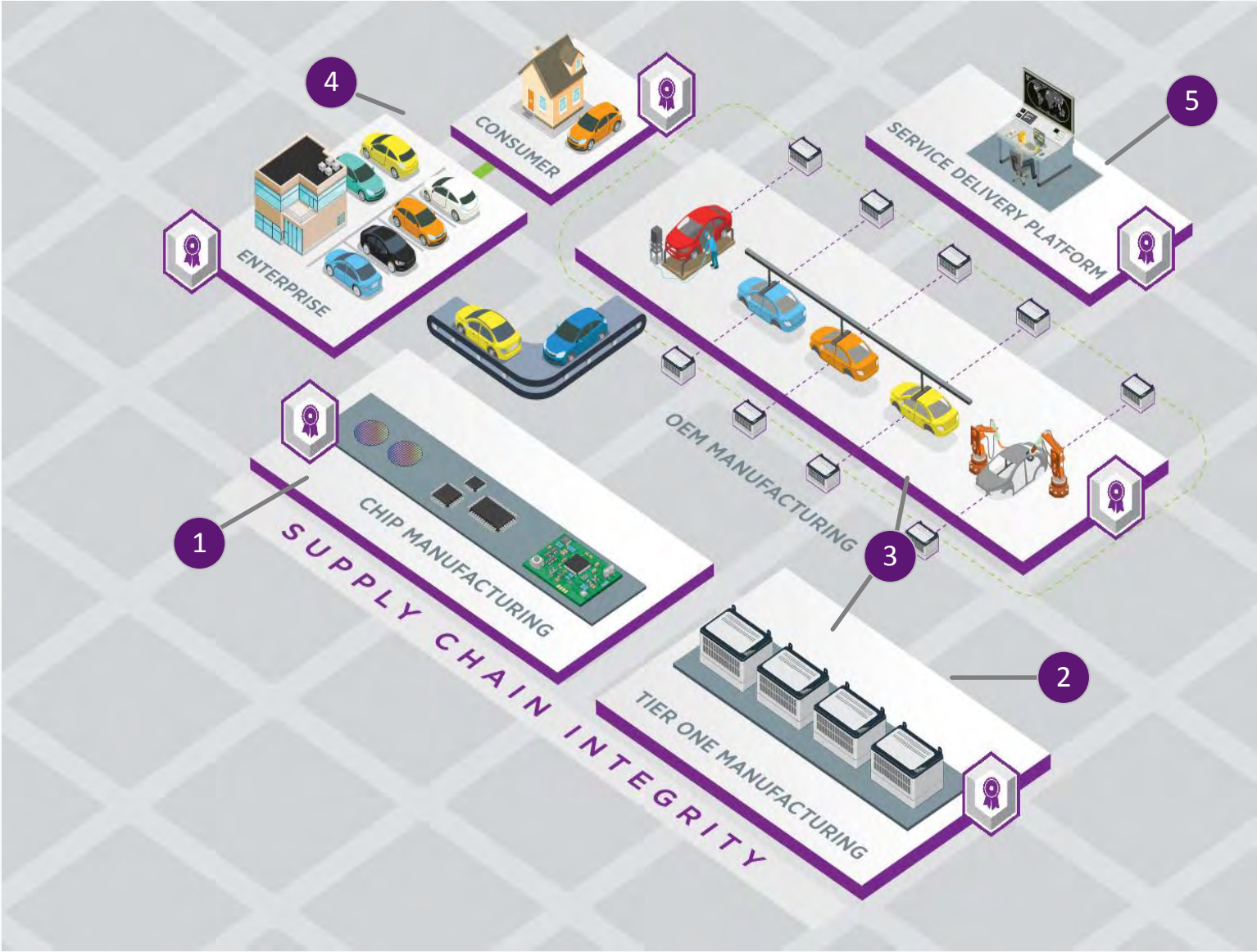# Use-Case: Supply Chain Integrity and Operations

1 – Establish Initial Identifier

2 – Create Managed Identity and Device Role

3 – Device Enrollment and Registration

4 – Establish User and Device Identity Relationship

5 – Secured Service Delivery

# ioTrust Security Solution

# Connected Things

## CONNECTED
## THINGS

Ensure the safety of your business, your customers and our connected world with trusted protection for your devices and apps across every interaction–from sensor to cloud. Defend against hacks, failures, botnets and the threats of tomorrow.

## BUSINESS GOALS

- **New Revenue Streams from Connected Products
Provide customers and internal stakeholders with new offerings built on connected products and real-time data**

- **Optimize Operations
Enhanced visibility over operations and system automation**

## OUR SOLUTIONS

- Supply-Chain Integrity: Make devices easily identifiable and ready to be secured from the earliest stages of manufacturing

- Trusted Infrastructure: Rapidly deployable and scalable security for your operational infrastructure, from endpoint to enterprise data hub, with an added view to the users

- Data Acquisition Management: Granular control of your data as it transits the network

# Trust Enablers

IDENTITY

AUTHENTICATION & AUTHORIZATION

CREDENTIAL LIFECYCLE / KEY MANAGEMENT

EQUIPMENT DATA MODEL MANAGEMENT

DATA SECURITY

SUPPLY CHAIN INTEGRITY

**DELIVERING VALUABLE, ACTIONABLE DATA**

# ioTrust Security Solution

Cloud ready, Application and Data platform agnostic

**ioTrust Value: delivering secured infrastructure between "things" and applications**

Enabling different classes of "things" existing or greenfield



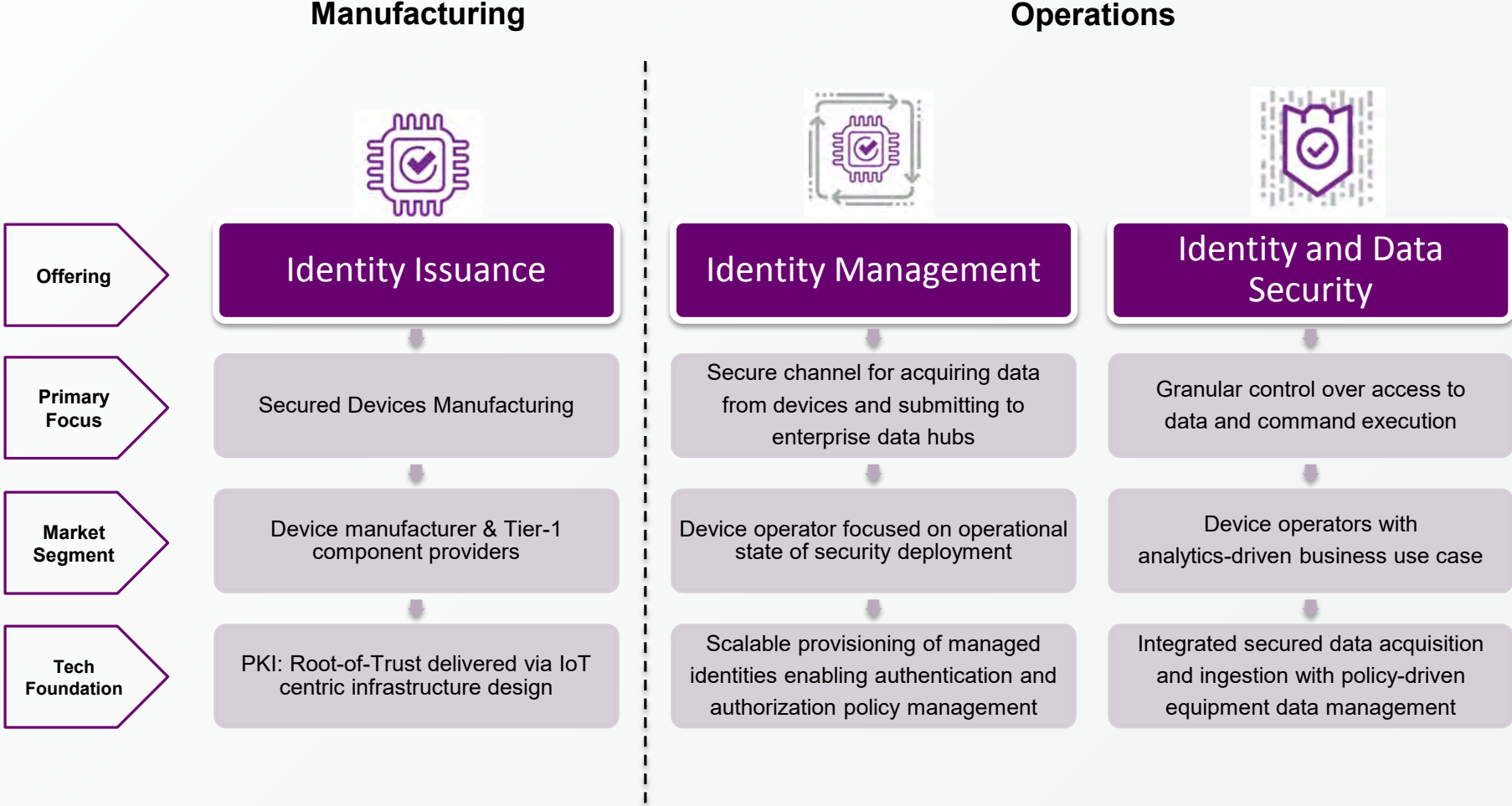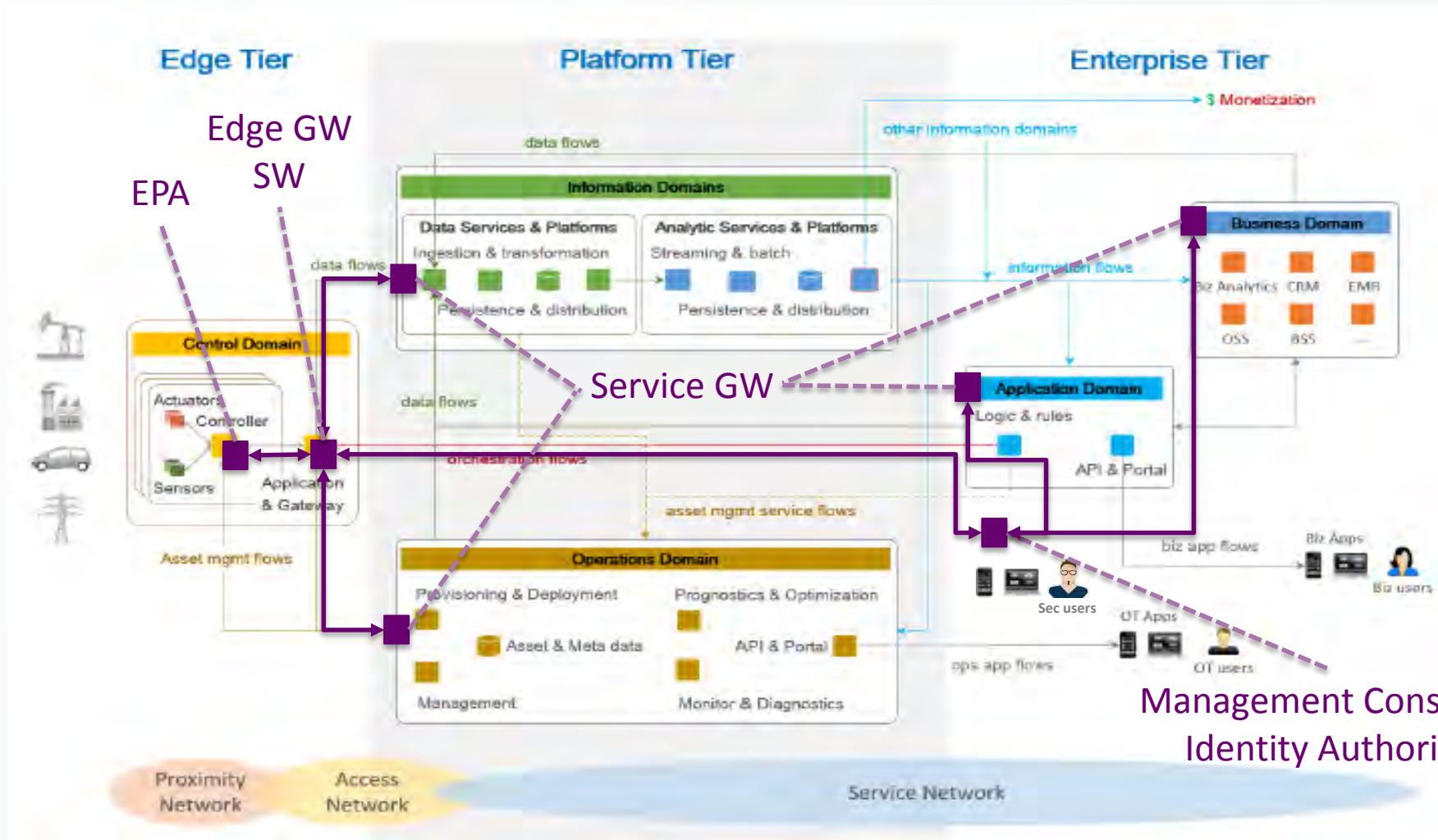| Integrated Device and Data Security | Identity Management: Manufacturing to Operations |
| Authentication and Authorization for every class of device | Data Acquisition Management |
| Supply Chain Integrity | Secure Auto Enrollment and Provisioning |

- STREAMLINED DEPLOYMENT FOR BUSINESS OUTCOMES
- STRONG SECURITY ALIGNED WITH OPERATIONS REQUIREMENTS
- SCALABLE AND ALIGNED TO EVOLVING ECOSYSTEM
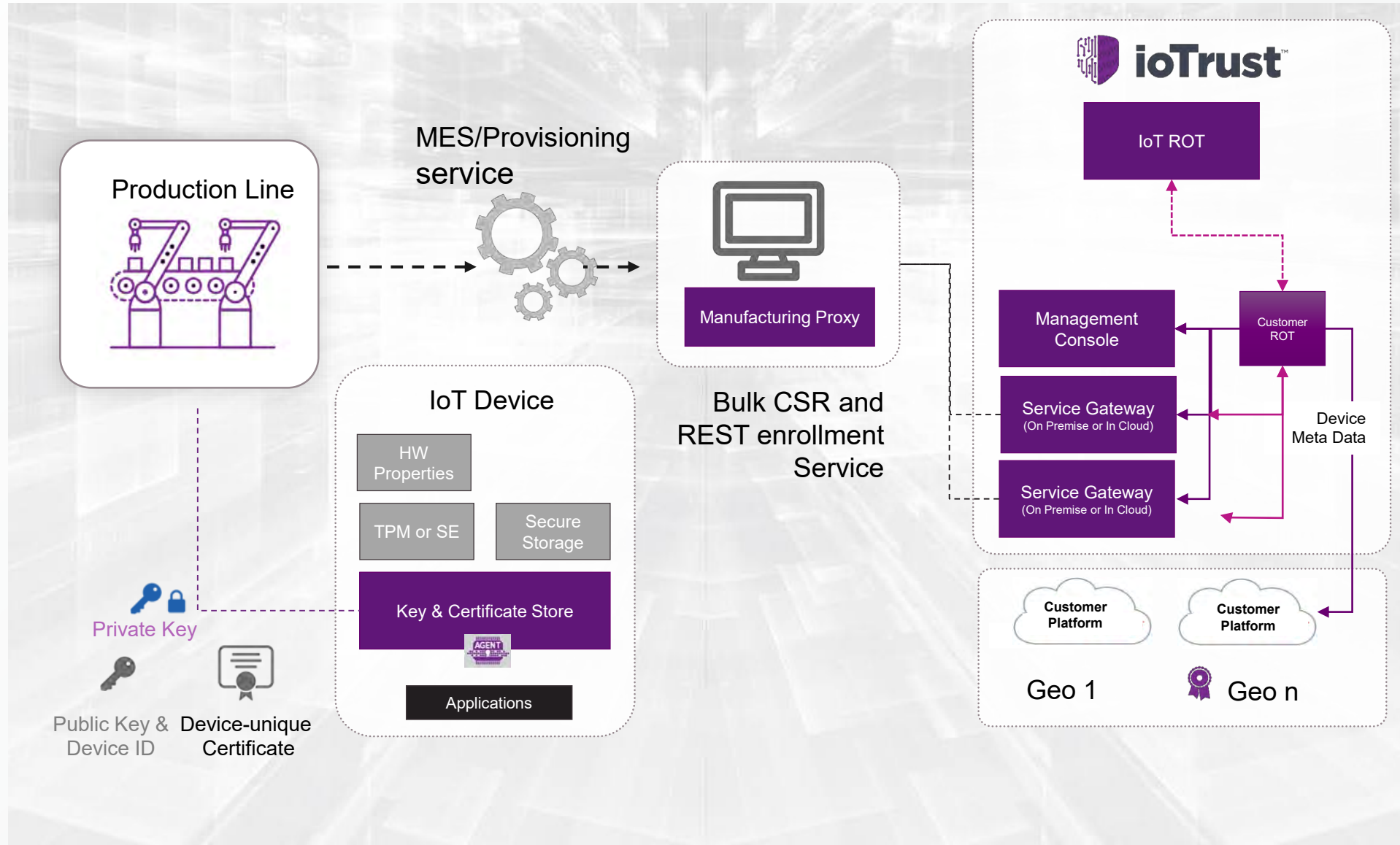
# A Tiered Offering to Fit a Variety of Needs

**Manufacturing**

**Operations**

| | Identity Issuance | Identity Management | Identity and Data Security |
|---|---|---|---|
| **Offering** | | | |
| **Primary Focus** | Secured Devices Manufacturing | Secure channel for acquiring data from devices and submitting to enterprise data hubs | Granular control over access to data and command execution |
| **Market Segment** | Device manufacturer & Tier-1 component providers | Device operator focused on operational state of security deployment | Device operators with analytics-driven business use case |
| **Tech Foundation** | PKI: Root-of-Trust delivered via IoT centric infrastructure design | Scalable provisioning of managed identities enabling authentication and authorization policy management | Integrated secured data acquisition and ingestion with policy-driven equipment data management |

# IIC Reference Architecture: ioTrust Offering



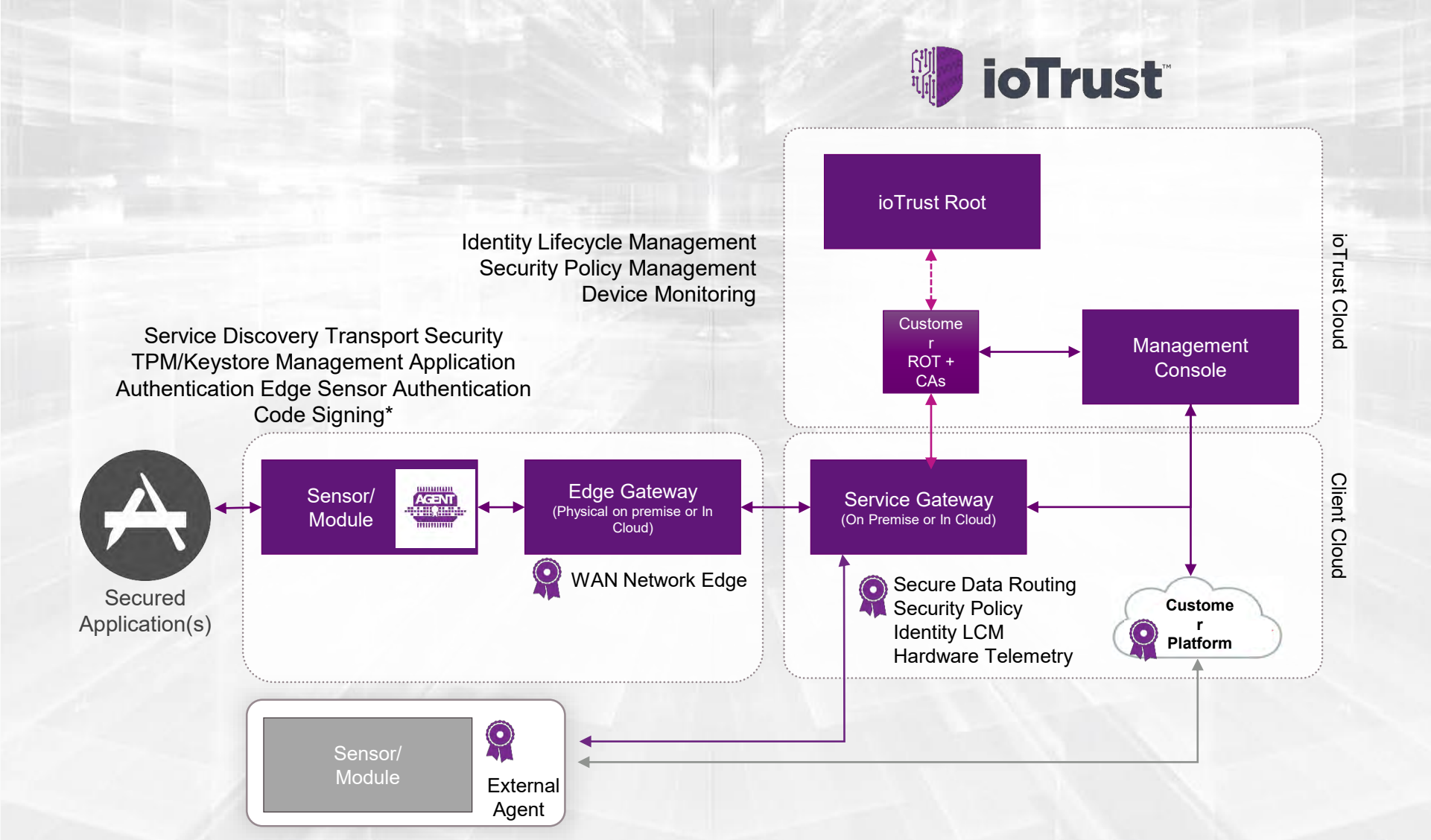Platforms (can be multiple) can be bought or built

# Manufacturing Identity Issuance

# Operational Identity Management



**ioTrust™**

Identity Lifecycle Management
Security Policy Management
Device Monitoring

Service Discovery Transport Security
TPM/Keystore Management Application
Authentication Edge Sensor Authentication
Code Signing*

ioTrust Root

Customer ROT + CAs

Management Console

ioTrust Cloud

Client Cloud

Secured Application(s)

Sensor/ Module — AGENT

Edge Gateway
(Physical on premise or In Cloud)

Service Gateway
(On Premise or In Cloud)

WAN Network Edge

Secure Data Routing
Security Policy
Identity LCM
Hardware Telemetry

Customer Platform

Sensor/ Module

External Agent

# Securing the Endpoint

The ioTrust™ Endpoint Agent is a small, lightweight Software binary that can be used to anchor customer security. The pre-built package reduces development effort to achieve secure and feature rich identity Management

Endpoint agent

Identity lifecycle management – enrollment, renew, suspend and terminate in real-time

Secure Software Keystore with on board key generation capabilities

Crypto libraries supporting ECC & RSA including TLS 1.2 stack

Auto enrollment and service discovery leveraging multicast COAP & Signed SCEP services

Device monitoring via mutually authenticated MQTT telemetry data pipe

# Trust Federation

Building secure applications requires a chain of trust established from manufacture to operational use case. Tools and infrastructure federating trust must seamlessly facilitate secure identity validation and management across organizations

Securely establish & manage device keys in a central PKI and Hardware Security stores

Autonomous mutual authentication for applications and things

Manage trust between organizations via secure IoT Root Of Trust provided by ioTrust™

Restrict trust relationships operationally via secure infrastructure throughout the solution stack

Migrate and on board legacy systems through CA and device cert Import/Export at Service Gateways

Create devices and components that are both usable & secure regardless of device class

# Creating Trust for Industries

**SMART MANUFACTURING**

We've partnered with one of the largest silicon manufactures and M2M providers in order to enable distributed manufacturers to uniquely issue trusted identities onto devices.

**SECURELY MANAGE INDUSTRIAL NETWORKS**

We enable a global leader in industrial automation and energy management solutions to ensure even the most complex, high risk, and distributed IOT systems can operate securely.
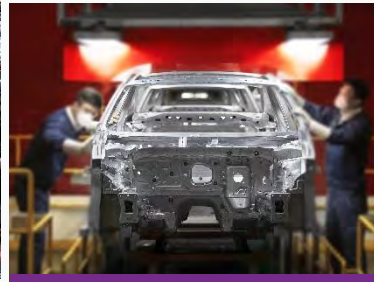
**VEHICLE-TO-VEHICLE AND VEHICLE-TO INFRASTRUCTURE**

We developed a solution for two of the biggest names in the automotive sector to enable them to embed trusted identities onto vehicular components at all levels of the supply chain.

**SMART GRID AND SMART ENERGY**

We're working with energy and utility companies from Canada to the Middle East, enhancing the safety and privacy of smart 'things' wishing to connect to the utility network – and authenticating and authorizing data channels that support data collection/analysis and remote device control.

**SECURED DATA MANAGEMENT AND ANALYTICS**

We're enabling our Telco/SI/ESP partners to realize value-added service delivery models for their customers, by enabling the secure collection and transfer of dynamic analytic insight from millions of devices.