



# Safe access and Connection

Omar Ochoa  
Palo Alto Networks



# Intro to 5G

# 5G in the Enterprise sector

- Nearly  $\frac{2}{3}$  of IT decision makers are aware of 5G and 47% say their organizations have already started planning for it



Source - Nokia

# Enterprise 5G - Use Cases

## Manufacturing - Industry 4.0

### Manufacturing

Overcome Wifi QoS, TCO and connectivity gaps

Inefficiencies in covering large areas  
Connectivity of people, machinery and sensors

### Chemical factories

Require outdoor, large area, along with indoor coverage

Sites operate in remote rural locations, with sensors, advanced machinery, complicated processes and a combination of IT and OT needs

## Warehouses

### Smart Warehouses

Autonomous devices, sensors and personnel are on premise

Require ultra low latency and high bandwidth

## Construction

### New business parks and buildings

Offer 5G connectivity, replacing or coexisting with Wi-Fi and network cables.

To support less cables and fewer Wi-Fi router deployment points, reducing complexity and cost.

# Enterprise 5G - Use Cases

## Medical

### Hospitals

**Unique requirements to support regular and crisis times.**

Private 5G network is used by hospitals in order to provide highly reliable, secured low latency, high bandwidth dedicated separated network – resilient, secure and able to operate even in crisis mode where all other networks are either being overloaded or decommissioned

## Seaports

### Seaports

**To provide independent isolated wireless cellular network connectivity around the port to manage location, security cameras, and personnel**

Specific connectivity needs in a wide area and highly dense metal environment

## Agriculture

### Smart Agriculture

**To provide low latency, high speed bandwidth and wide area connectivity**

Autonomous agriculture machinery, vehicles and smart sensors are connected to control centers to remotely monitor and manage the farms.

# 5G: The Catalyst of Change

# 5G will drive the future of Industry 4.0 and Critical Infrastructure



## INDUSTRIES

Manufacturing,  
transportation, logistics,  
smart agriculture, ...



## CRITICAL INFRASTRUCTURE

Utilities, oil & gas, public  
safety, defense, ...



## SOCIETY

Healthcare, smart cities,  
connected cars, digital  
commerce,  
entertainment, ...

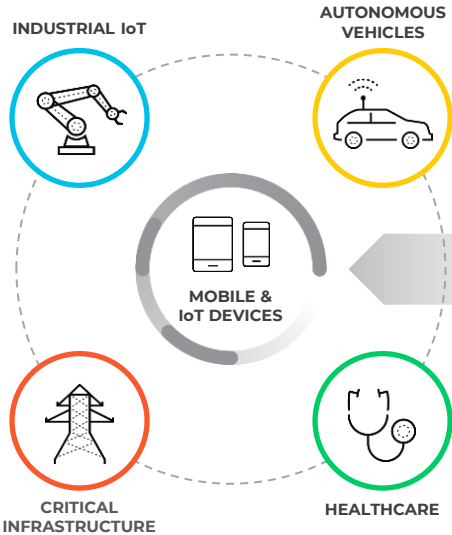
## DIGITAL TRANSFORMATION

5G CONNECTIVITY FABRIC

ENTERPRISE-GRADE SECURITY

# What's changing with 5G?

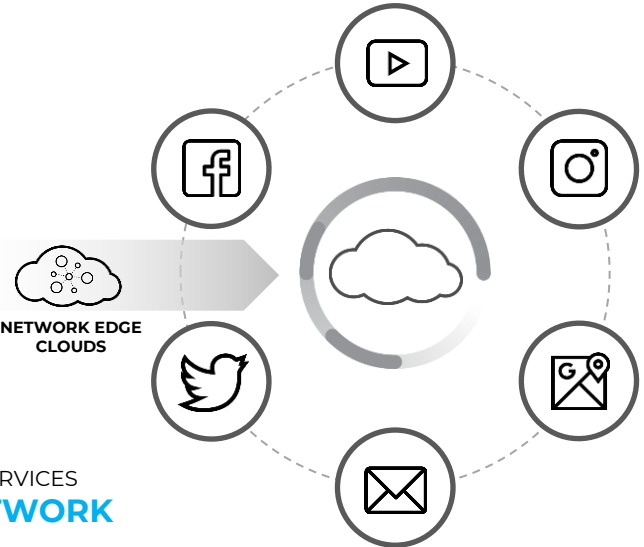
EXPANDED CUSTOMER BASE  
**KEY INDUSTRY VERTICALS/ENTERPRISES**



NETWORK CORE, APPLICATIONS & SERVICES  
**MOVE INTO THE EDGE NETWORK**

**4G** LTE

APPLICATIONS & SERVICES  
**RUN OVER-THE-TOP**



# What's driving this accelerated digital transformation

## Mobility

From power grids, sensors to actuators, ubiquitous connectivity and real-time communications shapes vision for 5G

---

1.01 billion

5G connections by 2023, 217.2% compound annual growth rate (CAGR) from 2019 to 2023

## IoT

Rising demand of IoT/M2M connections across industry verticals drive new 5G revenue models

---

41.6 billion

devices estimated to be connected to the Internet by 2025

## Cloud

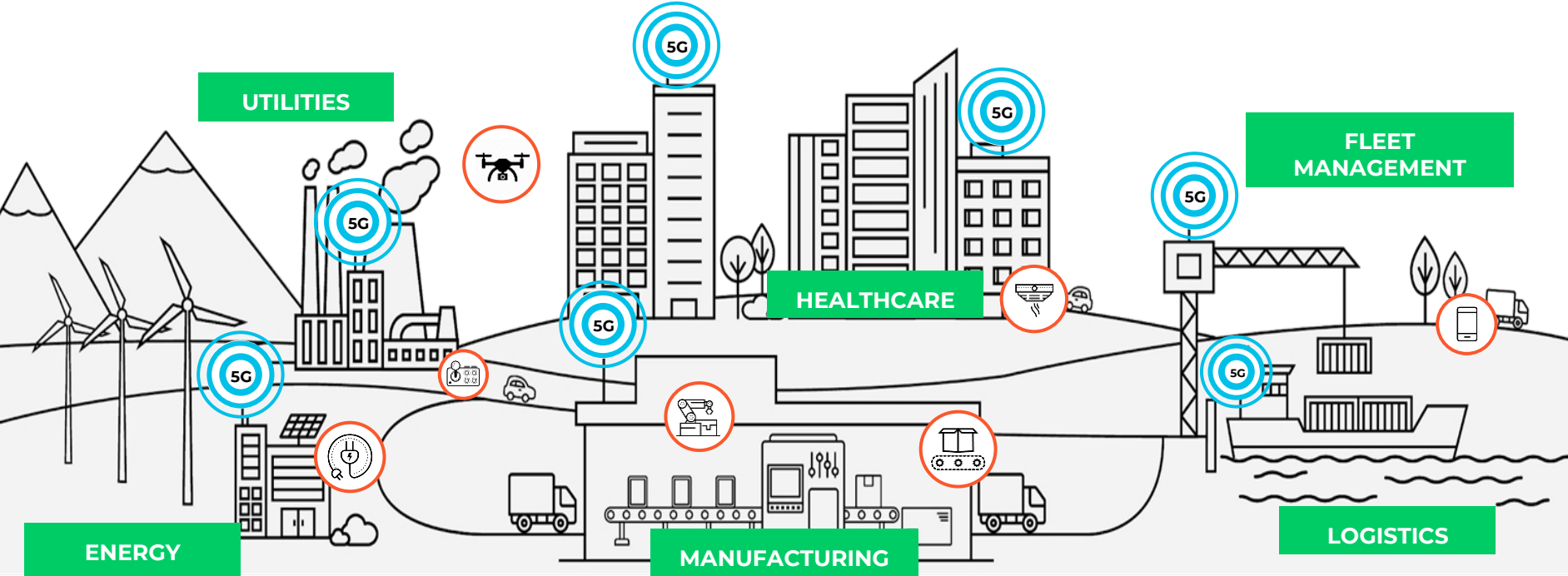
Shift to distributed edge computing architecture to handle emerging 5G use cases

---

157% CAGR

growth in multi-access edge computing (MEC) adoption in wireless networks by 2024

# 5G will drive the future of Industry 4.0



**Private Cellular Networks** | **Public Service Provider Networks**

## But enabling these opportunities creates risk

### More devices and data

mean more targets for cyber attacks.

---

41.6 billion

devices estimated to be connected to the Internet by 2025

### Cloud-native deployments

E2E stand alone 5G networks will be cloud native.

---

75%

Of our survey respondents said that cloud security tools and solutions are outpaced by threats to their cloud systems

### New 5G Services

Industry verticals demand enterprise-grade security.

---

67%

increase in cyber attacks over the last 5 years

IOT

# IOT OS



operating system used in most of the iot devices



All

Images

News

Videos

Shopping

More

Tools

About 70,300,000 results (0.62 seconds)

## Top 17 IoT operating systems for IoT devices in 2021 and beyond

- Raspbian Pi.
- Ubuntu Core.
- Ubuntu MATE.
- RISC OS OPEN and RISC OS Pi.
- FreeRTOS.
- OSMC.
- Contiki.
- Tizen.

More items... • Nov 16, 2021

<https://www.intuz.com> › top-iot-operating-systems-for-iot... ⋮

Guide on Top 17 IoT Operating Systems For IoT Devices | Intuz

# First Things First

## What is an IoT?

IoT stands for Internet of Things. A non-traditional thing/device connecting to internet in an enterprise network

### Examples of IoT

*Prevalent across all industries*



## What is an IoMT?

IoMT stands for Internet of Medical Things. IoMT devices are medical technology devices connecting to a healthcare delivery organization (HDO) network

### Examples of IoMT

*Prevalent in healthcare*



## What is an OT?

OT stands for Operational Technology. Sometimes they are also called IIOT (Internet of Industrial Things). OT devices monitor or control other devices. **Most OT devices are not internet facing today**

### Examples of OT

*Prevalent in industries like manufacturing automotive, building oil & gas, utilities, etc*



# Massive Growth of Connected IoT Devices Across All Verticals



CRITICAL INFRA

**6B**  
177% ↑



SMART BUILDING

**4.7B**  
220% ↑



RETAIL

**2B**  
180% ↑



GOVT

**1.8B**  
162% ↑



HEALTHCARE

**1.3B**  
244% ↑



BANKING

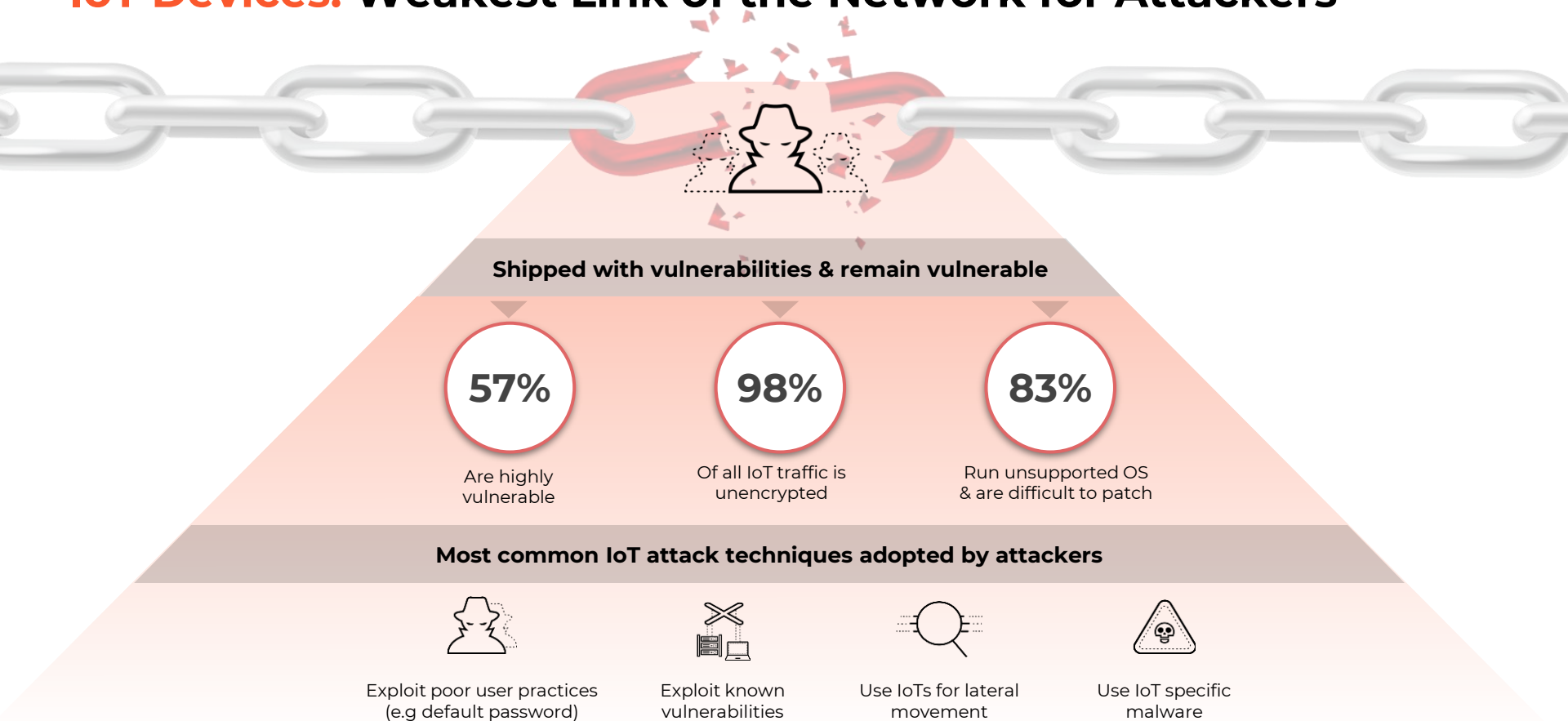
**.6B**  
47% ↑

**10M** new smart devices added to networks every day

**4X** the number of enterprise IoT devices than users

\*Expected # of devices in 2030 and % increase from 2020 to 2030

# IoT Devices: Weakest Link of the Network for Attackers



**3B** attacks on IoT devices in 2021  
**2X** from 2020

## **Bloomberg**

**150,000** Verkada cameras footage stolen affecting **Tesla, Nissan, Schools, Hospitals and Jails.**



**40 million** Credit card data stolen from ~ **2000 Target stores** using HVAC. Ongoing legal impact.

## **DIGILOCK AWARE**

**600,000 IoT** attacks affecting **AirBnB, Amazon, Github, HBO, Netflix, Paypal, Reddit, Twitter** and more.

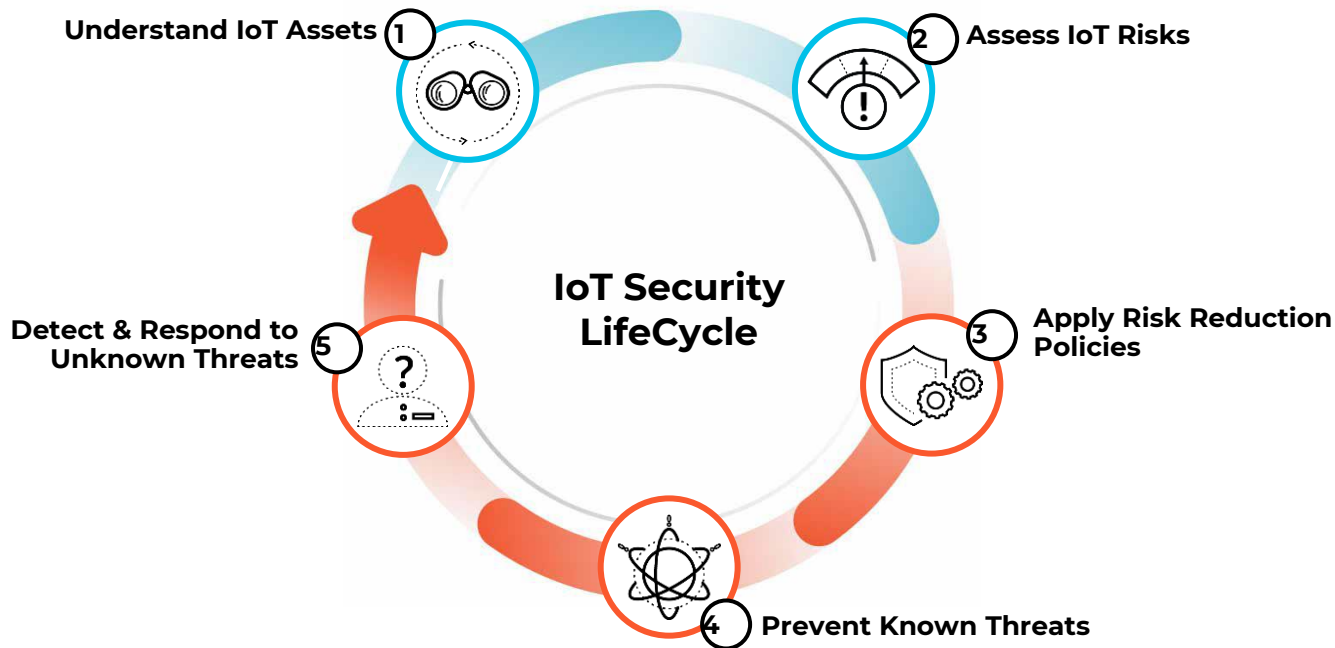
## **B B C**

**Colonial hack: How did cyber-attackers shut off pipeline with Compromised Passwords**

## **BECKER'S HEALTH IT**

Cyberattack on Alabama hospital linked to **1st alleged ransomware death**

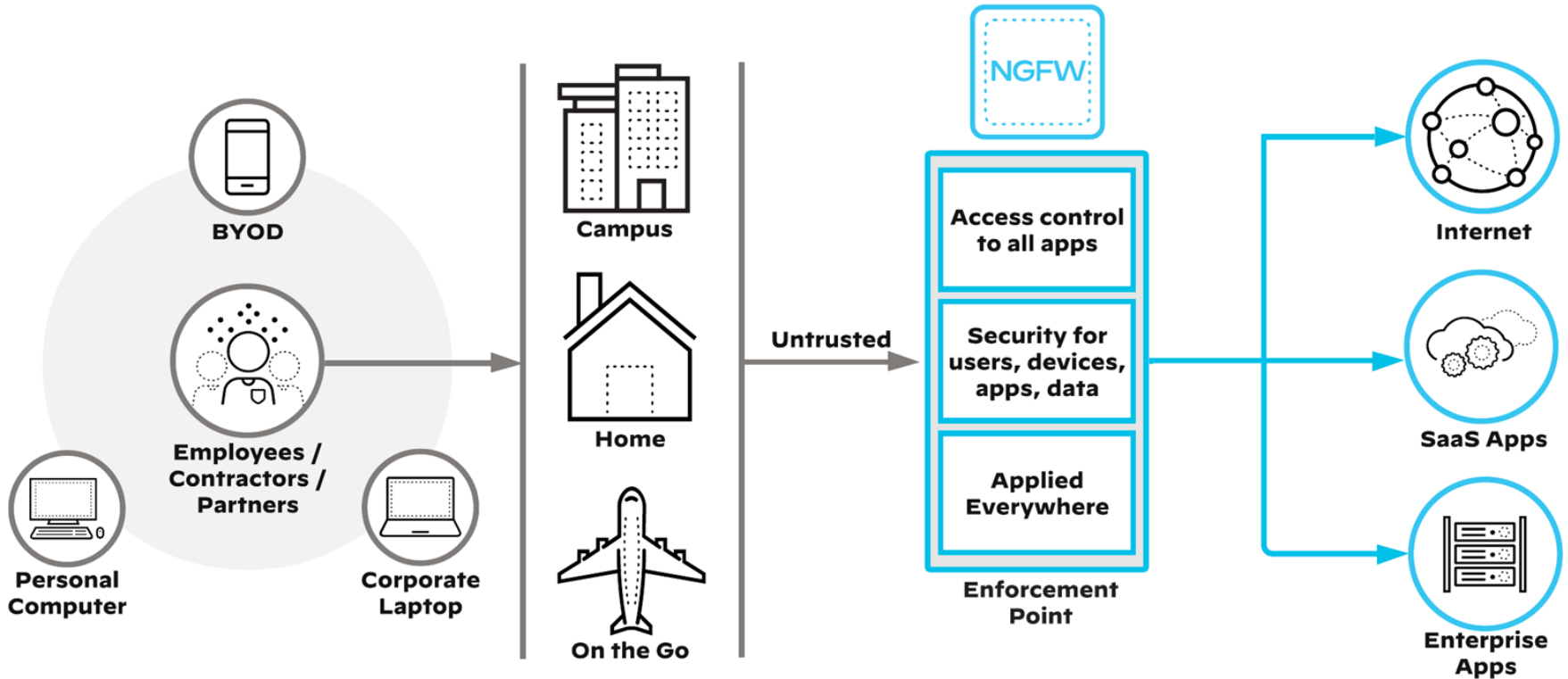
# The Right Methodology to Secure IoT Devices



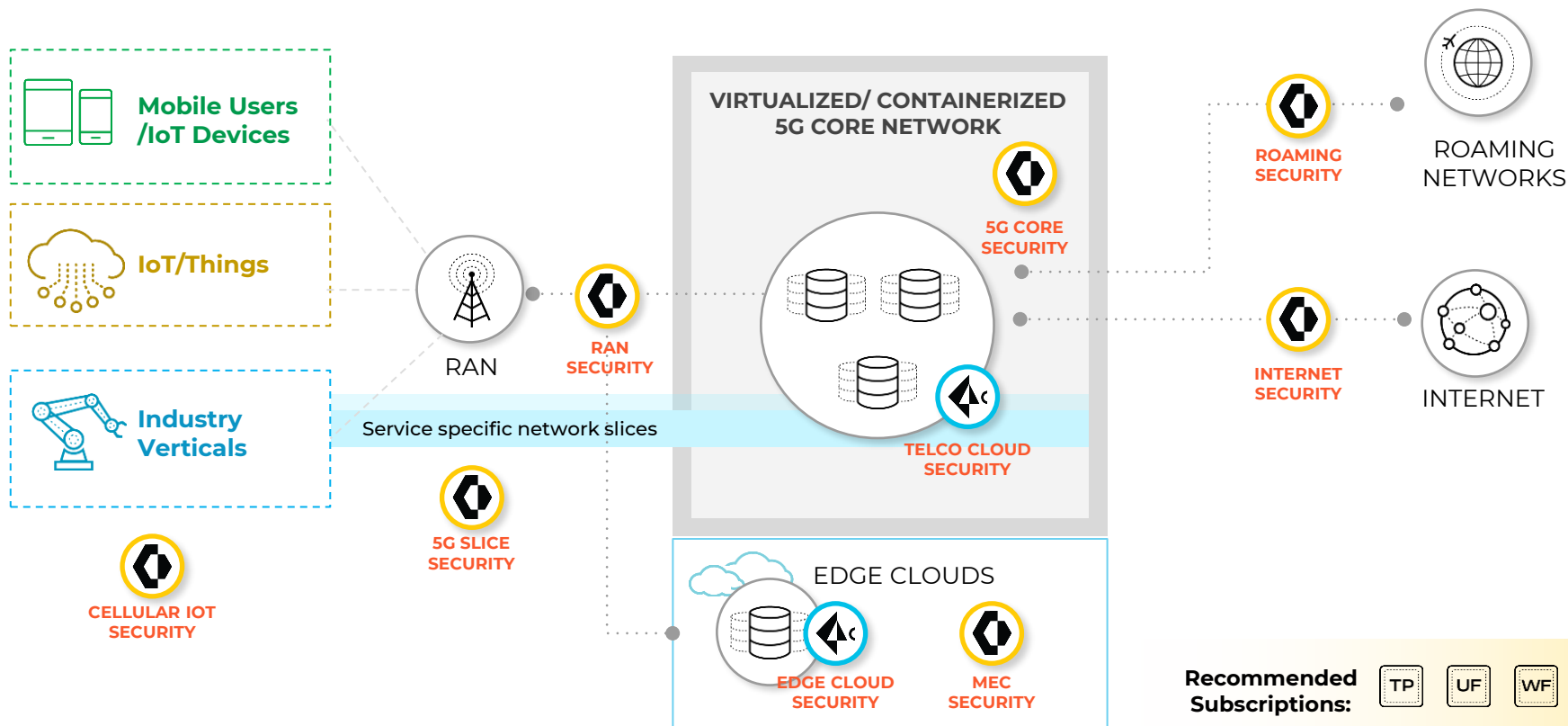
[See how IoT Security maps to the methodology](#)

# Zero Trust

# What is Zero Trust



# Securing Service Provider 5G While Monetizing Investments





# Thank you



## NEW NETWORKS, NEW ARCHITECTURES...

The topic of IoT elicits many ideas when it comes to architectures, applications, things, and processes. Where PAN currently exists in the world of IoT is fairly specific; any North/South, East/West, Tap or pseudo-wire can be a source for ingestion. Ideally we will have access to DHCP data, layer 2 and layer 3 connectivity, deep within the customer's network. That being said, there are many new trends and architectures in as well as new frontiers as it relates to IoT. Many of which need to be explored with our clients' OT counterparts.

### *Operational Network Models*

With the advent of IoT (or operational networks) interconnecting to the larger organizational network, new architectures have emerged that break the traditional core/distribution/access architectures. As an example, the Purdue Reference Model (developed in the 90s) is a reference data flow model for manufacturing and other process-related environments, i.e. using computational devices to control the production process.

## *Edge Computing*

As the need for computation, control and interconnection to the physical world becomes necessary, the concept of edge computing plays a part into the complexities of devices at the edge. As an example, in manufacturing, a company may want to monitor a variable frequency drive's (VFD) power factor that may be monitored to enable predictive maintenance over the motor. Depending on the location of the device in the network, the links to said devices having throughput challenges and resolution requirements may not allow for the data extracted from the VFD to be processed in a central location. By processing the data locally to the device in question, more accurate information can be gleaned by use of analytics or other statistical means.

## *Wireless and Where We Might Apply*

As the rise in various wireless technologies have emerged over the past two decades, additional architectures and protocols have emerged, not all of which we can support. The following are brief descriptions of the networks and how or if we can interact with them:

LoRAWAN - Long range, Wide Area Networking began in 2009 and currently supports more than 100 million devices worldwide. Due to the low cost of this technology (both in power and hardware) it has become extremely popular due to the simplicity of the architecture, the long range of the connections and the overall stability of the protocol. While data eventually traverses over IP, LoRA networks do not employ IP within the wireless network infrastructure. Instead, LoRA relies on an application server to broker the network connections and transfer data northbound. In the case of LoRA, we would not be able to identify devices on the network, however, we would be able to profile the application server and traffic northbound.

NB-IoT - Narrowband IoT aligns fairly well with traditional cellular provider networks. That being said, use of 3GPP/LTE allows for the use of DHCP for devices to join the network. Based on capabilities of discovery via DHCP, we can intercept, discover and profile devices. By sniffing traffic or creating a barrier between the RAN we can collect the data and profile it accordingly. This is also similar to the capabilities and core architecture of 5G.

$\mu$ Wave / mmWave - Both microwave and millimeter wave technologies are typically used in point-to-point or point-to-multipoint communication technologies. These are traditionally terminated at the edge of the network as a way to extend a layer 2 or layer 3 boundary to remote sites and devices, or to create a more expansive, geographically diverse network. Much like any layer 2 or layer 3 network, we should deploy IoT security where we will see interesting traffic or where we can intercept DHCP data for device discovery. For more information on architectures and how we might deploy in these environments, please reach out to your CDSS counterparts for more information.