LOCH TECHNOLOGIES

IoT Security for the *new* Multi-Access Edge

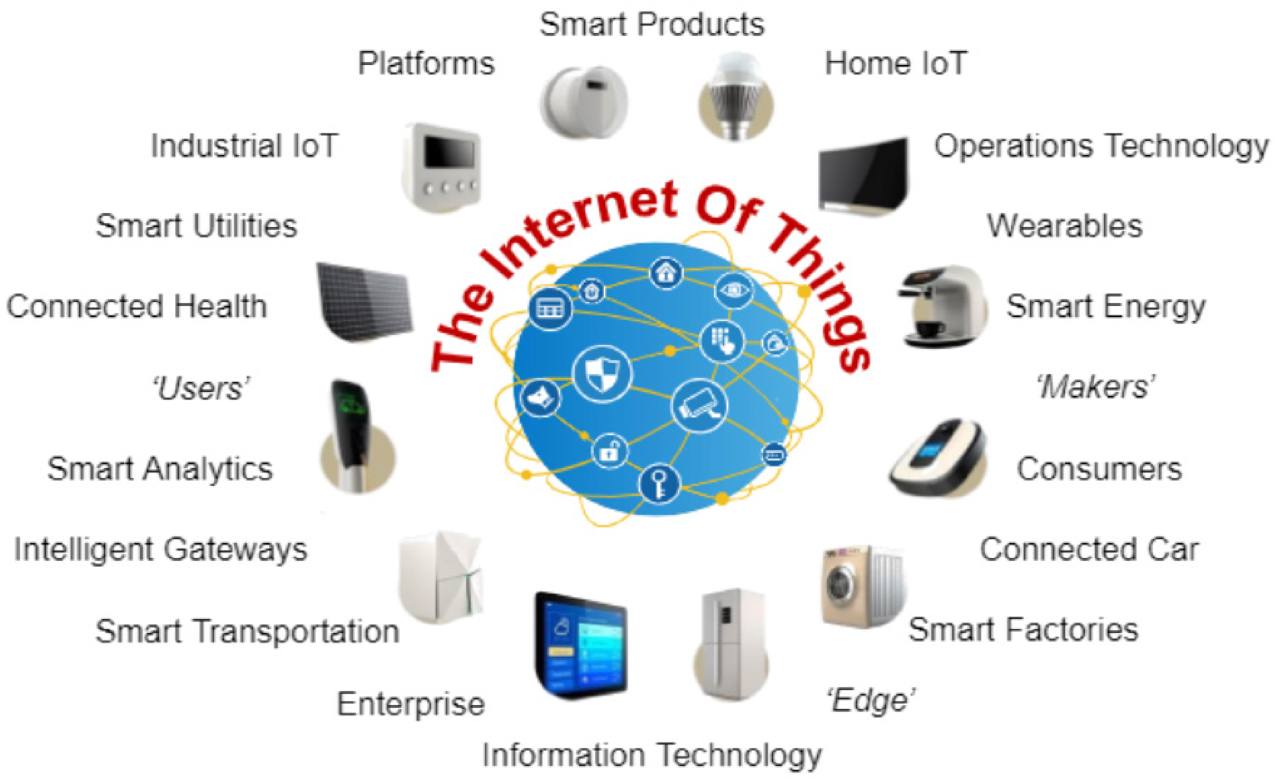
Invisible Threats. Visible Protection

Garry Drummond, CISSP, CWNA, CWSP
Founder & CEO
+1-510-703-6149
gdrummond@loch.io

Background

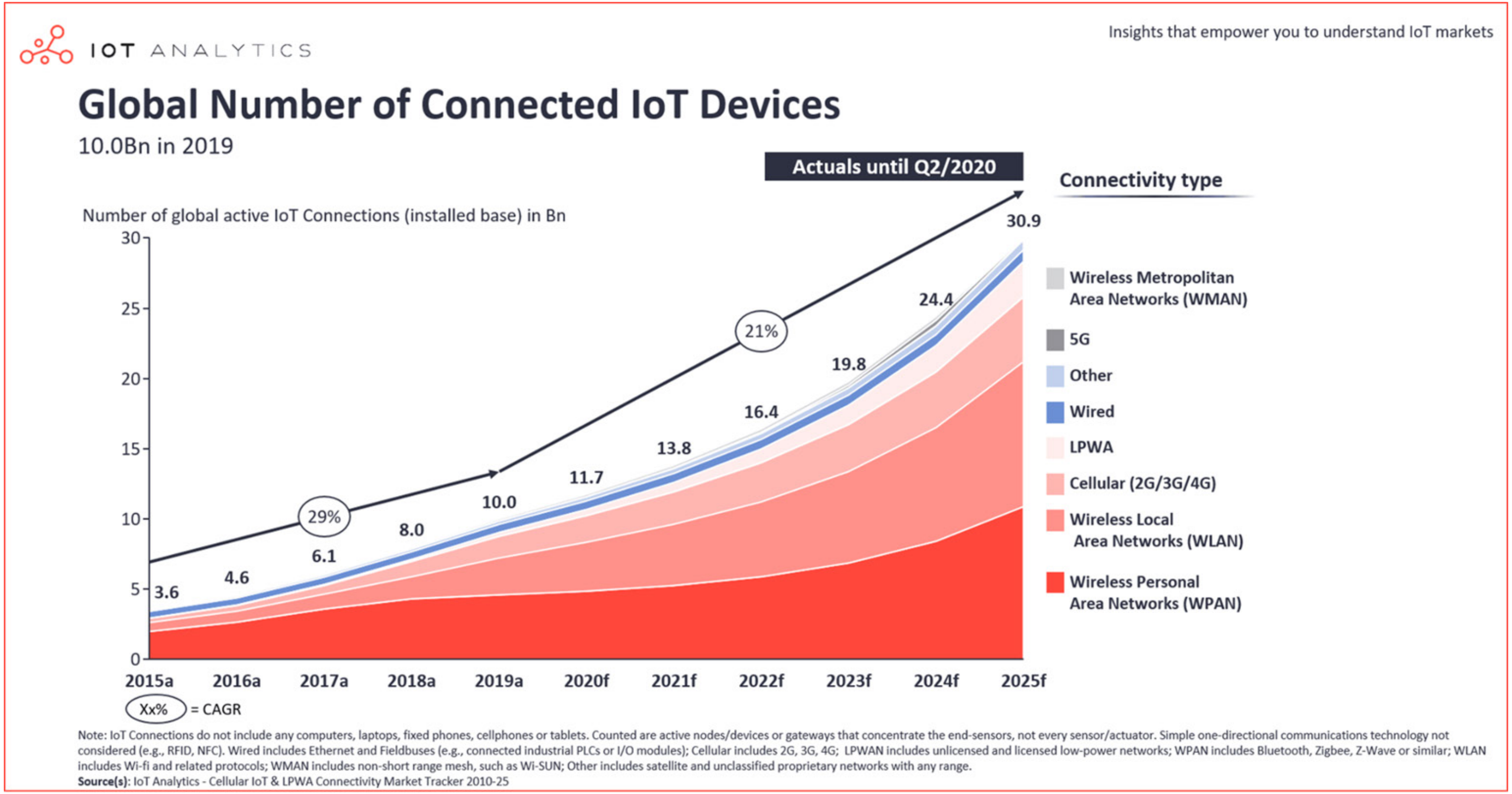
- Certified Information Security Professional (CISSP)
- Certified Wireless Security and Network Professional (CWNA/CWSP)
- Business owner and entrepreneur specializing in B2B technology
- Silicon Valley Startup of the Year in 2015
  Silicon Valley Company of the Year in 2016
  In 2017 Most innovative CEO of the Year
- I hold 5 patents for IoT security
- June 2021 - Gartner Cool Vendor for Edge Computing

The Internet of Things (IoT) has created the world's largest attack surface



- Everything now connects to something, or someone
- 80% of IoT is wireless, wireless is now the new network and new attack surface

Connected IoT Devices



IOT ANALYTICS

Insights that empower you to understand IoT markets

Global Number of Connected IoT Devices

10.0Bn in 2019

Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WMAN includes non-short range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

Wireless Is The New Attack Surface

LOCH TECHNOLOGIES

Lack of visibility

50+ Billion Devices by 2025

Lack of assessment tools

Plethora of new OS's and new software packages

ARMmbed

Google Developers

Green Hills SOFTWARE

TIZEN

NUCLEUS

Attack surface is increasing

Exploding number of protocols and frequencies

ZigBee

LoWPAN

P25

Wi Fi

LoRa

lte

sigfox

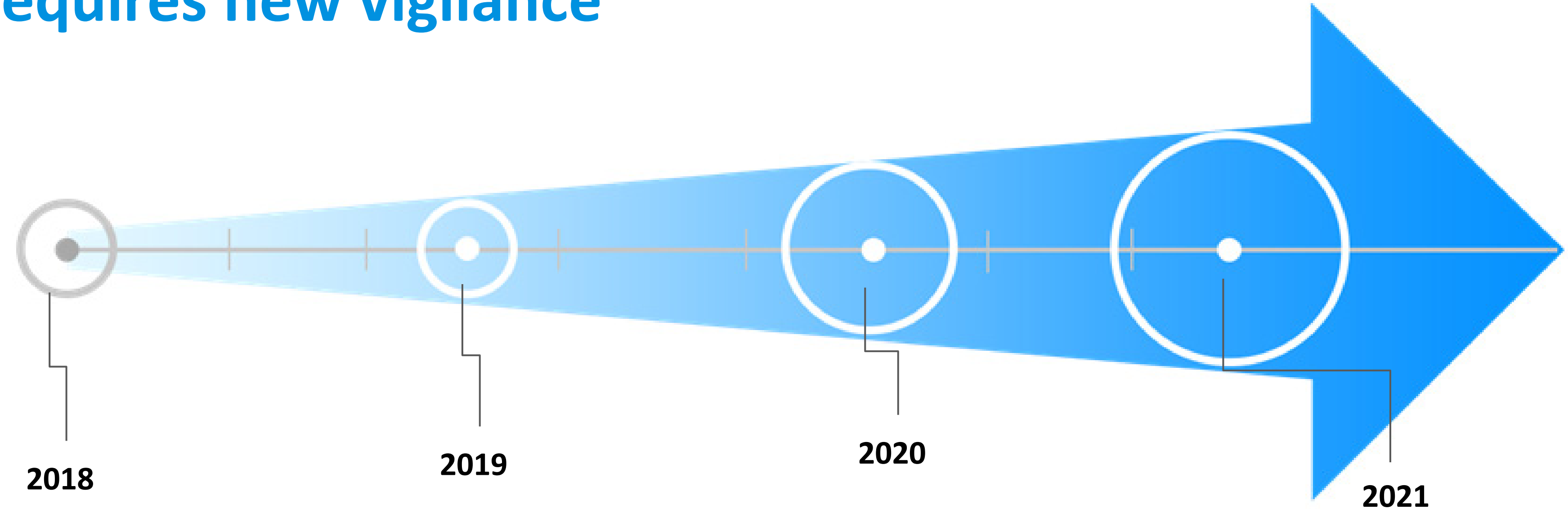
Z-WAVE

75%

By 2023, 75% of organizations will be forced to restructure risk and security governance to address the convergence of IT and IoT security needs.

The speed at which IoT is being exploited requires new vigilance

LOCH TECHNOLOGIES



2018

- 83% of IoT run on unsupported operating systems

2019

- 25 Billion IoT online
- 57% of IoT is vulnerable to high impact attacks that can lead to data exfiltration

2020

- 50 Billion IoT online
- IoT attacks every 1 min
- Cost of Breach $2.7M

2021

- IoT attacks every 3 secs
- Cost of Breach $5.8M
- More attacks in 1H/21 than in all of 2020
- 98% of IoT traffic is unencrypted

IoT Device Security at the Edge Poses Unique Challenges

IoT World Today

May 7th 2021

IoT practitioners need to adapt traditional methods to ensure IoT device security at the edge

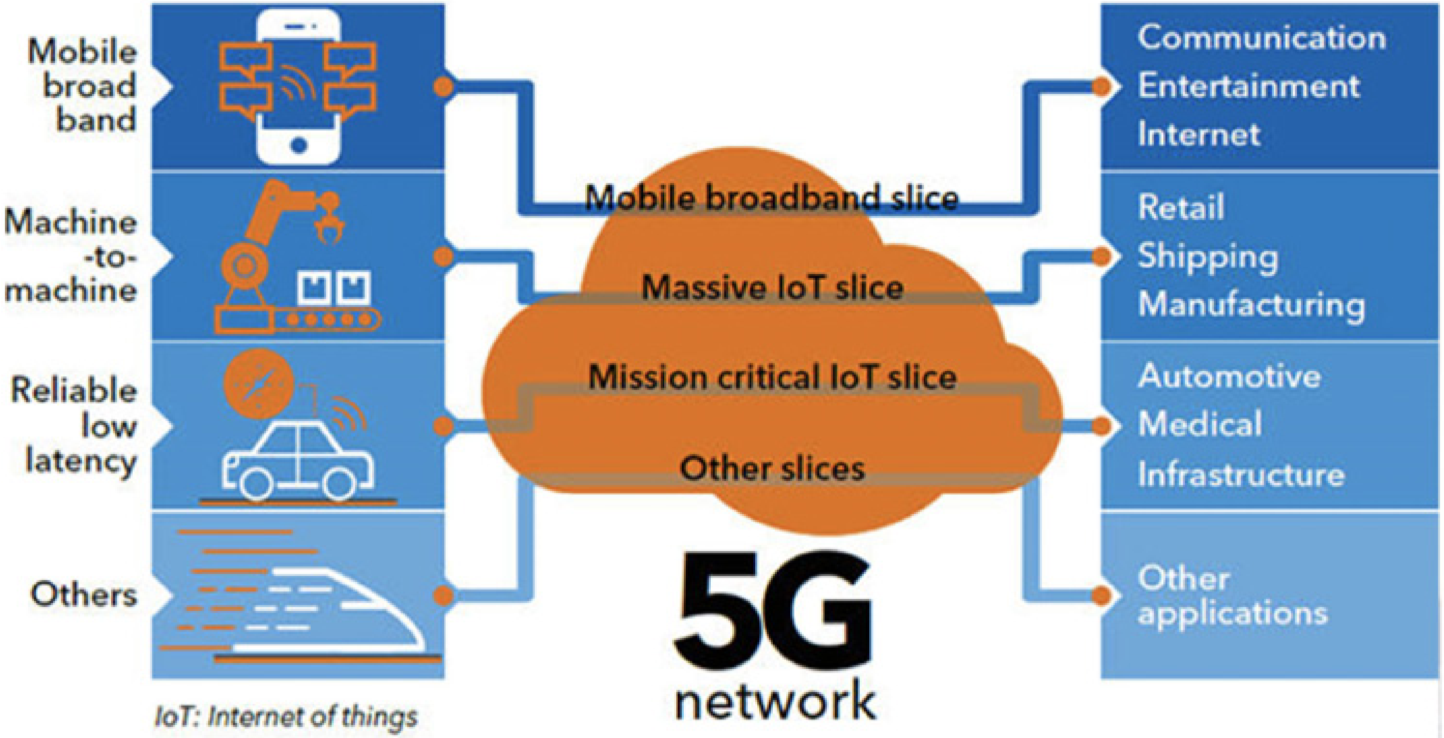
https://www.iotworldtoday.com/2021/05/07/iot-device-security-at-the-edge-poses-unique-challenges/?Issue=IOT-001UBER_20210518_IOT-001UBER_565&sfvc4enews=42&cl=article_1&utm_rid=CPNET000011857520&utm_campaign=37803&utm_medium=email&elq2=fe47e74d158441c3b9d57904a34aa12c

The Promise of 5G?

- Low Latency - allows for the enablement of new edge applications (microservices)
- Higher Bandwidth = faster download speeds
- Ubiquitous Internet Access - indoor and outdoor (Hybrid plans combine WiFi & Cellular)
- Better Security - PKI
- Competitive Advantage -lower cost

Source: Qualcomm

5G Network Slicing

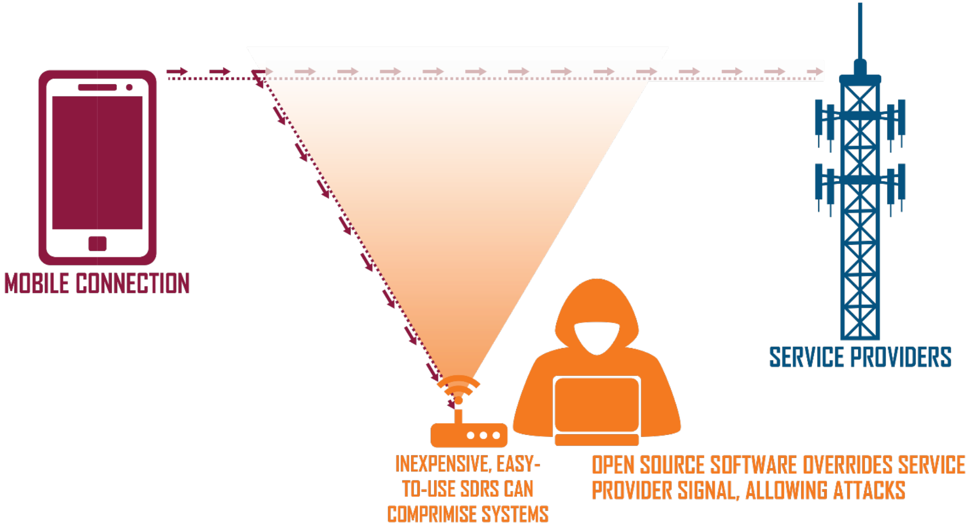


Source: Trend Micro

A New Architecture = New Security Issues

Identifying and Preventing Cellular Attacks

- Cellular denial-of-service (DOS)
- Insertion of malware/virus/ransomware into cellular devices
- Exploiting smartphones as a bridge to sensitive corp infrastructure
- Malicious location tracking

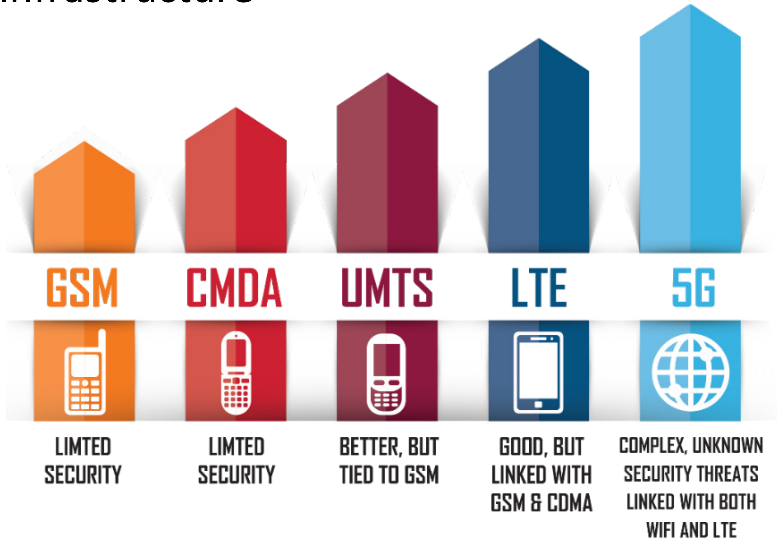


MOBILE CONNECTION

SERVICE PROVIDERS

INEXPENSIVE, EASY-TO-USE SDRS CAN COMPRIMISE SYSTEMS

OPEN SOURCE SOFTWARE OVERRIDES SERVICE PROVIDER SIGNAL, ALLOWING ATTACKS



GSM — LIMTED SECURITY

CMDA — LIMTED SECURITY

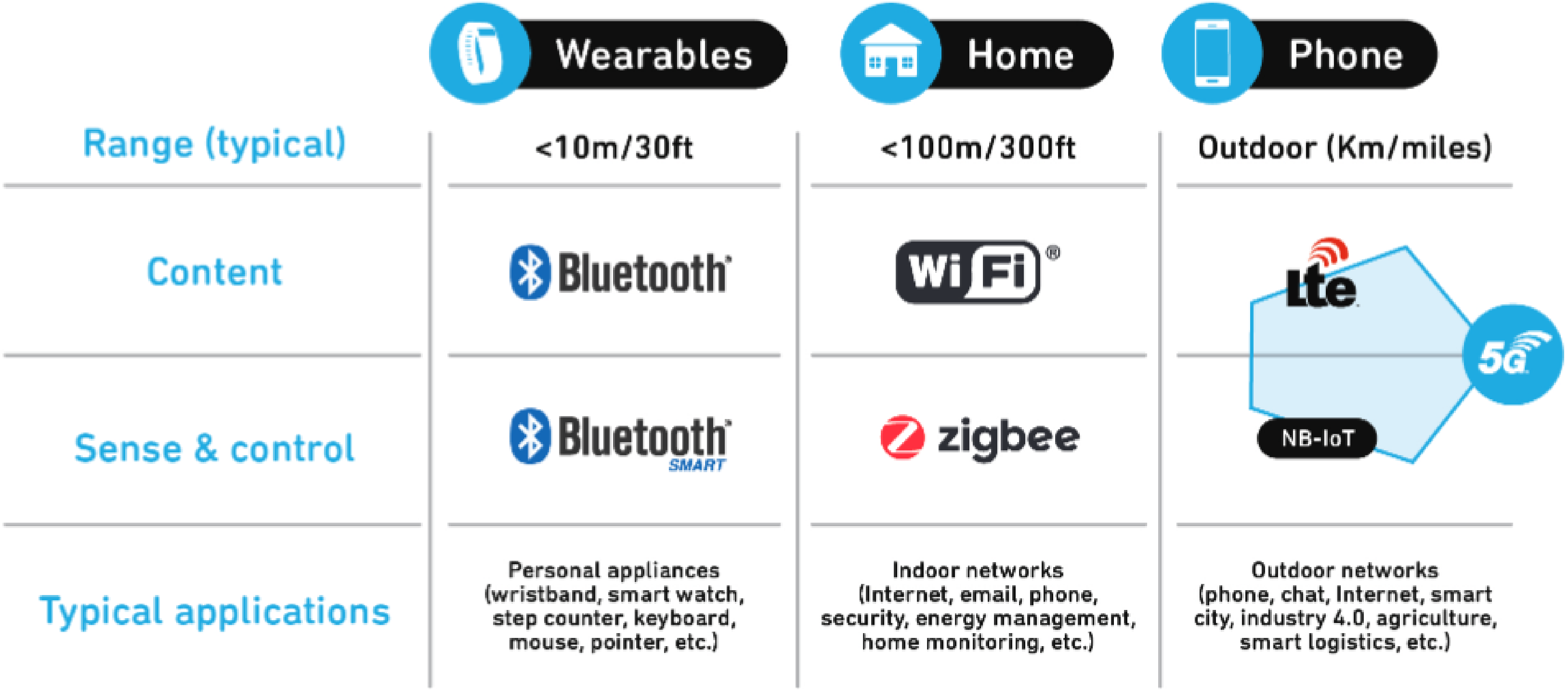
UMTS — BETTER, BUT TIED TO GSM

LTE — GOOD, BUT LINKED WITH GSM & CDMA

5G — COMPLEX, UNKNOWN SECURITY THREATS LINKED WITH BOTH WIFI AND LTE

chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.etsi.org/deliver/etsi_TS/133500_133599/133501/15.01.00_60/ts_133501v150100p.pdf

Is 6Ghz Wi-Fi (802.11ax) the new 5G?



	Wearables	Home	Phone
Range (typical)	<10m/30ft	<100m/300ft	Outdoor (Km/miles)
Content	Bluetooth	Wi Fi®	lte 5G
Sense & control	Bluetooth SMART	zigbee	NB-IoT
Typical applications	Personal appliances (wristband, smart watch, step counter, keyboard, mouse, pointer, etc.)	Indoor networks (Internet, email, phone, security, energy management, home monitoring, etc.)	Outdoor networks (phone, chat, Internet, smart city, industry 4.0, agriculture, smart logistics, etc.)

Source: Qorvo Wireless

The Problem

ZigBee

lte

sigfox

Z WAVE

5G

DAMNED if you do
DAMNED if you don't
Larson

"C'mon, c'mon — It's either one or the other."

WiFi

P25

LoRa

Wireless Attacks

PREVENT CELLULAR ACCESS - As wireless devices may have cellular access, an attacker may want to ensure cellular access is unavailable while performing WiFi attacks — in doing so they create fake cell towers and deny authentication to the network.

DOWNGRADE CELLULAR NETWORK - Attacks against weaker cellular networks require disabling more secure networks allowing for man in the middle attacks to take place, installing Trojans.

EVIL TWIN AP - Attacker creates an Access Point and draws devices towards it through a higher signal power and/or existing network using deauthentication. Connected devices may expose credentials or be directed to malicious services, compromising the system.

WEAK AUTHORIZATION - An at-home network used by remote office staff may have WiFi Protected Setup (WPS) enabled. The access codes to many devices are well known or easily brute force allowing the attacker access to the network

WEAK ENCRYPTION – wireless networks may not follow strong and required network security practices by using common/easily recovered WPA/WPA2 passphrases, unencrypted or known weak-ciphered networks

ROGUE DEVICES - A rogue device, such as a spy camera, wireless-enabled USB drive, or an open printer may put the network at risk

Cellular Attacks

UE/Device Threats

Malware, Firmware Hacks, Senor Compromises IoT, TFTP MitM Attacks, Bots DDos, Device Tampering

Air Interface Attacks

MitM Attacks, Rogue communication lead to data exfiltration, Jamming

SIM Port Hijack / SIM Swapping

Loss of control over your SIM connectivity

DOWNGRADE CELLULAR NETWORK

Allowing for man in the middle attacks to take place, installing Trojans.

RAN Threats

MEC Server Vulnerabilities, Rogue Nodes,Malware, DDoS and BOTNETs

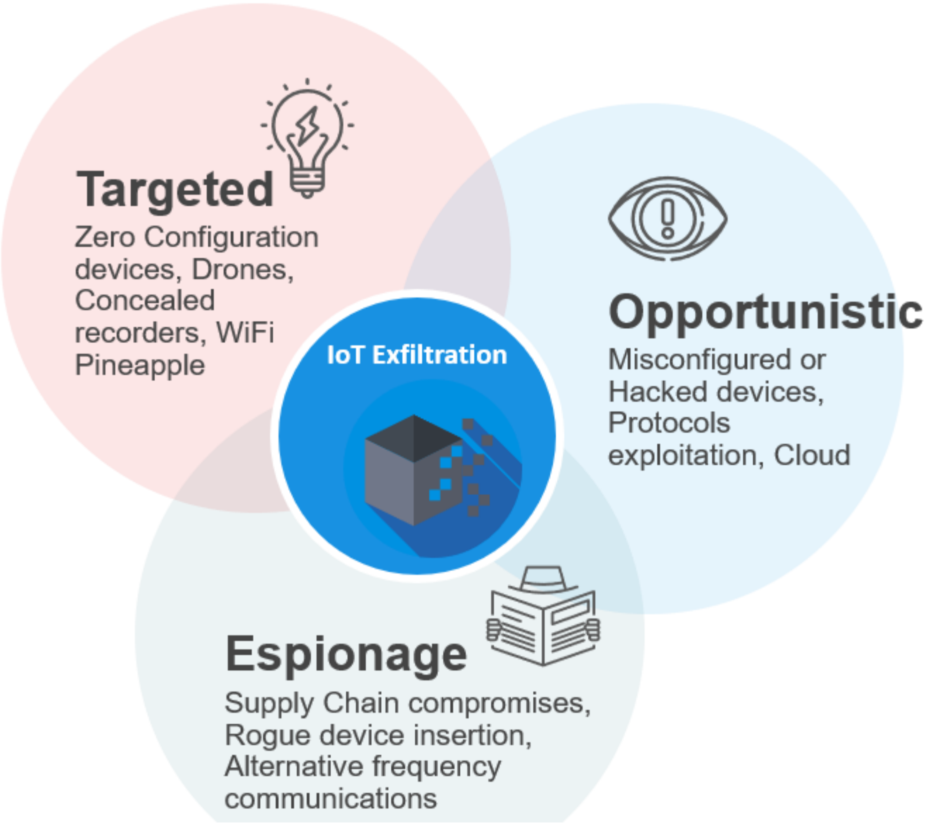
Rogue Cell Tower Detection

SIM devices connecting to an evil-twin cell tower. Steal credentials and data

Roaming

Increases data usage and excessive billing costs. Enforce no unauthorized roaming

IoT Exfiltration Methods



IoT Exfiltration

Targeted

Zero Configuration devices, Drones, Concealed recorders, WiFi Pineapple

Opportunistic

Misconfigured or Hacked devices, Protocols exploitation, Cloud

Espionage

Supply Chain compromises, Rogue device insertion, Alternative frequency communications

Zero Configuration

Are obscured from normal network operations – can operate autonomously outside the scope of the enterprise network.

Supply Chain Integrity

Data is back channeled or close proximity listening stations.

Communications is obfuscated by the cloud or use of alternate protocols and frequencies.

Protocol Limitations

Many IoT protocols lack even basic authentication, integrity and privacy considerations.

Zero Trust Framework

LOCH TECHNOLOGIES

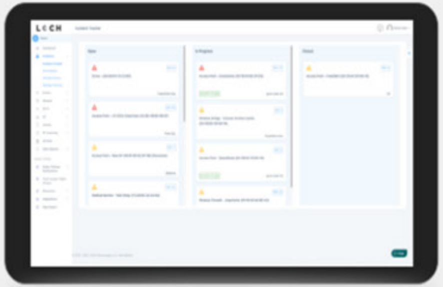
DETECT

- Detect, identify & classify all broad spectrum RF emitting devices in range
- Device and network pairing communication map analysis and correlation
- Risk assessment threat ranking for zero trust network access control
- Mobile App for hunting rogues even if mobile

TRACK

- Wireless deep packet inspection
- Behavioral baselining, analysis and anomaly detection/alerts
- DVR-like capabilities for forensics, including geo-positioning
- Carrier integration with cellular devices for anomaly detection, fraud/theft and cost management

REMEDIATE



- List & map devices on dashboard or directly into SIEMs.
- Interact with MDM & EMM assets for correlation & feedback on exceptions
- Rectify network segmentation via interactions with SOAR, FW and/or NAC systems
- Automate response & closure via collaboration with ITSM/ITSL & CMDBs

API Integrations

LOCH TECHNOLOGIES

LOGGING / ALERT

splunk>

elastic

McAfee

IBM QRadar

ALIEN VAULT
An AT&T Company

syslog

slack

T

WebHooks

ASSET MANAGEMENT

cisco Meraki

aruba
a Hewlett Packard Enterprise company

servicenow

vmware
Workspace ONE

mobileiron

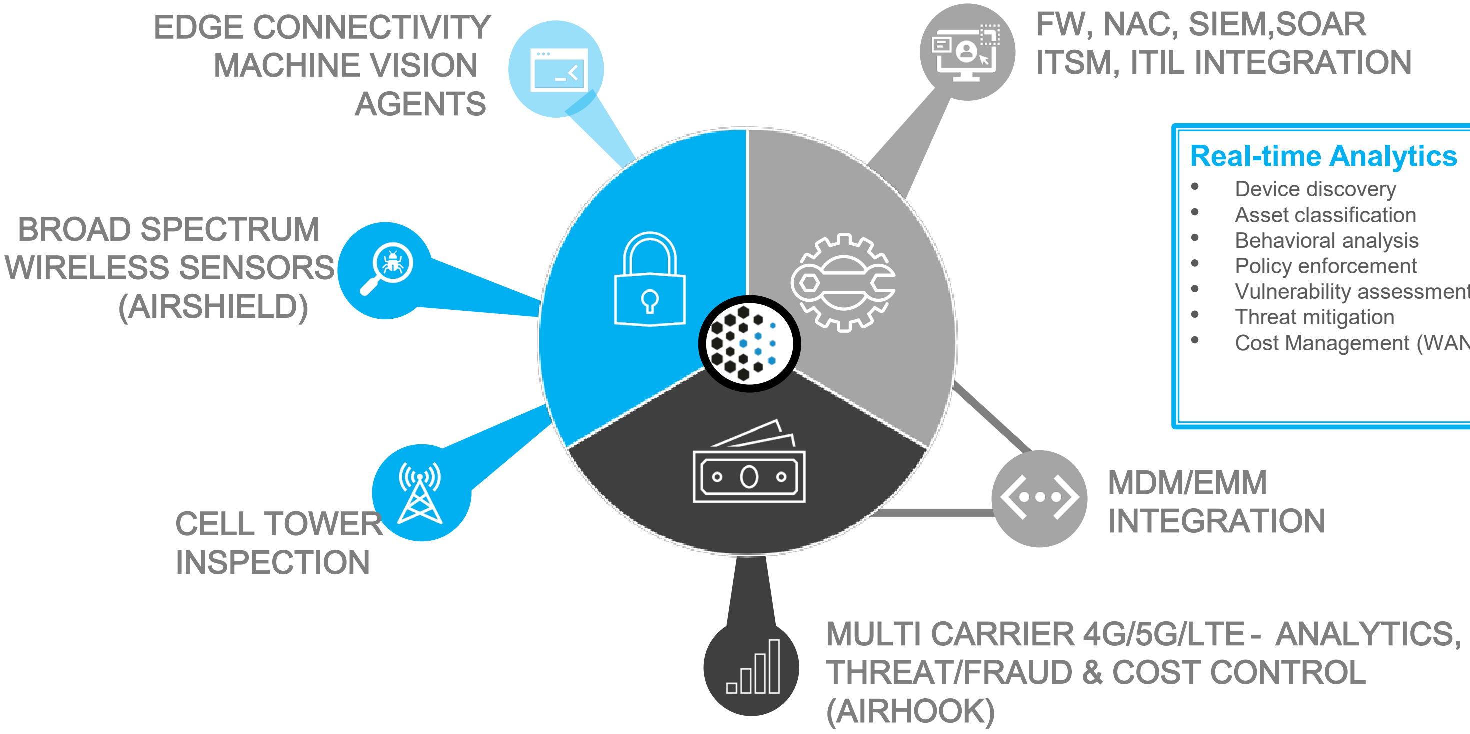
Quest KACE

CITRIX XenMobile

BlackBerry UEM

Additional integrations available

Wireless Machine Vision - See Everything



Real-time Analytics

- Device discovery
- Asset classification
- Behavioral analysis
- Policy enforcement
- Vulnerability assessment
- Threat mitigation
- Cost Management (WAN)

Resources

The Evolution of Security in 5G - https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf

What is 5G by Qualcomm Dr. Jon Smee -https://www.qualcomm.com/news/onq/2017/01/16/what-5g-101-seconds-dr-john-smee

Comparing WiFI 6 to 5G - https://www.intel.com/content/www/us/en/wireless-network/5g-technology/5g-vs-wifi.html

Thank You

Garry Drummond, CISSP, CWNA, CWSP
CEO
510-703-6149
gdrummond@loch.io