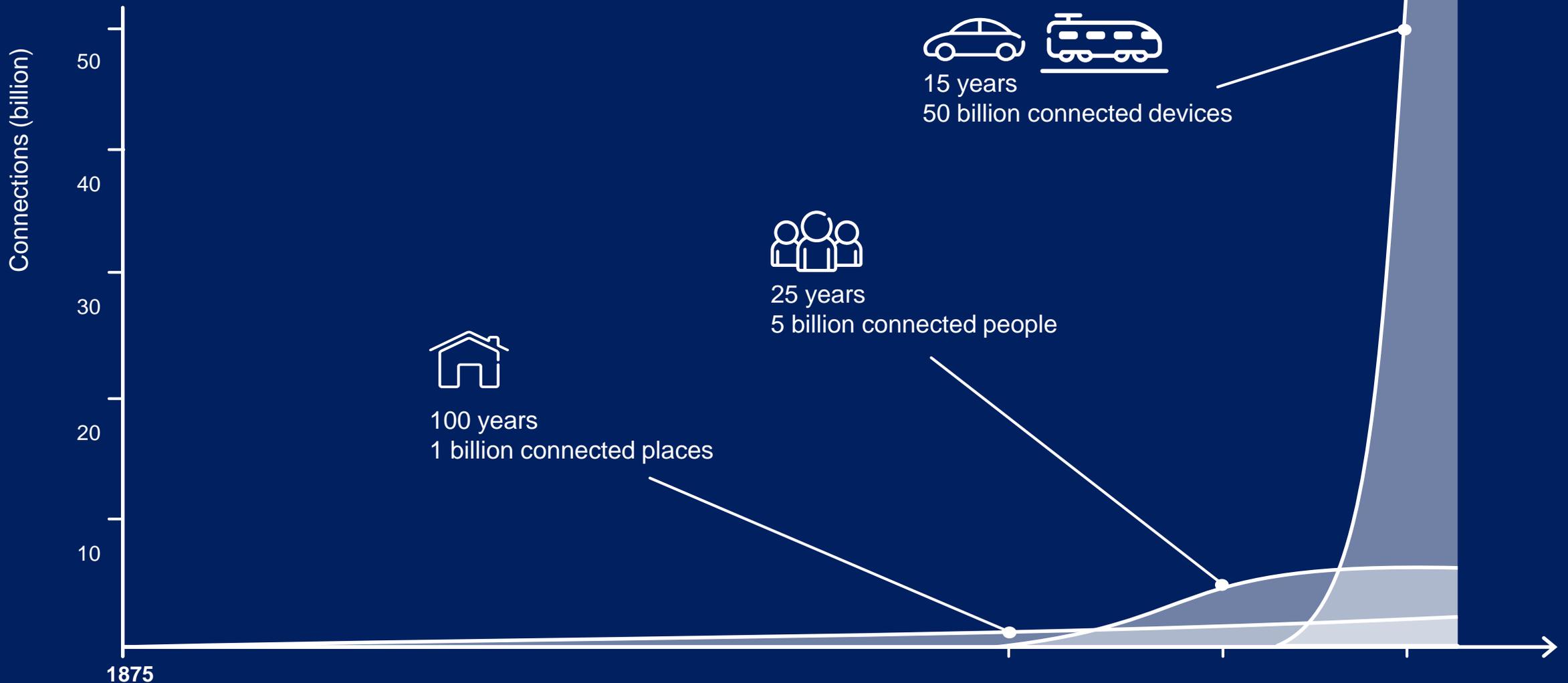# WELCHE TECHNOLOGIEN SIND NOTWENDIG, UM DIE KONNEKTIVITÄT & DATENSICHERHEIT ZU GEWÄHRLEISTEN

Frank Henschke, Ericsson AG

ERICSSON

THE NETWORKED SOCIETY
WHERE EVERY PERSON AND EVERY INDUSTRY IS EMPOWERED
TO REACH THEIR FULL POTENTIAL

Connections (billion)

50

40

30

20

10

15 years
50 billion connected devices

25 years
5 billion connected people

100 years
1 billion connected places

1875

MOBILITY GENERATIONS

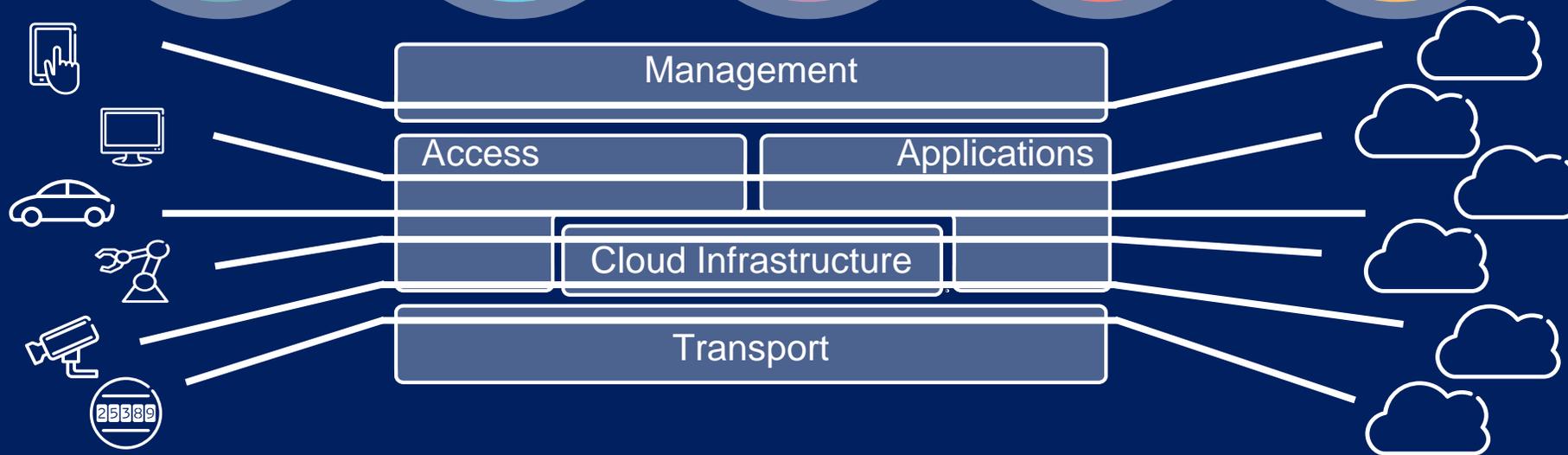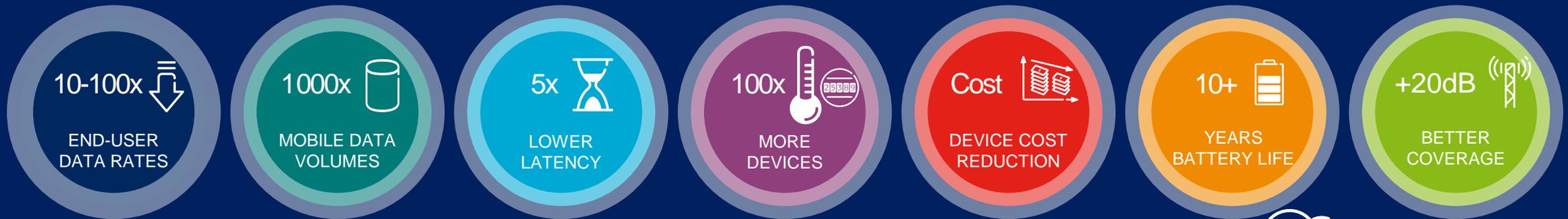| The foundation of mobile telephony	Mobile telephony for everyone	The foundation of mobile broadband	The evolution of mobile broadband	The Networked Society / IoT / IoE
1G NMT, AMPS, TACS	**2G** GSM, CDMA, PDC	**3G** WCDMA, HSPA	**4G** LTE	**5G** LTE enh. + NR
~1980	~1990	~2000	~2010	~2020
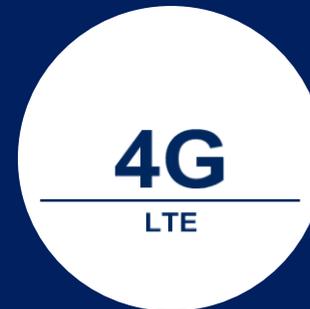
5G for non-limiting access to information and sharing of data anywhere and anytime for anyone and anything

The 5G network shall be a platform on which any future wireless application can be implemented

WHAT IS 5G – WHAT WILL IT BRING
A NETWORK FOR THE NETWORKED SOCIETY

10-100x
END-USER DATA RATES

1000x
MOBILE DATA VOLUMES

5x
LOWER LATENCY

100x
MORE DEVICES

Cost
DEVICE COST REDUCTION

10+
YEARS BATTERY LIFE

+20dB
BETTER COVERAGE

Management

Access

Applications

Cloud Infrastructure

Transport

One network supporting multiple use cases (Industries)

5G – CLASSES OF USE CASES

Massive MTC

SMART BUILDING

LOGISTICS, TRACKING AND FLEET MANAGEMENT

SMART METER

SMART AGRICULTURE

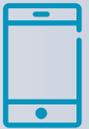CAPILLARY NETWORKS

Critical MTC

TRAFFIC SAFETY & CONTROL

INDUSTRIAL APPLICATION & CONTROL

REMOTE MANUFACTURING, TRAINING, SURGERY

Enhanced Broadband

Smartphones

Home, Enterprise, Venues, Mobile/Wireless/Fixed

Non-SIM devices

4k/8k UHD, Broadcasting, VR/AR,

LOW COST, LOW ENERGY
SMALL DATA VOLUMES
MASSIVE NUMBERS

ULTRA RELIABLE
VERY LOW LATENCY
VERY HIGH AVAILABILITY

4G

5G

SOME INTELLIGENT TRANSPORTATION USE CASES
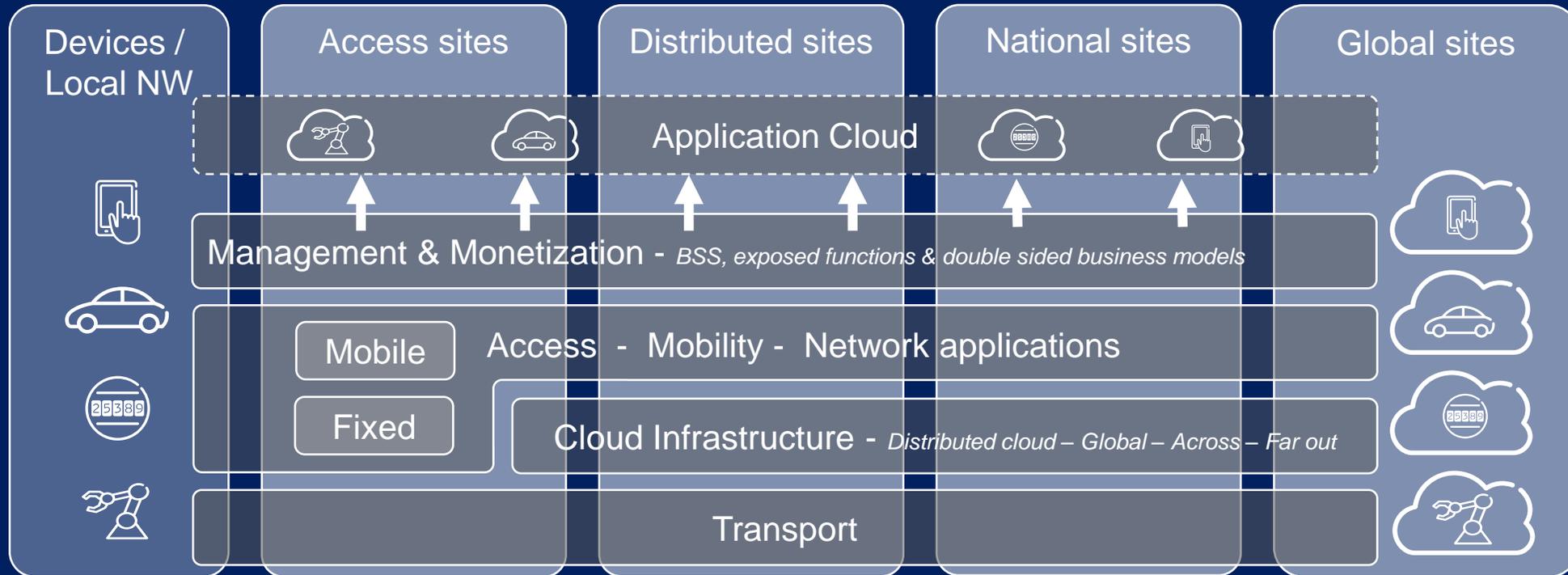

Cooperative perception

See-through video

Rescue Lane

Automated guided vehicles

Platooning

DYNAMIC 5G NETWORK

Devices / Local NW	Access sites	Distributed sites	National sites	Global sites

Application Cloud

↑ ↑ ↑ ↑ ↑ ↑

Management & Monetization - *BSS, exposed functions & double sided business models*

Mobile	Access - Mobility - Network applications
Fixed	Cloud Infrastructure - *Distributed cloud – Global – Across – Far out*

Transport

Flexible deployment of applications based on different needs

Green…   …and Secure

KEY ENABLING TECHNOLOGIES

5G

Management & Orchestration & Analytics & Exposure

Virtualization

VNF   VNF

Software Defined Networking (SDN)

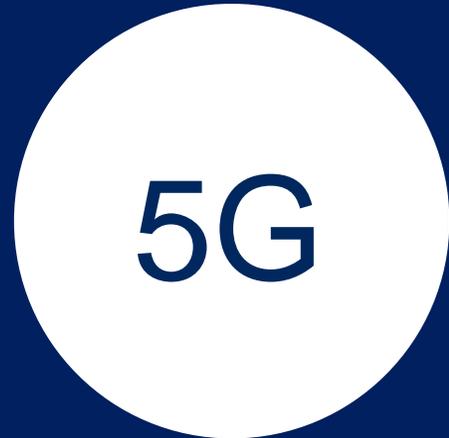### Distributed Cloud CORE & RAN

Network Slicing
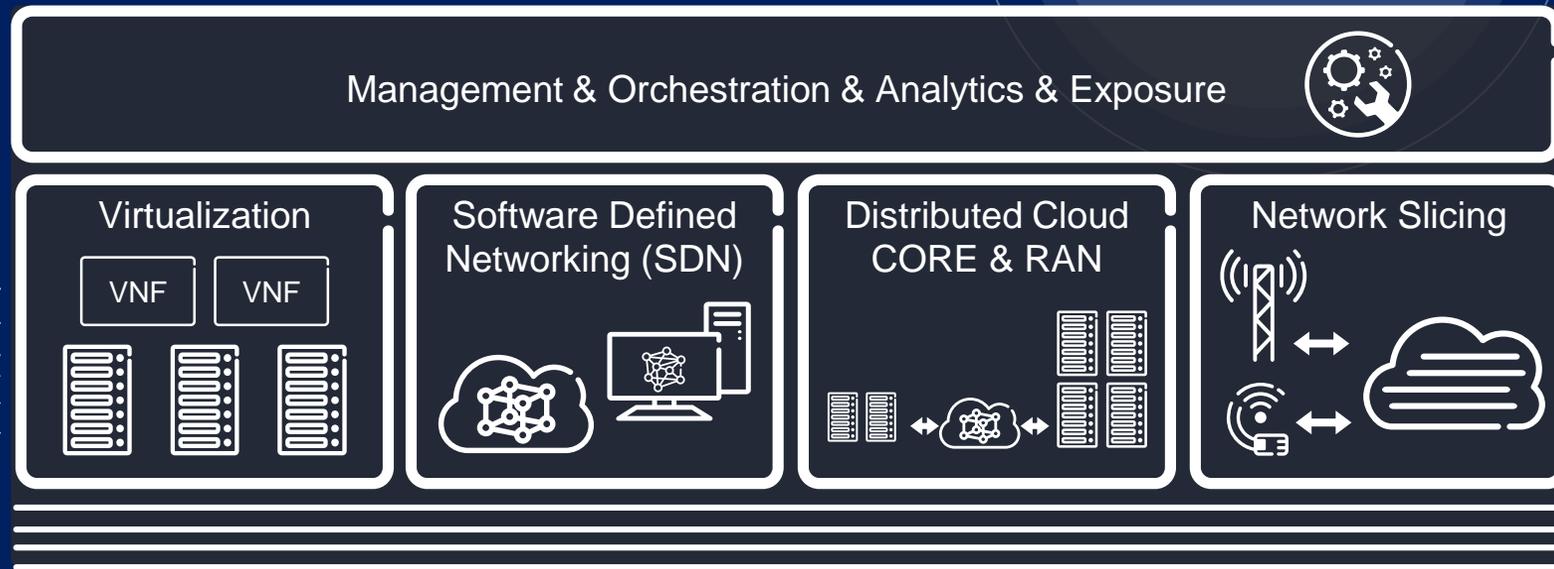
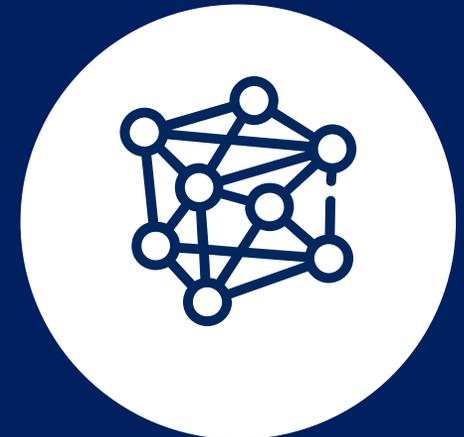# OUR EVOLVING SOCIETY

5G GAME CHANGER

DIGITALIZATION

SYSTEMS GO MOBILE

MISSION CRITICAL ICT INFRASTRUCTURE

5G

Enabler for more advanced use cases

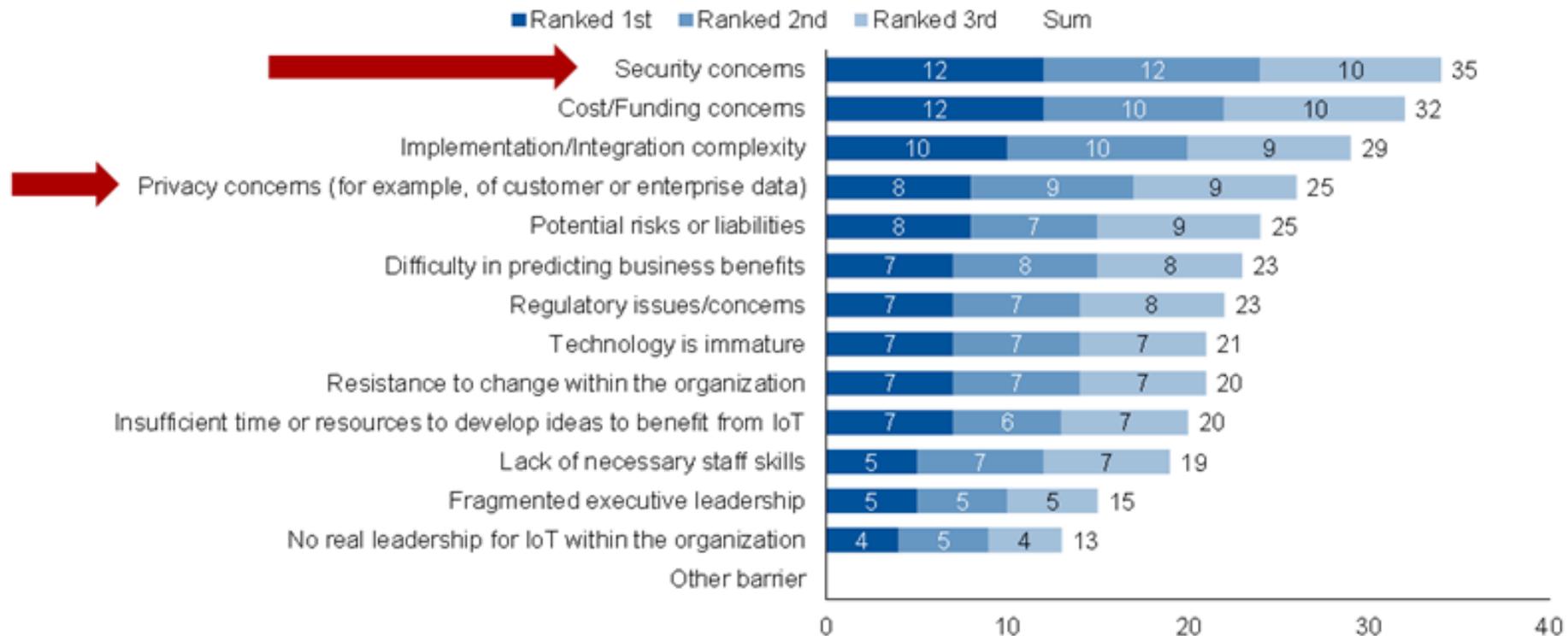Every company is a digital company

New attack vectors emerge

More value, more attacks

CONSEQUENCES CAN BE FATAL IF SECURITY IS NOT ENSURED

MAIN IOT CONCERN IS SECURITY

Top 3 Barriers to IoT Success

■Ranked 1st ■Ranked 2nd ■Ranked 3rd   Sum

Barrier	Ranked 1st	Ranked 2nd	Ranked 3rd	Sum
Security concerns	12	12	10	35
Cost/Funding concerns	12	10	10	32
Implementation/Integration complexity	10	10	9	29
Privacy concerns (for example, of customer or enterprise data)	8	9	9	25
Potential risks or liabilities	8	7	9	25
Difficulty in predicting business benefits	7	8	8	23
Regulatory issues/concerns	7	7	8	23
Technology is immature	7	7	7	21
Resistance to change within the organization	7	7	7	20
Insufficient time or resources to develop ideas to benefit from IoT	7	6	7	20
Lack of necessary staff skills	5	7	7	19
Fragmented executive leadership	5	5	5	15
No real leadership for IoT within the organization	4	5	4	13
Other barrier				

Q. What are the three greatest barriers to your organization's IoT activities?
N=2,539. Multiple responses were allowed

Source: Gartner Survey Analysis: 2016 Internet of Things, Backbone Survey (G00317142)
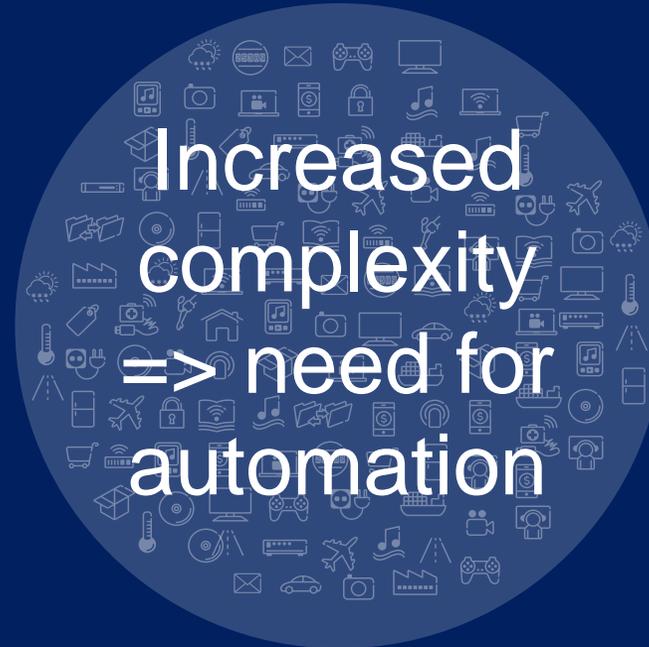
9   ©2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner.

IOT CHARACTERISTICS PUT NEW DEMANDS ON SECURITY
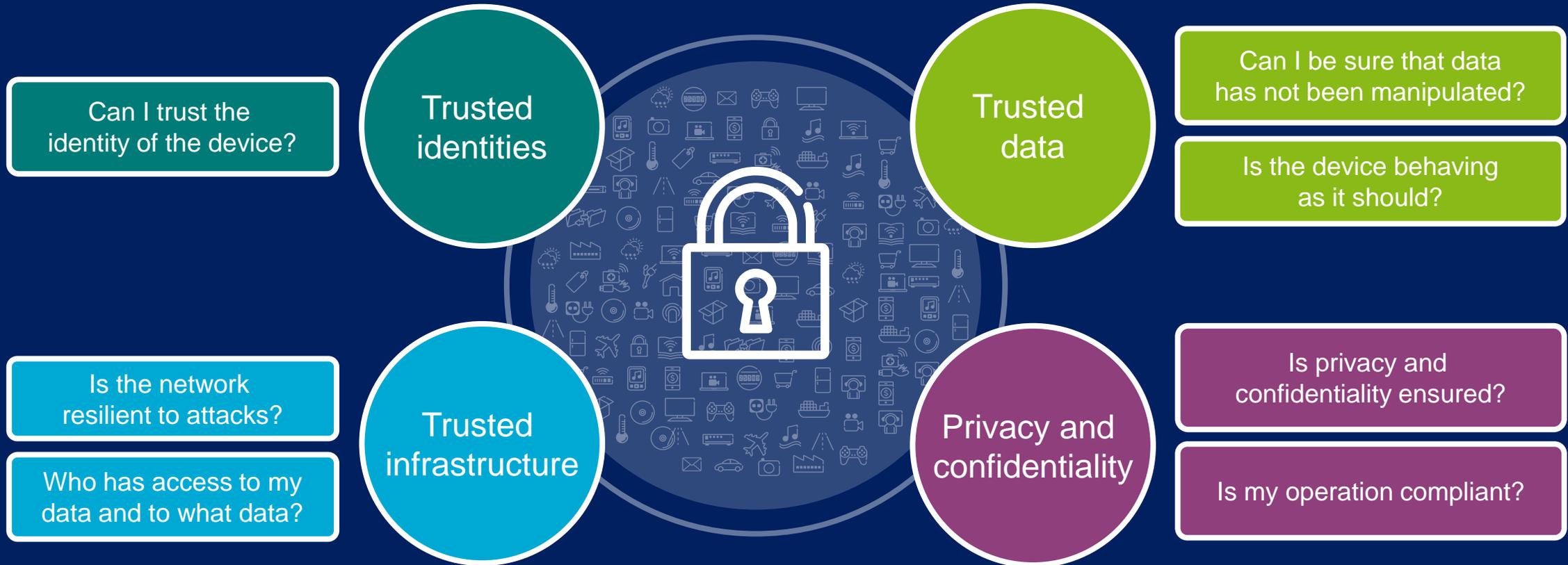
Decisions taken based on data

Increased complexity => need for automation

Ecosystems with many stakeholders

Volume of devices

Devices Connectivity Platforms Applications Users

End-2-end security

IOT SECURITY CHALLENGES
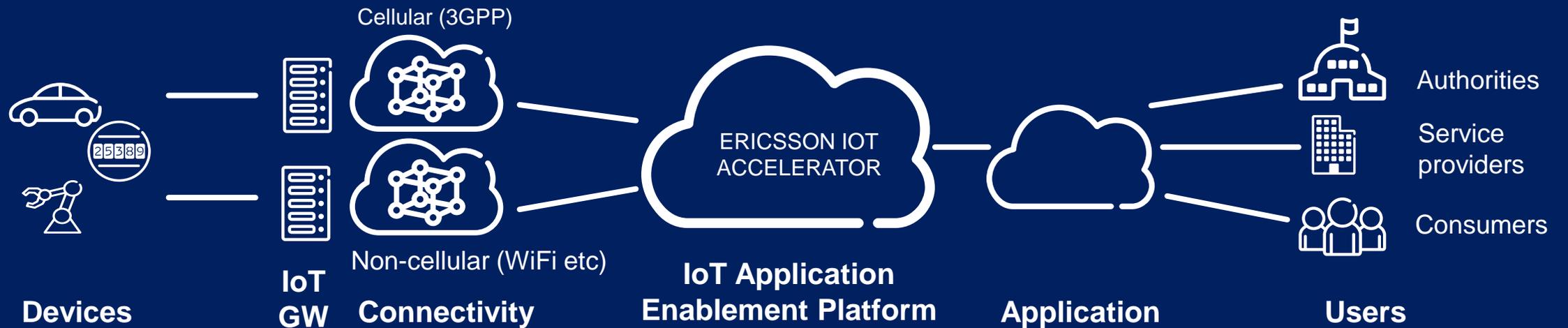
Can I trust the identity of the device?

Trusted identities

Can I be sure that data has not been manipulated?

Trusted data

Is the device behaving as it should?

Is the network resilient to attacks?

Trusted infrastructure

Who has access to my data and to what data?

Privacy and confidentiality

Is privacy and confidentiality ensured?

Is my operation compliant?

KEY PRINCIPLES OF IOT SECURITY

1. Identities of IoT devices must be trusted

2. Services should always be available

3. Confidentiality of IoT communication must be protected

4. All access to information and data shall be authorized

5. Integrity of IoT data must be ensured

6. When IoT data is enriched with personal data, privacy must be protected