12th InfoCom July 2022

“Trust” in the Digital World

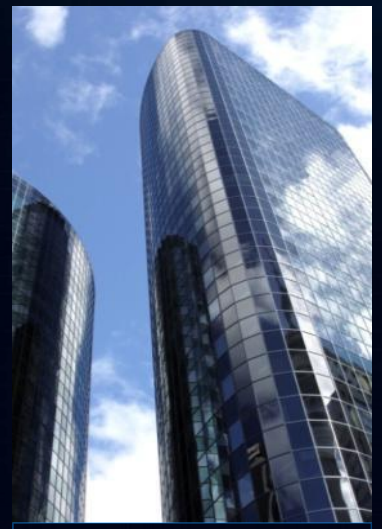
Ioannis Solomakos - CSO, Huawei South Balkans

HUAWEI

Leading Global Provider of ICT Infrastructure and Smart Devices

194,000
(R&D 96,000)
EU: 13000
EU R&D: 2400
Employees

No. 2
Largest R&D Investor



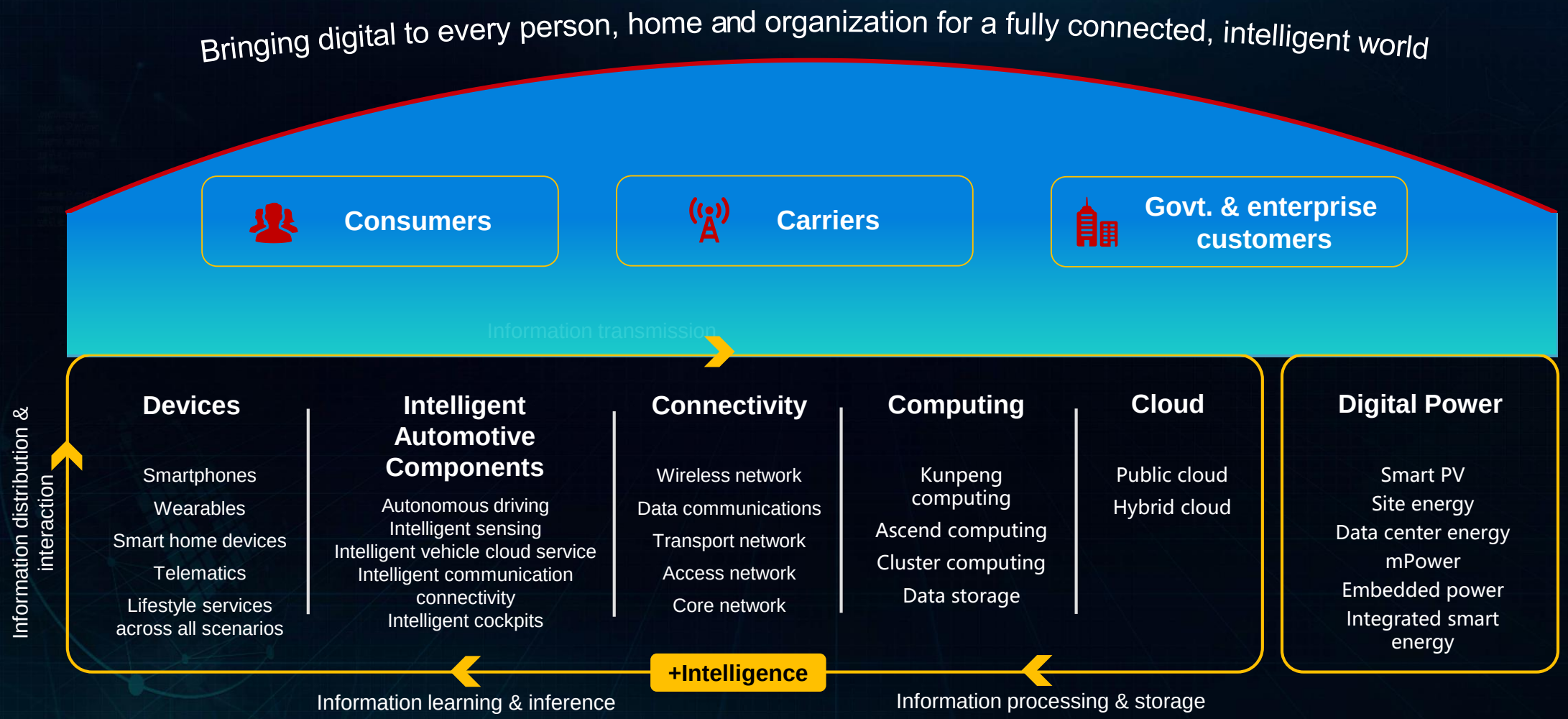
No. 8
Most Innovative Company

No. 9
Most Valuable Brand

170+
Countries

$100 BIL.
Global Revenue 2021

Provide ICT products – solutions - services



Intelligent Digital World

Ubiquitous connectivity

Pervasive intelligence

Personalized experience

Digital platform

Cyber Security Challenges

Escalating threats

- Security risks faced by new services (5G, cloud, and smart devices)
- Increasing attack sources, attack paths, and attack traffic

Vulnerable networks

- Open network architecture
- Virtualization & cloudification
- Unexplainability of AI

Open source risks

High-value assets

- Industry applications (governments, energy, public safety, and finance)
- Terminal applications (home, individuals, and IoT)

E2E security assurance system

Governance, development, supply, delivery, and verification

Secure and resilient products and solutions

5G security, industry security, terminal security, and HiSec

Security engineering capabilities and technologies

Software engineering, security engineering, security technologies, security architecture, and platform/component security

Standards, ecosystem, and cooperation

3GPP, CC, bug bounty, and partners

Safeguarding Secruity in the Digital World

Intelligent Digital World

Ubiquitous connectivity

Pervasive intelligence

Personalized experience

Digital platform

Cyber Security becomes a top priority

EU institution

2021: Six European Union institutions were hacked part of the SolarWinds supply chain attack.

Italian Energy Mining Company

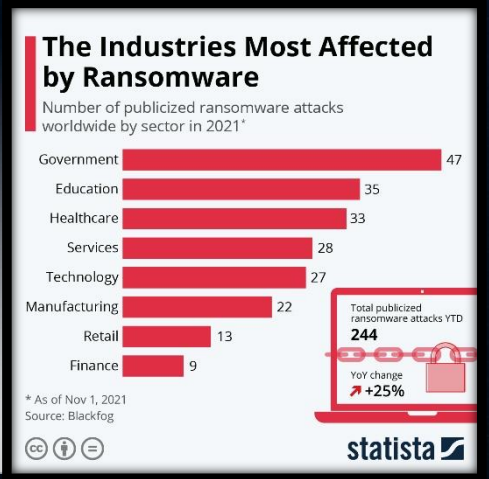
2018:10% data was damaged by Shamoon's variation attack

EMA(European medicines agency)

2021: hackers manipulated leaked coronavirus vaccine data

US Fuel Pipeline Operators

2021: Forced to shut down key oil supplying networks of its eastern coastal states by attack in US



E2E security assurance system

Governance, development, supply, delivery, and verification

Secure and resilient products and solutions

5G security, industry security, terminal security, and HiSec

Security engineering capabilities and technologies

Software engineering, security engineering, security technologies, security architecture, and platform/component security

Standards, ecosystem, and cooperation

3GPP, CC, bug bounty, and partners

Safeguarding Secruity in the Digital World

EU Cyber Attacks Trends

Cyber Security Threats are on the rise.

Cyber Security attacks continue to increase in terms of:

- Numbers
- Vectors
- Impact

Increased online presence

Traditional transitions to Cloud

Advanced interconnectivity

Emerging tech's exploits (AI)

Hybrid Office Model

"New Normal" exploits

2020-2022 COVID-19 pandemic increased these ever growing trends

EU Cyber Threat Landscape

- Ransomware became the prime threat for 2020-2021.
- Governmental organizations have stepped up their game.
- Cybercriminals are increasingly motivated by monetization
- Traditional Malware attacks decline observed in 2020 & 2021.
- The volume of crypto-jacking infections is record high.
- COVID-19: the dominant lure in campaigns for e-mail attacks.
- Surge in healthcare sector related data breaches.
- Traditional DDoS campaigns are targeted, persistent and multi-vector.
- IoT along with mobile networks creates a new wave of DDoS attacks.
- Spike in non-malicious incidents, as the pandemic increased human errors

“Trust”… no more?

Physical Network Era:

Trust all internal traffic by default. Provide unrestricted access inside the network

Cloud Era:

No Traffic is inherently “trusted”. Access to all data or assets must be approved by policy

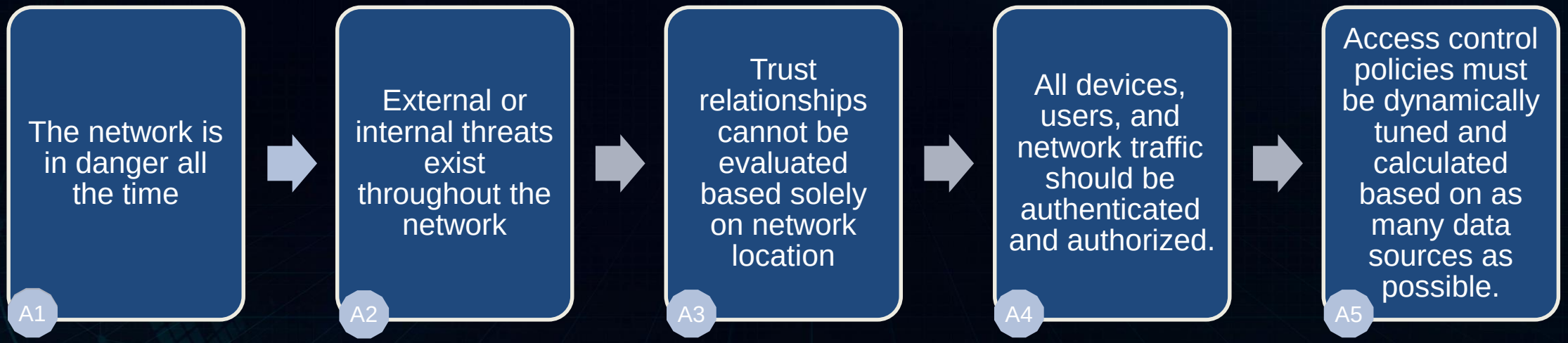
The word “Trust” has become a vulnerability that can be exploited by malicious actors

“Trust” is an emotional term that should not be applicable to the security of digital systems.

Hello… “Zero Trust”

The traditional border defense model that builds trust based on network boundaries cannot meet the security requirements of the current IT environment.

- There is no longer a clear **boundary** between trusted and untrusted devices (such as cloud computing).
- No more trusted or untrusted **networks** (e.g. wireless networks/mobile computing)
- No more trusted or untrusted **users** (such as intranet attacks/privilege abuse)



Zero-Trust ABC principle: Assume nothing, Believe nobody, Check everything

“Zero Trust” Implementation Ecosystem

Person & Entity

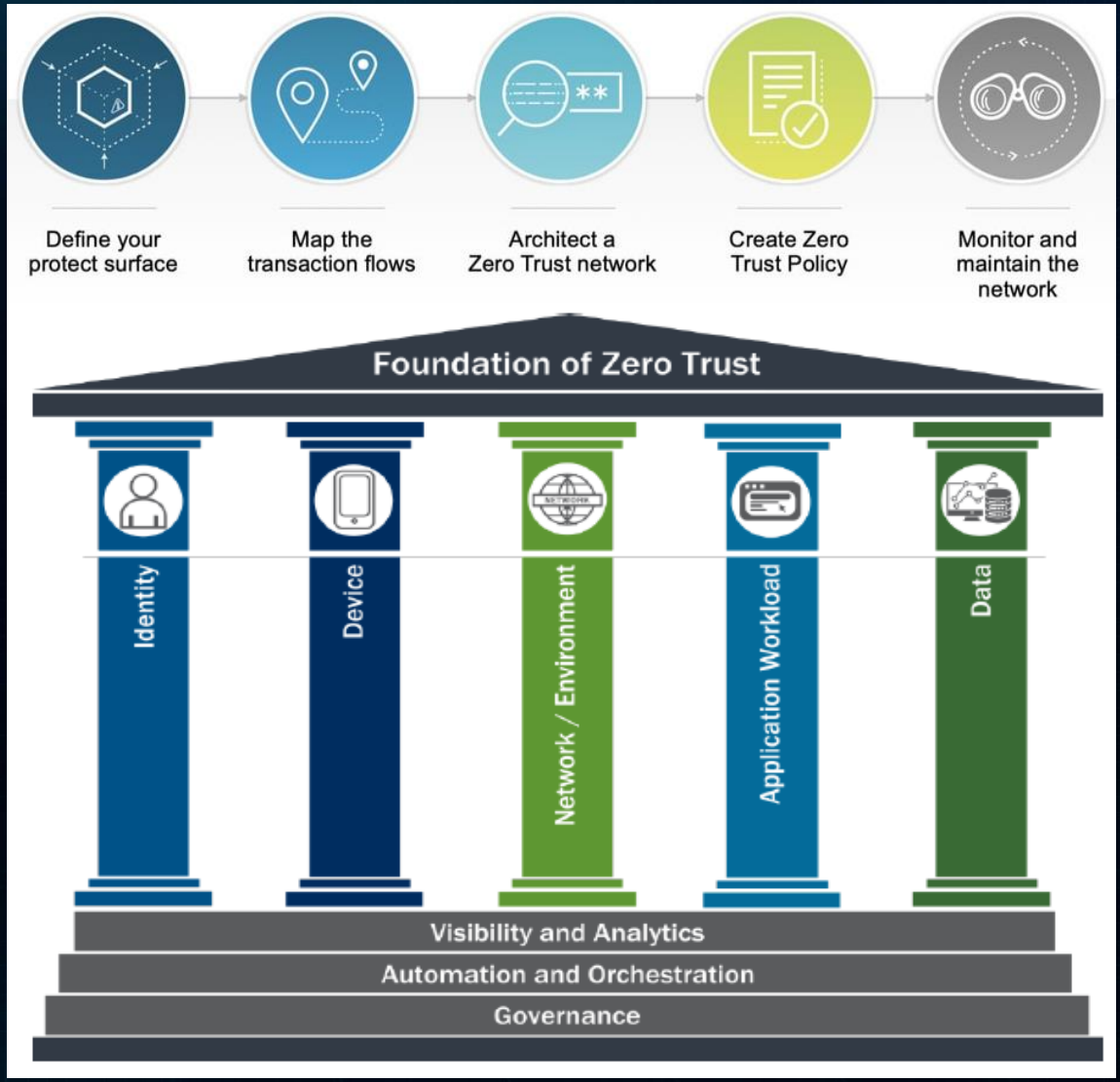
Hardware & IoT Device

Network & Com/s Medium

Program & Service

On-premise & Cloud

Data Flow & Protection



Tools for Creating Trust in a Zero Trust environment: Common Standards

Industry Wide Standards

Common Criteria

EUCC

CC

Baseline Security Controls

Cyber Security Assessment Mechanisms

Assurance Schemes

GSMA

Network Equipment Security Assurance Scheme (NESAS)

- Standardized Cyber Security Assessment Mechanism involving Customers, Regulators, Vendors, Partners.

Assurance Specifications

3GPP A GLOBAL INITIATIVE

NESAS Security Assurance Specifications (SCAS)

- Security requirements and test cases for the security evaluation of network equipment

5G Cyber Security Knowledge Base

Common Standards generate Trust in a Zero Trust ecosystem

Tools for Creating Trust in a Zero Trust environment: Certifications

270+Security Certificates of Product

Common Criteria
ICT, 40+

FIPS 140-2
Encryption
Modules, 20

PCI
Payment Card
Industry, 14

CSA
Cloud Security, 3

ePrivacy
GDPR based, 1

Certifications of Security management system

ISO27001 Information
Security Management

ISO9001 Quality
Management System

ISO28000 Supply Chain
Security Management

ISCCC Qualification of
Information Security

Actively improve security standard

- 17 chairman or vice-chairman positions
- 3GPP SA3 in 2019: No.1 contributor, 385 proposals accepted, 5G security architecture proposal accepted

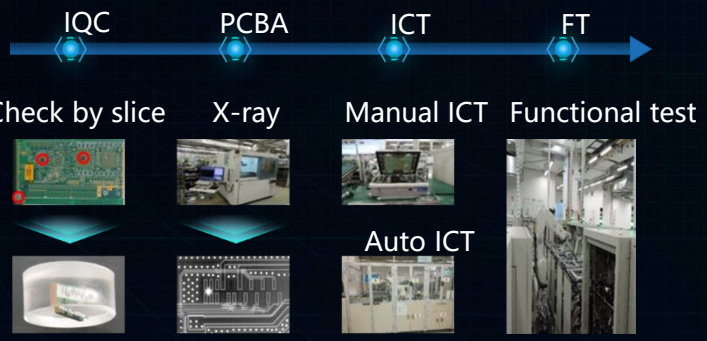
Certifications generate Trust in a Zero Trust ecosystem

Tools for Creating Trust in a Zero Trust environment: Supply Chain Security

Security responsibilities are shared by different parties in the entire Production and Supply Chain: Everyone should do their part…

Cyber security baselines built into supply chain process

Manage product supply/ manufacturing design				Manage customer supply (project supply/PO supply)		
Planning	PO	Logistics	Manufac turing	Reverse	Supply operations	Supply networks



Risk management, end-to-end traceability, infrastructure management and access control

Prevent hardware implantation

Tools for Creating Trust in a Zero Trust environment: Security Transparency

Cyber Security Transparency Centers: An Open Collaborative Exchange Platform towards Stakeholders

HCSTC Brussels：Communication, Innovation and Verification




Myths & Facts about “Zero Trust”

Myths	Facts
Zero Trust is all about identity management and device security.	Enhancees the Security posture and prevents the exfiltration of sensitive Data
You have to rip and replace everything to achieve it.	Compliance with applicable standards and regulations (e.g. HIPAA, PCI-DSS)
Zero trust is difficult to implement and there is only one way to do it	Benefits integration of new tech (Cloud, IoT, AI) to existing ICT environment
Zero trust implementation hurts network availability.	Boosts Data, Assets, Application & Services overall Risk Management

A “Zero Trust” Approach is the best way to build Trust

Technical measures

- Security Verification via Penetration Testing & Source Code Validation
- Supply Chain Traceability
- Justify in depth: Security Architecture & Security by Design
- Embed Strict Access Control & Security Protocols for third parties
- Follow Standards & Obtain Certifications

Non-Technical measures

- Transparency towards secure production & supply chain processes
- Robust organizational measures
- ISMS, Cyber Security Awareness Trainings, etc.

Zero-Trust ABC principle: Assume nothing, Believe nobody, Check everything


Thank you
www.huawei.com
HUAWEI