IoT Security: Establishing Frameworks to Protect Consumers

May 19
10:00 AM CT

Sponsored by psacertified™

PARKS ASSOCIATES

Speakers

Anurag Gupta
Director Business Development, Platform Security Architecture
Arm

Carlos Serratos
Senior Director of Strategy, Policy and Advocacy
Brightsight

Hector Tejero
IoT Solutions Architect
Arrow Electronics

Patrice Samuels
Senior Analyst
Parks Associates

Agenda

- ✓ Why device manufacturers must rethink their approach to connected device security.
- ✓ Key ways in which connected device security must evolve.
- ✓ Important considerations for implementing new security measures.
- ✓ How PSA certification addresses device security

Webcast Replay

Webcast Recording Playback

Parks Associates and PSA Certified invite you to view and listen to the webcast recording.

Click link to view recording:
https://attendee.gotowebinar.com/recording/406045653132994817

Why device manufacturers must rethink their approach to connected device security

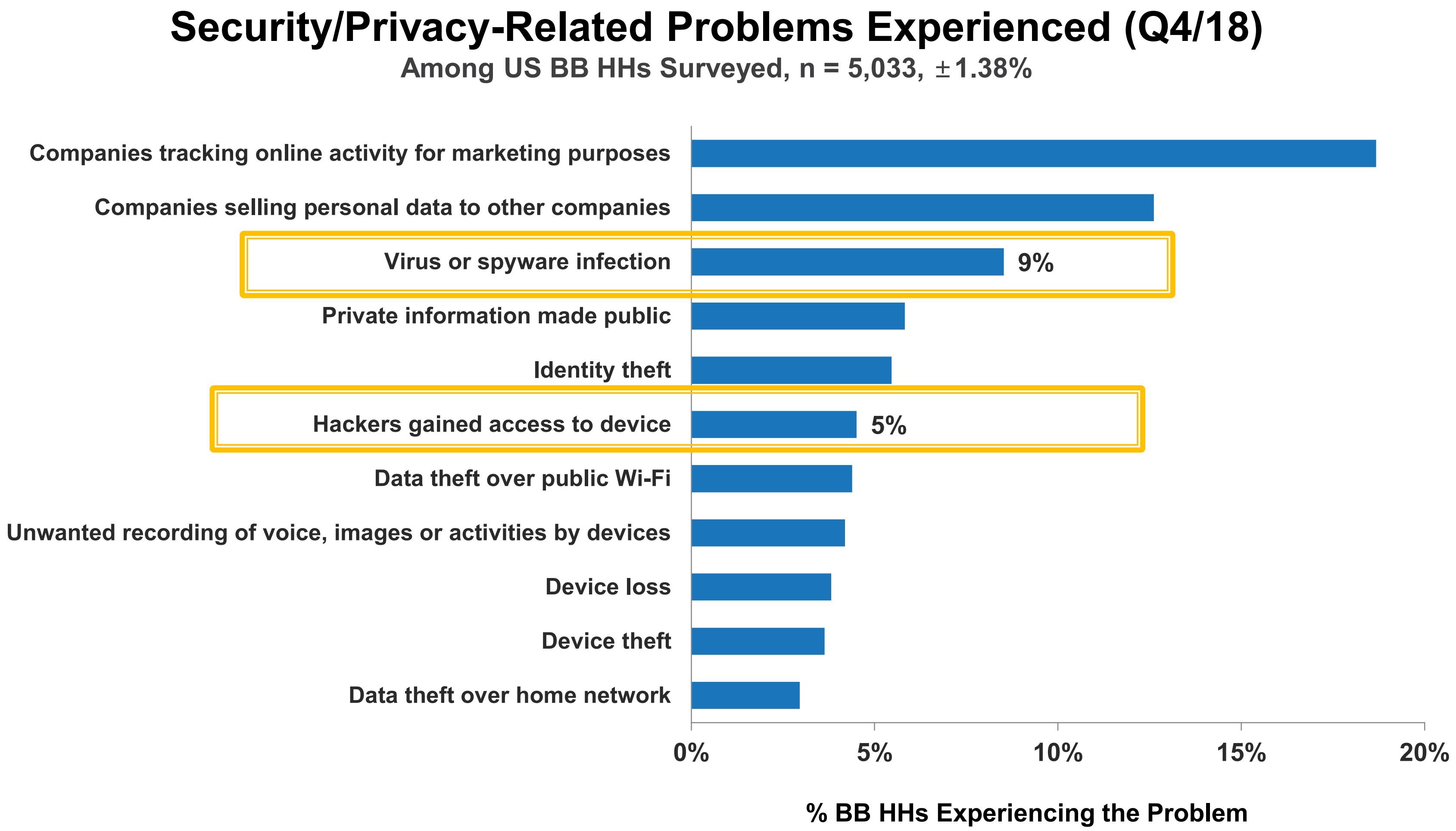
Device and network security has evolved.

- **Connected devices are built with baseline security**
- **Broadband service providers offer home network security**

- **Consumers have adopted data security services**
  - 63% have at least one data security service
  - 79% of smart home device owners use at least one data security service

- **Connectivity protocols mandate security**
- **The FCC has issued guidelines on security**

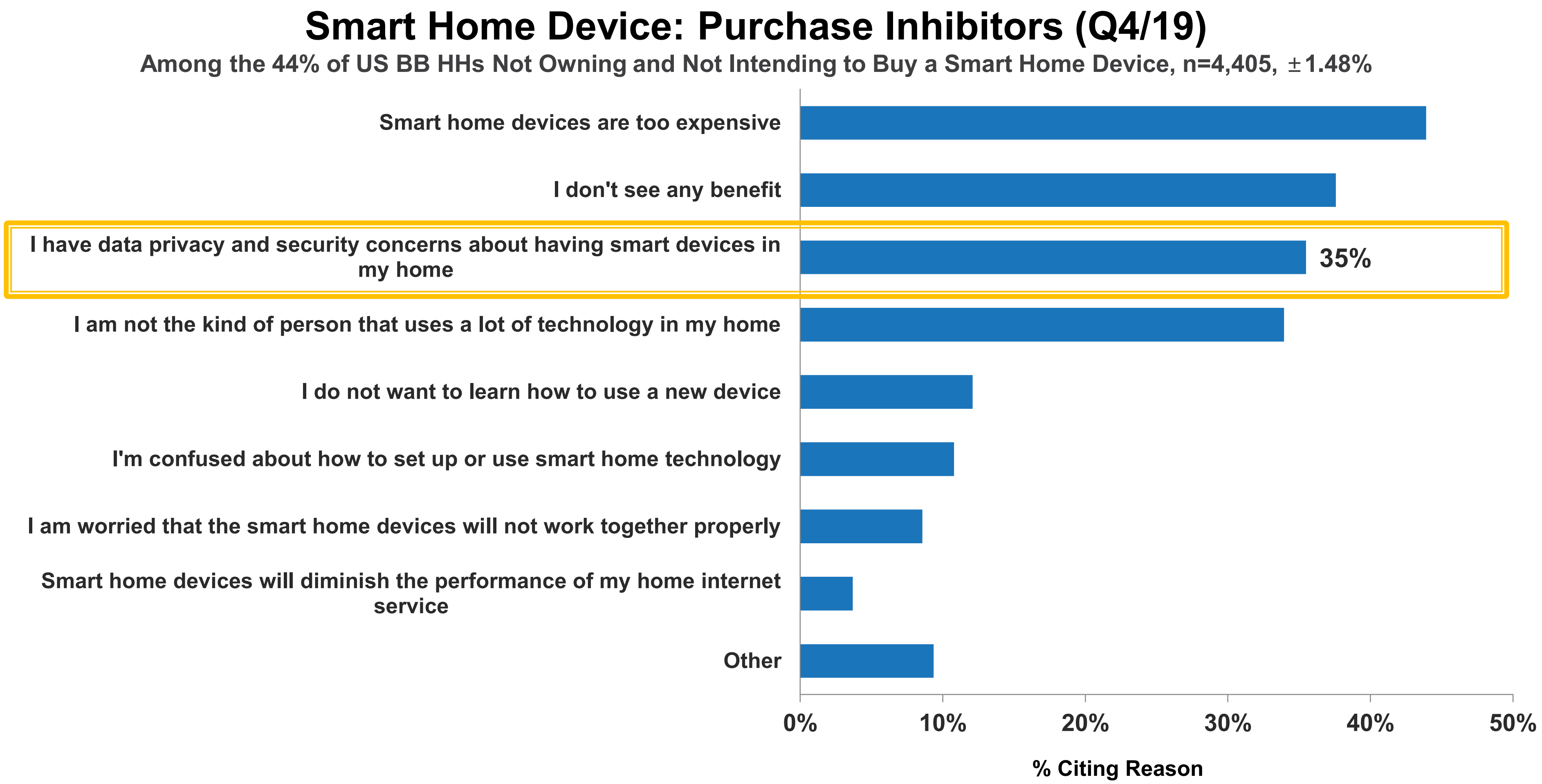
Device breaches remain a concern.



“T8105. Over the past 12 months, which of the following security or privacy related problems have you experienced?" | Asked of a Subgroup of 5,033 US BB HHs | Source: American Broadband Households and Their Technologies Q4 2018 | N=10,050, ±0.98% | © 2019 Parks Associates

35% of US broadband households have experienced a security breach.

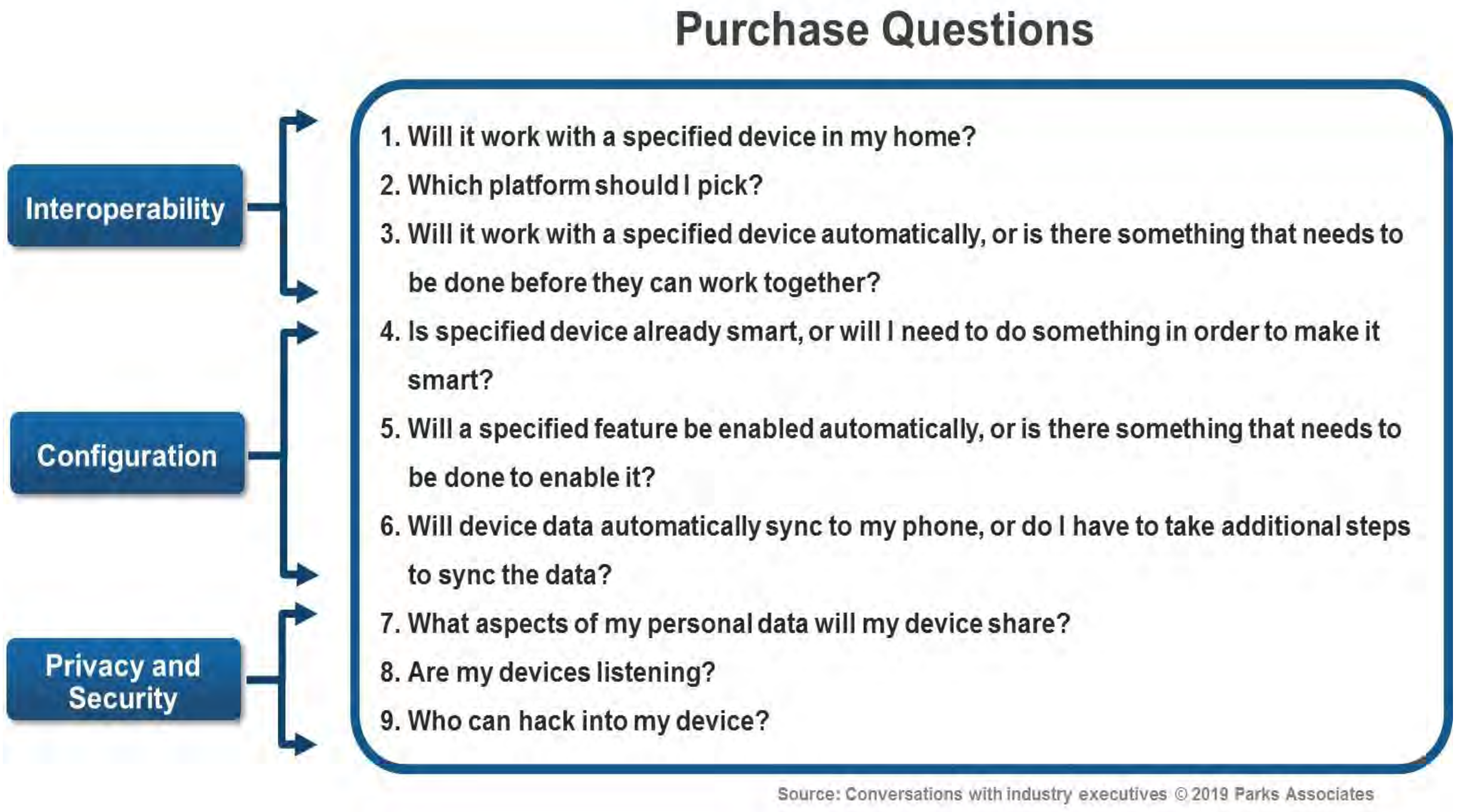
Effects of device breaches.



"ST2680. Why don't you now own or intend to purchase any smart home devices in the next 12 months?"
Source: American Broadband Households and Their Technologies Q4 2019| N=10,021 ±0.98% | © 2020 Parks Associates

Consumers are apprehensive about purchasing smart home devices, and reports about data and device breaches can adversely impact sales for all device makers.

Consumers have questions about device security before they buy.

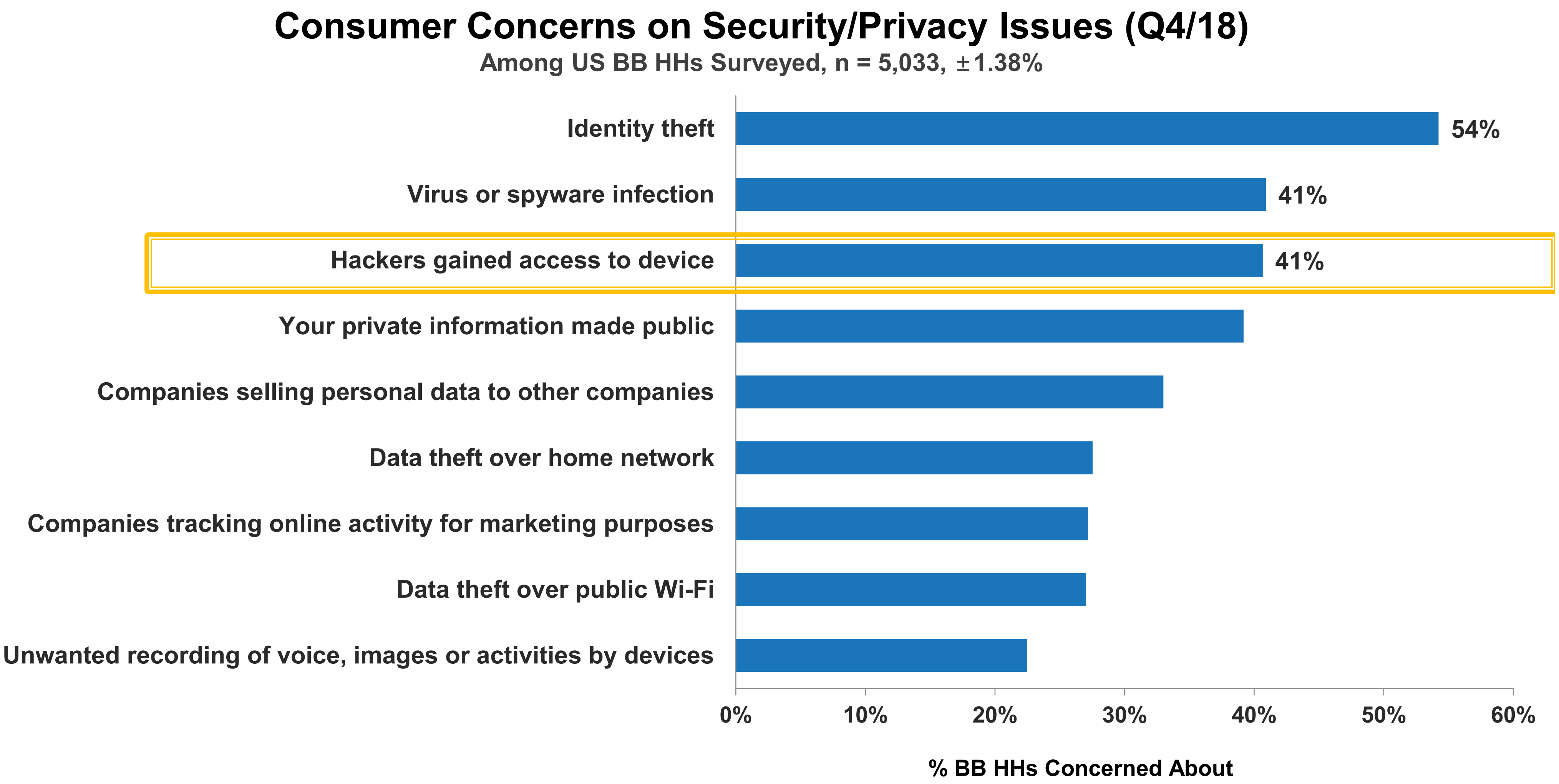


Purchase Questions

1. Will it work with a specified device in my home?
2. Which platform should I pick?
3. Will it work with a specified device automatically, or is there something that needs to be done before they can work together?
4. Is specified device already smart, or will I need to do something in order to make it smart?
5. Will a specified feature be enabled automatically, or is there something that needs to be done to enable it?
6. Will device data automatically sync to my phone, or do I have to take additional steps to sync the data?
7. What aspects of my personal data will my device share?
8. Are my devices listening?
9. Who can hack into my device?

Source: Conversations with industry executives © 2019 Parks Associates

Concerns about hackers are relatively high.

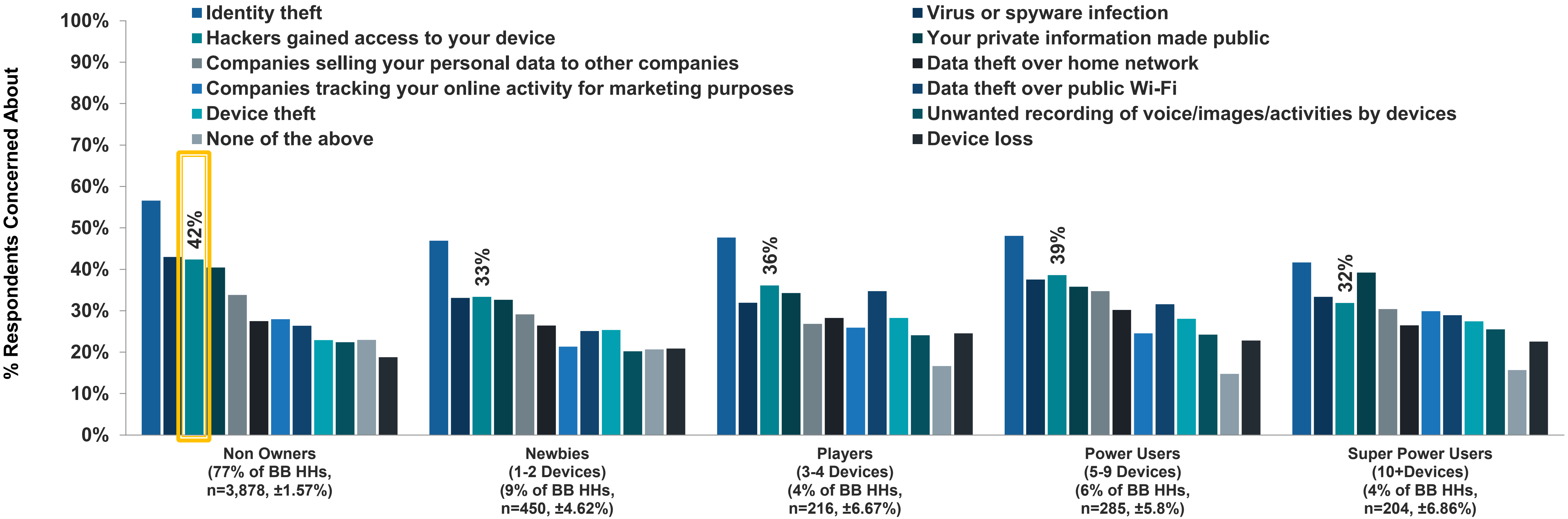


"T8105B. Which of the following security or privacy related problems are you most concerned about?" | Asked of a Subgroup of 5,033 US BB HHs
Source: American Broadband Households and Their Technologies Q4 2018 | N=10,050, ±0.98% | © 2019 Parks Associates

Concerns are higher among non-owners.

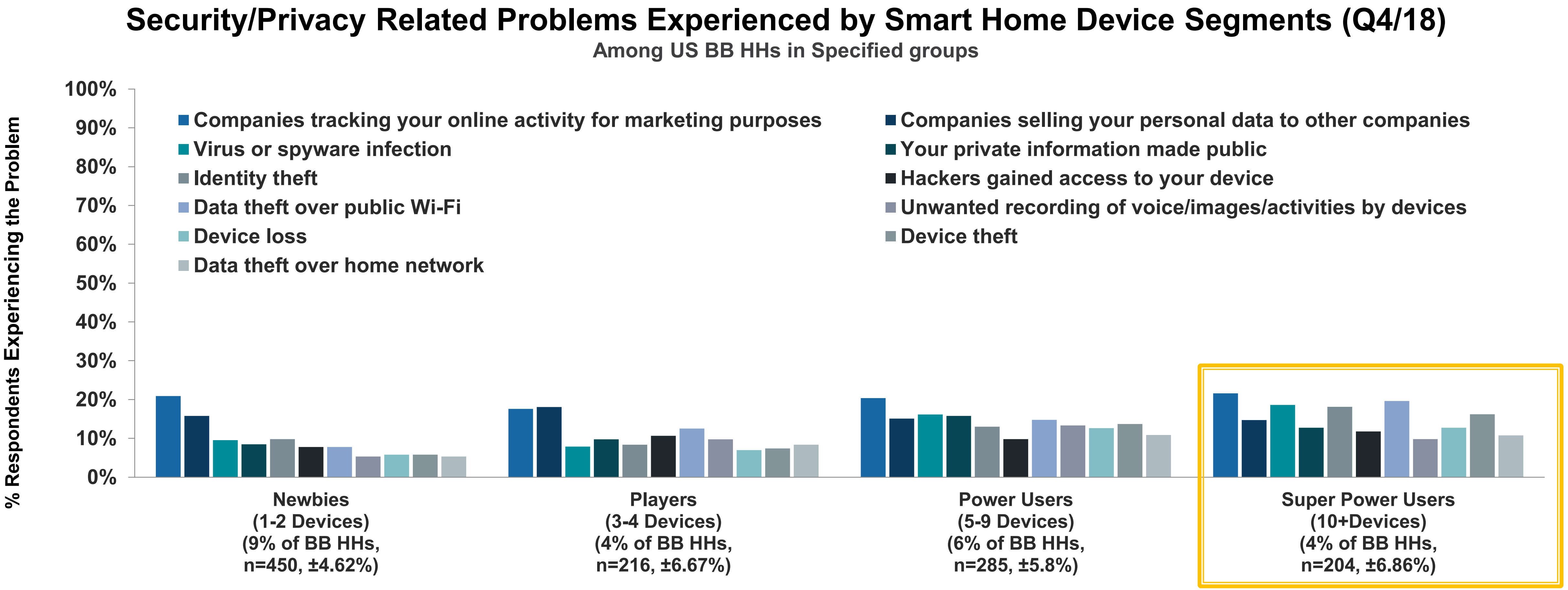
Consumer Concern on Security/Privacy Issues by Smart Home Device Segments (Q4/18)

Among US BB HHs in Specified Groups



"T8105B. Which of the following security or privacy related problems are you most concerned about?" | Asked of a Subgroup of 5,033 US BB HHs
Source: American Broadband Households and Their Technologies Q4 2018 | N=10,050, ±0.98% | © 2019 Parks Associates

Breaches are higher among Super Power Users.



“T8105. Over the past 12 months, which of the following security or privacy related problems have you experienced?" | Asked of a Subgroup of 5,033 US BB HHs | Source: American Broadband Households and Their Technologies Q4 2018 | N=10,050, ±0.98% | © 2019 Parks Associates

Poll Question #1

1. **What do you think is the biggest barrier to developing robust device security?**

   a. High cost

   b. Inexperienced product developers

   c. Fragmented regulation/standards

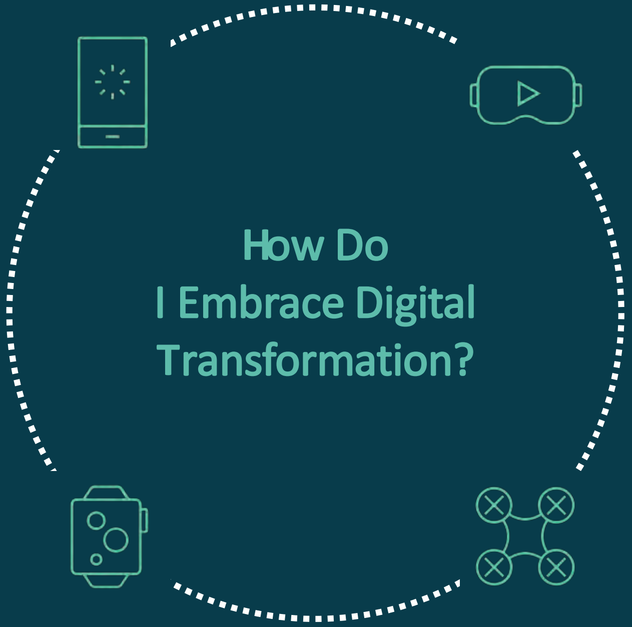
   d. Security has not been a high priority

Hector Tejero

IoT Solutions Architect

Arrow Electronics

Businesses Face Challenges



How Do
I Embrace Digital
Transformation?

Unleashing digital transformation is the common denominator of successful companies in the last 10 years

While not losing sight of 'business as usual'

Product Development Challenges

- Multiple regulations
- New manufacturing technologies
- Fragmented frameworks
- Inconsistent security

Financial Challenges

- High failure cost
- Total cost of ownership
- Liability
- Data breaches can put companies out of business

Consumer Challenges

- USP / differentiation
- New revenue streams

Businesses Face Challenges

How Do
I Embrace Digital
Transformation?

Unleashing digital transformation is the common denominator of successful companies in the last 10 years

While not losing sight of 'business as usual'

Security is at the heart of all these concerns

Product Development Challenges

- Multiple regulations
- New manufacturing technologies
- Fragmented frameworks
- Inconsistent security

Financial Challenges

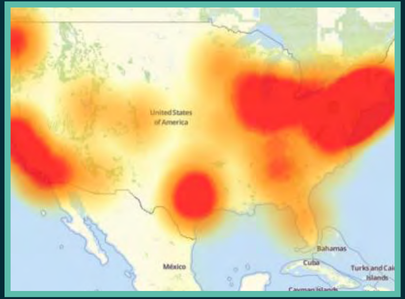
- High failure cost
- Total cost of ownership
- Liability
- Data breaches can put companies out of business

Consumer Challenges

- USP / differentiation
- New revenue streams

Data Breaches

2015: J eep hack[1]

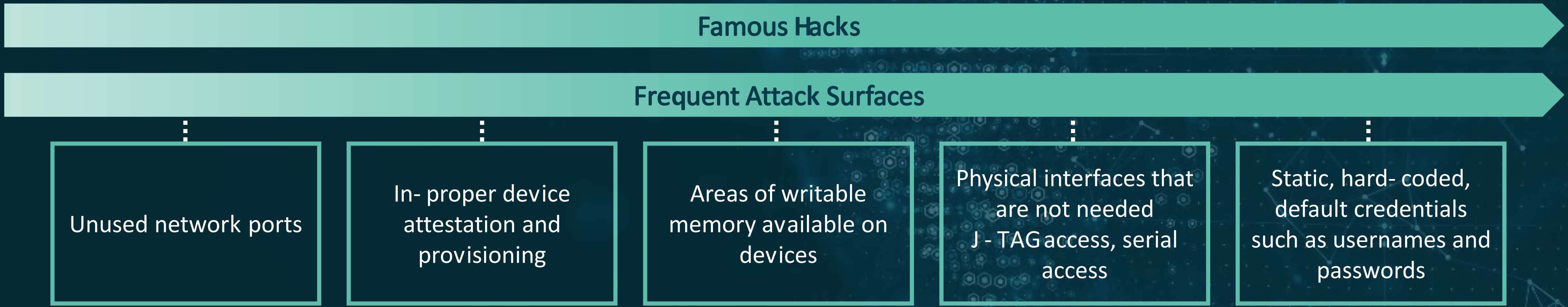


2016: Mirai Botnet[2]

2017: Casino Fishtank

2018: Bluetooth lock[3]

2019: Mississippi Camera



Famous Hacks

Frequent Attack Surfaces

Unused network ports

In- proper device attestation and provisioning

Areas of writable memory available on devices

Physical interfaces that are not needed J - TAG access, serial access

Static, hard- coded, default credentials such as usernames and passwords

Image sources:

[1]www.wired.com/2015/07/hackers- remotely- kill- jeep- highway/ | [2]krebsecurity.com/tag/mirai- botnet | [3]www.bbc.co.uk/news/technology- 44457166

Security Is More Important Than Ever

Skipping Security Poses Significant Risks to your Business

Your reputation is damaged due to reports of hacking affecting your devices

Businesses struggle to exist after successful hacks take place

The attack surface continues to grow, with more devices joining the network

Regulation comes into effect in your key geographies and you’re deemed non- compliant

IoT hacks continue to get more sophisticated – you’re only as strong as your weakest link

Financial risk due to loss of revenue and/ or fines and penalties

Consumers are apprehensive about purchasing devices due to security and privacy concerns

The Cost of Security Inaction Is Growing

6 TRILLION

US DOLLARS

Anticipated cyber crime damages by 2021 (1)

5,400

ATTACKS

Per month on average targeted at IoT devices (2)

75.44

BILLION

Connected IoT devices by 2025 (3)

Governments around the world see cyber crime as a leading threat to national security

(1) 2019 Official Annual Cybercrime Report
(2) Symantec Internet Security Threat Report
(3) Statista

Varying Govt Regulations/Guidelines & Standards body Specs

North America Regulations

- California Govt – Senate Bill 327 – Currently in effect
- Oregon Govt – House Bill 2395 – Currently in effect
- US National Institute of Standards & Technology - evolving cybersecurity guidelines NISTR- 8259
- Cross references PSA Certified L1

Europe Regulations

- EU General Data Protection Regulation (GDPR) – Currently in effect
- UK Govt Department for Digital, Culture, Media and Sports (DCMS) – Adopted IoT Security Foundation Best Practice
- European Union Agency for Cybersecurity (ENISA) – 150 baseline recommendations

Global standard bodies

- Council to Secure Digital Economy(CSDE) – International Botnet and IoT Security Guide 2020
- European Telecommunications Standards Institute (ETSI) - EU Std body– Released ETSI 303 645 technical specification
- The International Society of Automation (ISA) –Std. body – developed ISA/ IEC 62443 security capabilities for control system components specification

Australia

- Australia Cyber Security Center (ACSC) – The draft Code of Practice: Securing the Internet of Things for Consumers

China

- Official standards released by government-sponsored working group as follows:
  - TAF/CCAA – TAF delivered IoT security standard v1.0
  - Standards Administration of China (SAC) - GB/T 36951—2018

Asia

- Singapore Cyber Security Agency (CSA/ GovTech) - May adopt NIST or DCMS or ETSI EN 303 645, but evaluating others
- India's Centre for Development of Advanced Computing (CDAC) – A govt. agency – still evaluating

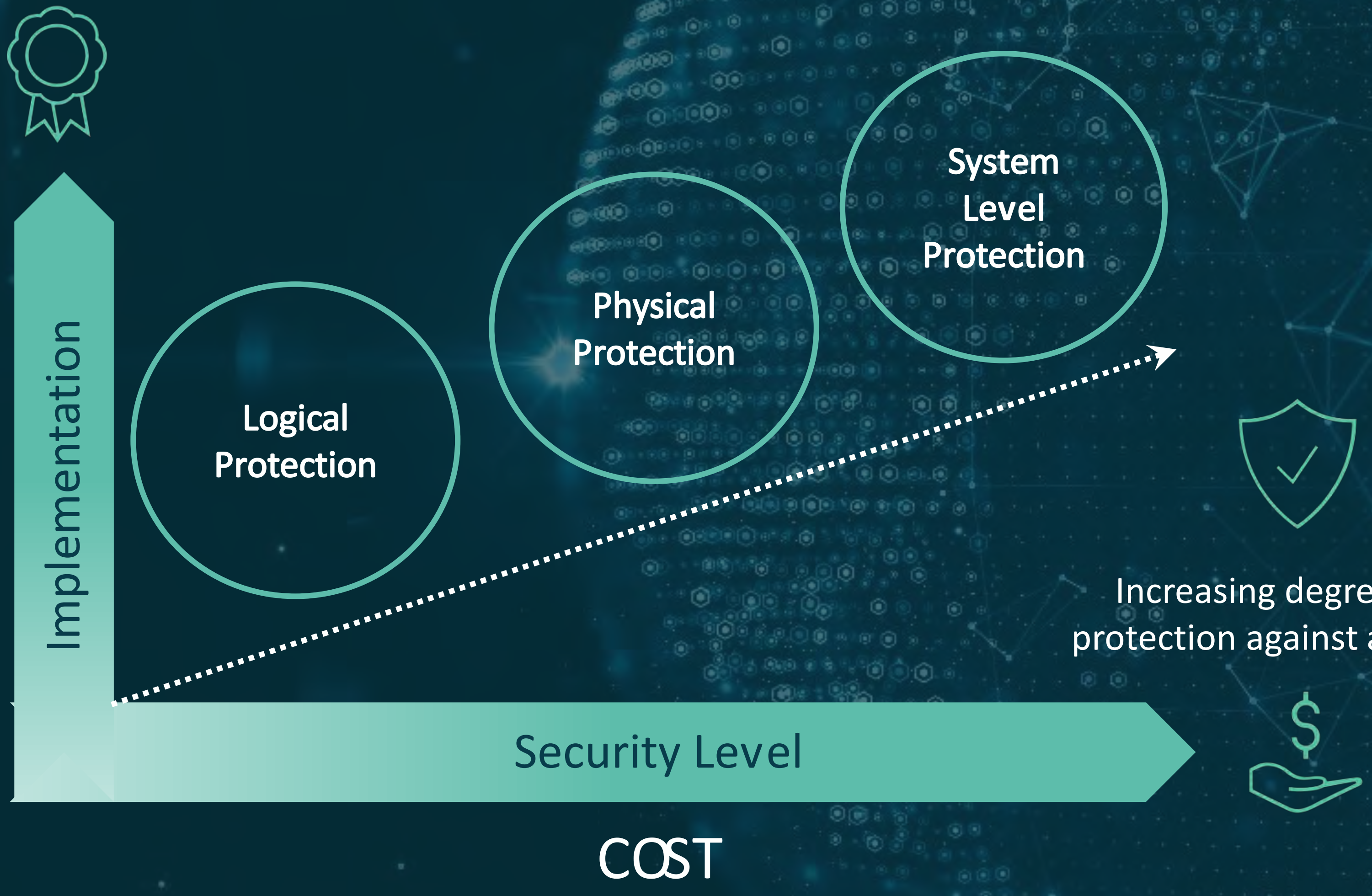
J apan

- MIC Govt - Ministry of Internal Affairs defines IoT device law
- CCDS Consortia (Connected Consumer Device Security Council) on best practices for IoT- GW
- J ETRO Govt - (J apan External Trade Organization)

Korea

- The Ministry of Science and ICT (MSIT)
  - Korea Internet Security Agency & certification (KISA) – IoT Security Standard

Balancing Security, Cost and Risk



Poll Question #2

1. **What are the most important considerations for security evolution?**

   a. Improving consumer trust/experience

   b. Product differentiation

   c. Meeting regulatory requirements

   d. Reducing risk (financial, reputation, etc.)

   e. Sustainability of the security strategy

Anurag Gupta

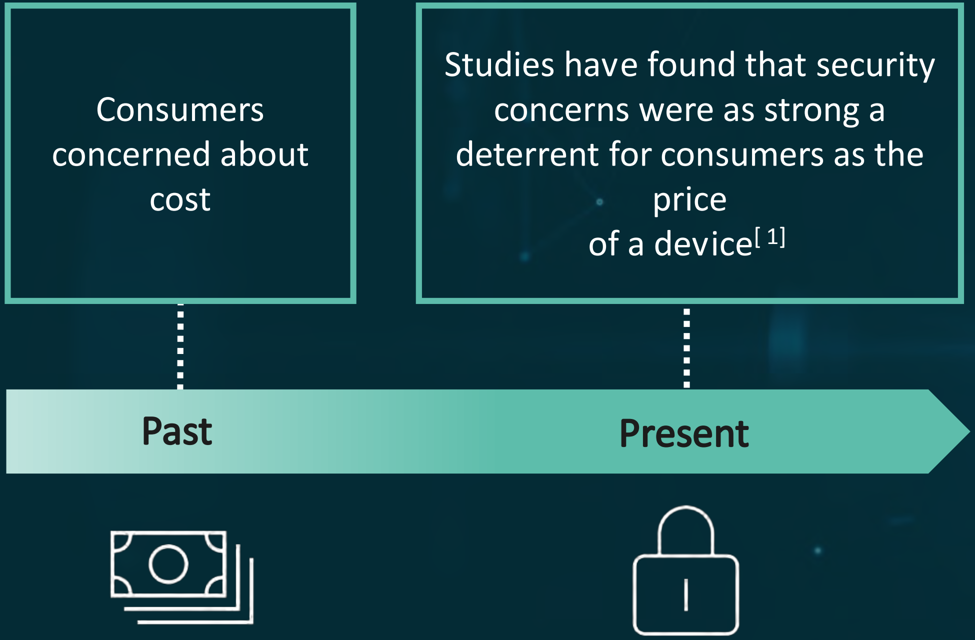
Director Business Development, Platform Security Architecture

Arm

Key strategies and considerations for device security evolution

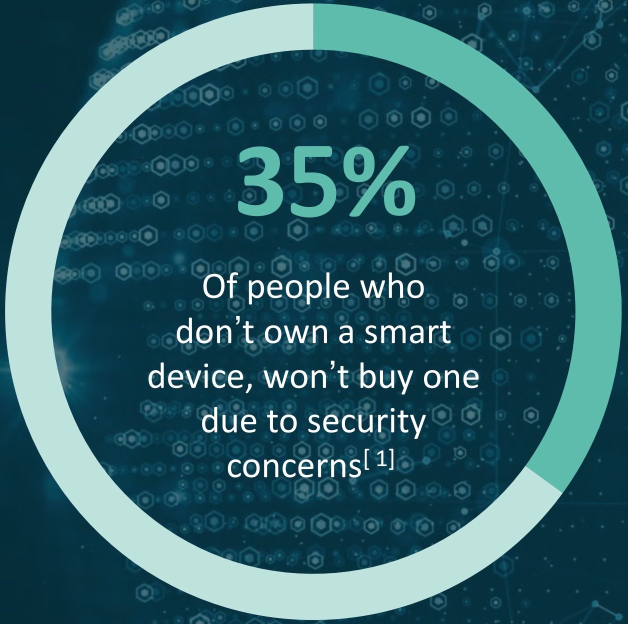
Anurag Gupta
Arm

Consumer Perspective Is Changing



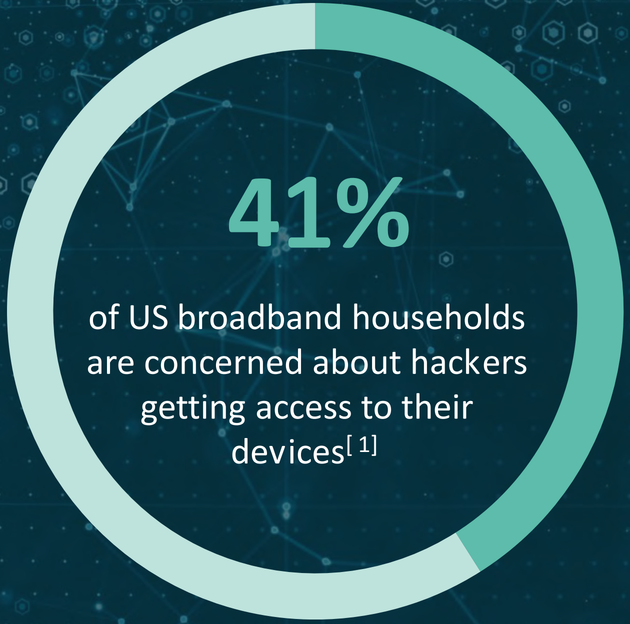
Consumers concerned about cost

Studies have found that security concerns were as strong a deterrent for consumers as the price of a device[1]



35%

Of people who don't own a smart device, won't buy one due to security concerns[1]



41%

of US broadband households are concerned about hackers getting access to their devices[1]

Embracing PSA Certified helps you to address consumer concerns by improving your security strategy

[1] Parks Associates

Security Implementation Considerations

Consumer experience

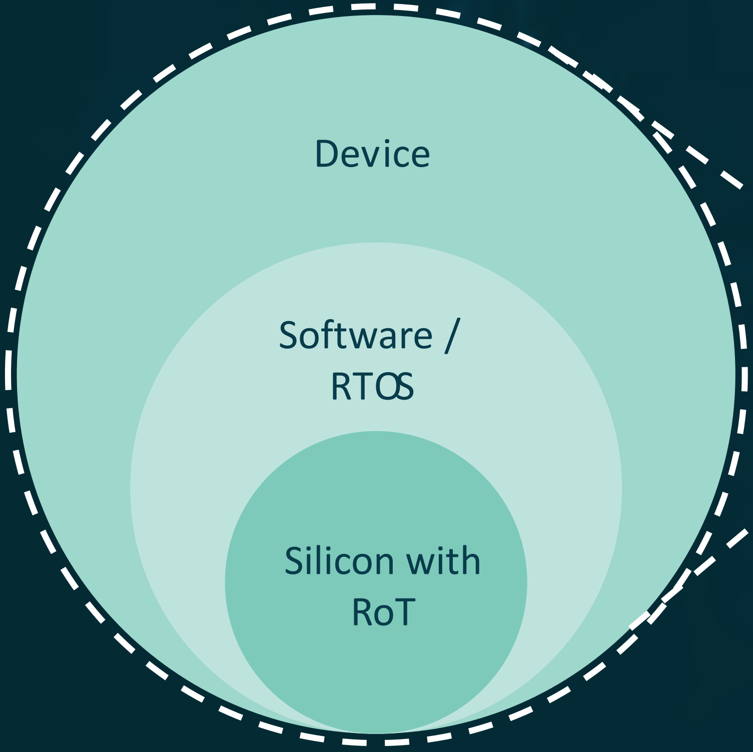
Expertise is important but often localized

Security isn't static – don't be complacent

Security needs to be comprehensive

Security shouldn't be seen as just a "cost" – it's a competitive differentiator

OEMs Have a Lot to Think About



How do I meet baseline IoT security requirements?

How do you design- in sound security principles?

How do you utilise a reliable RoT that has been assessed by a security lab?

How do I keep costs low?

Security brings trust and trust brings assurance in the marketplace

PSA Certified Framework

Analyze

Threat models & security analyses

Methodically developed

Architect

Hardware & firmware architect specifications

Open architecture

Implement

Firmware source code

Reference Implementation

Certify

Independently tested

psacertified™

Enabling Trust

Certification scheme with three levels

1 level applicable to OEMs

Choose silicon with the best RoT level for your device

10 security goals

psacertified™

PSA Certified: Built By Experts

Seven companies continuously developing PSA Certified

brightsight®

the number one
security lab
in the world

riscure

CAICT

中国信息通信研究院

China Academy of Information and Communications Technology

UL ®

PROVE & RUN

arm

TRUSTCB®

TRUST AND VERIFY

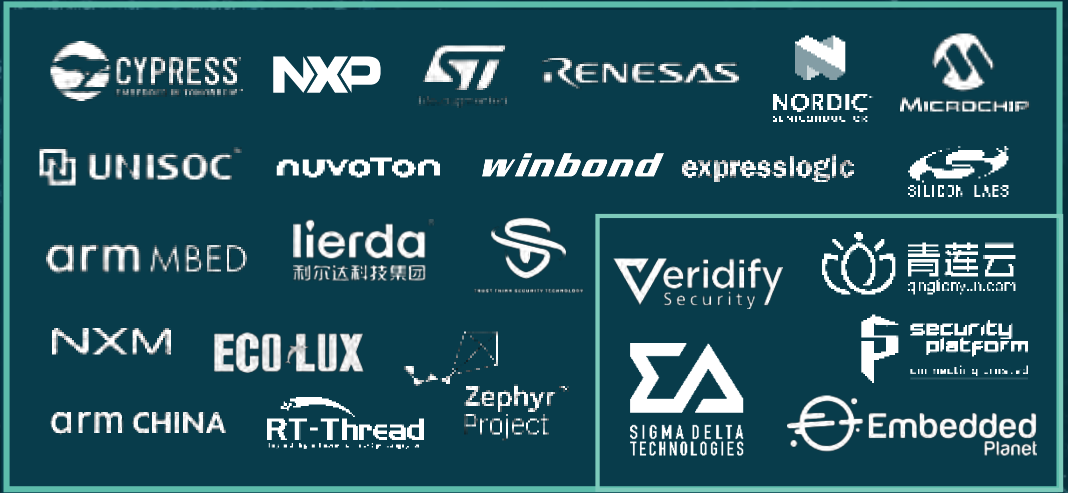
PSA Certified

2019

2020

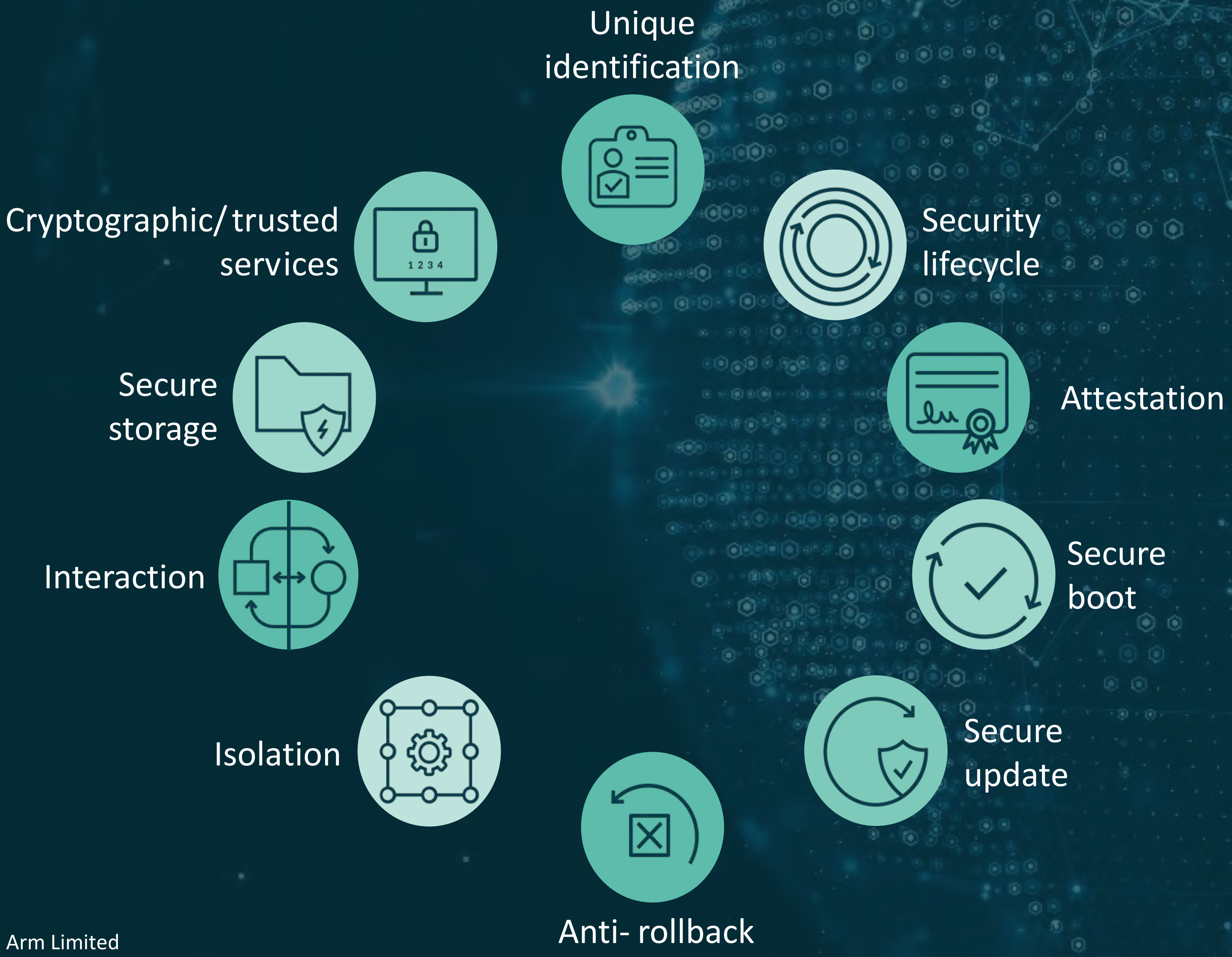
PSA Certified Level 1 launch
at Embedded World 2019

40+ PSA Certified solutions
Expanding PSA Certified Level 1 ecosystem



+ strategic partners like ARROW

Security Goals



Unique identification

Security lifecycle

Attestation

Secure boot

Secure update

Anti- rollback

Isolation

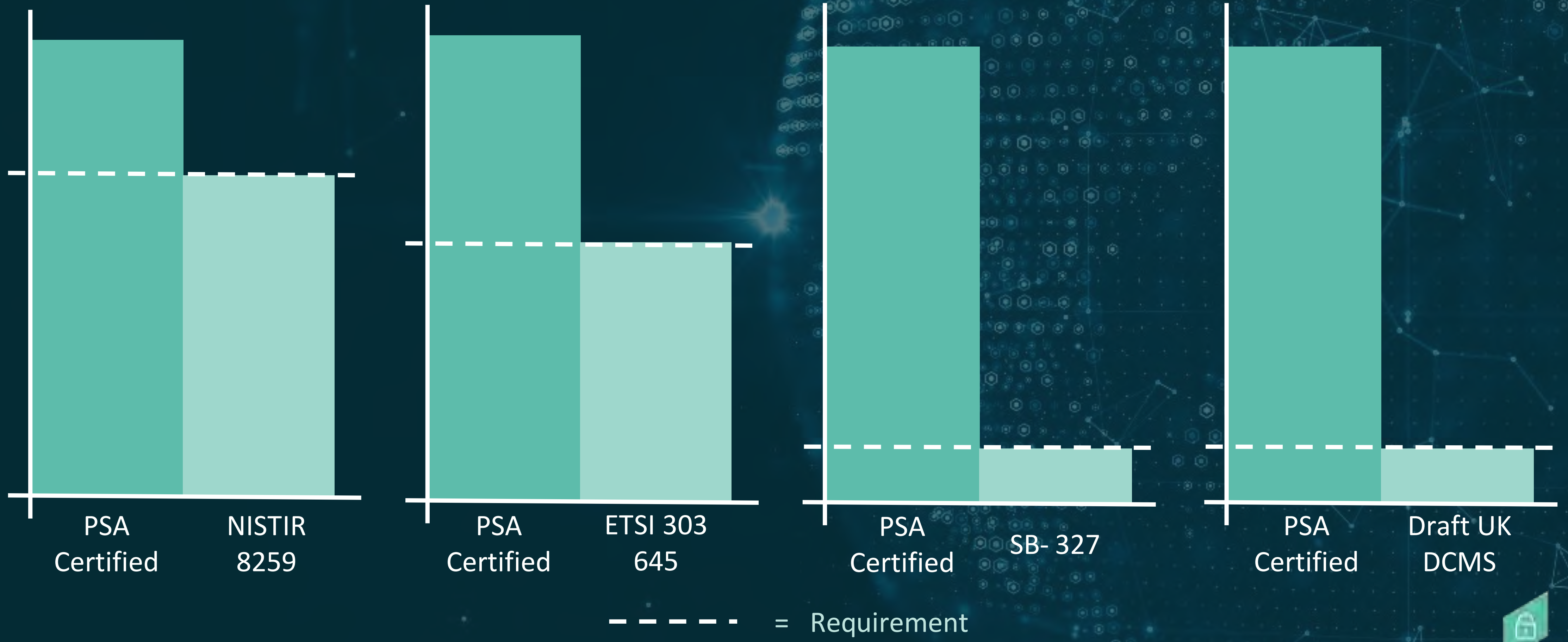
Interaction

Secure storage

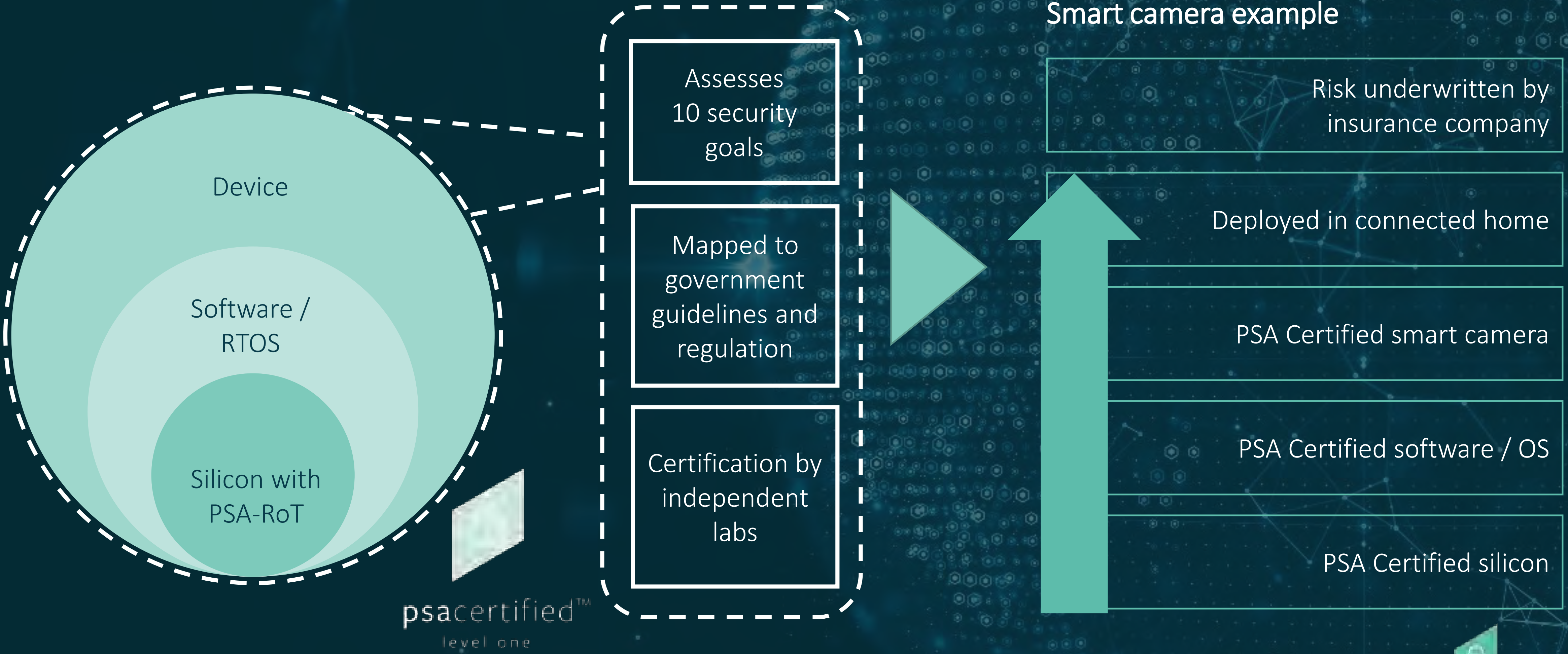
Cryptographic/ trusted services

Aligning to Major Standards and Law

PSA Certified Level 1 2.0



PSA Certified Journey for OEMs



Assesses 10 security goals

Mapped to government guidelines and regulation

Certification by independent labs

Smart camera example

- Risk underwritten by insurance company
- Deployed in connected home
- PSA Certified smart camera
- PSA Certified software / OS
- PSA Certified silicon

Poll Question #3

1. **Which of the following will have the highest impact on consumer confidence about device security?**

    a. Education on security threats

    b. Enforcement of security regulations

    c. Industry association or governmental trust label

    d. Advanced security features

Carlos Serratos

Senior Director of Strategy, Policy and Advocacy

Brightsight

Case studies

“Trust Me”: 3rd party assessments

- Enable the trust chain
- Gain increased brand reputation and consumer trust
  - Marketing tool
- Streamline your product development cycle
  - Cost reduction
- Completive edge
  - Reputation
  - Verify performance
  - Ensure compliance

brightsight
the number one
security lab
in the world

psacertified

Use case: the smart lock OEM

- "smart locks" are secure
  - "Bold. Sturdy. Secure"
  - "Unbreakable"
  - FTC violation to section 5 of the act

- FTC concluded the vendor is lacking
  - Reasonable measures, precautions and best practices
  - Security program in place

- The OEM agreed to undertake security measures
  - Including independent assessments every two years

brightsight the number one security lab in the world

psacertified

Pick me! Pick me!

60%vulnerabilities are discovered internally

64%subsequently attacked again

78 days in the system without being noticed

FireEye 2019 Mandiant M- Trends Report

brightsight
the number one
security lab
in the world

psacertified™

Hands on

Embedded Planet

“As the frequency and publicity of IoT devices being compromised increases, so does the mandate to prioritize security in design. Certification demonstrates acknowledgement of the challenges of IoT security and competence in design.”

SIGMA DELTA TECHNOLOGIES

“Customers know what they want to build (ex. metering system, heart rate monitor, air purifier, etc.). They all want their devices connected to some cloud (ex. Pelion, AWS, etc.). They do not have security or IoT engineers in-house.

Most embedded security companies sell DIY security technologies to customers, but SDT sells the security itself.”

Veridify Security

“A common challenge when implementing security into a product is ensuring that the process of building the solution does not introduce weaknesses or vulnerabilities that could be exploited. A proven certification framework builds trust into the platforms and products created. It can be leveraged by product developers with less security experience with the goal of simplifying the delivery of IoT security.”

brightsight

the number one security lab in the world

psacertified

PSA Certified Level 1 Benefits

psacertified™
level one

Independent third-party evaluations deliver the validation beyond the “trust me” claim

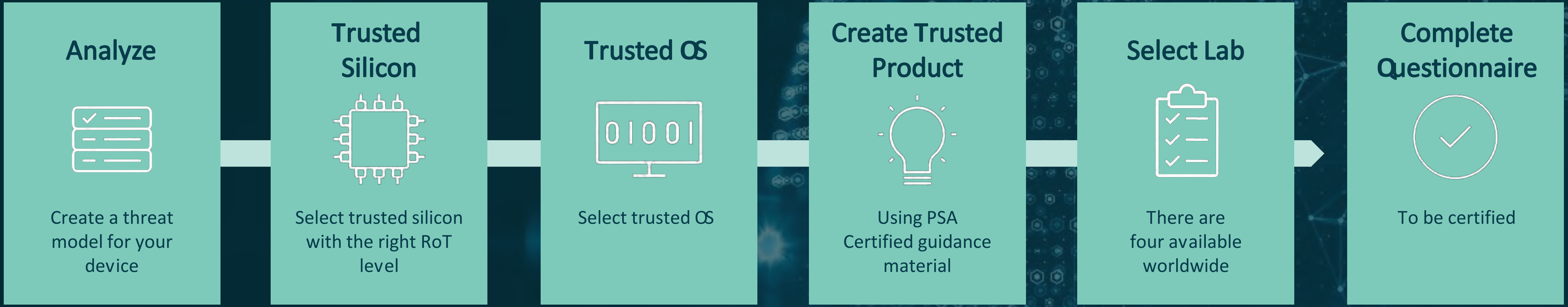
PSA Certified Level 1 provides a path for validating security claims against ETSI, NIST and California requirements

The evaluation is based on a self- declaration questionnaire that challenges the OEM into capturing the security functionality of their products, with answers verified by security experts from the evaluation laboratory

This evaluation has an additional layer of assurance by introducing the figure of certification body as the authority that validates the report from the security evaluation laboratory as part of the chain of trust

psacertified™

Your Next Steps



Analyze

Create a threat model for your device

Trusted Silicon

Select trusted silicon with the right RoT level

Trusted OS

Select trusted OS

Create Trusted Product

Using PSA Certified guidance material

Select Lab

There are four available worldwide

Complete Questionnaire

To be certified

PSACertified.org

- Level 1 – download the questionnaire
- Download the step by step guide
- Download examples

arm.com/ psa- resources

- For example threat models,
- Architecture specifications
- Implementation example

Questions

Questions

PARKS ASSOCIATES

Thank You

Patrice Samuels

Senior Analyst

972.490.1113

patrice.samuels@parksassociates.com

WWW.PARKSASSOCIATES.COM