The world is growing more connected

27 BILLION

connected IoT devices were in use in 2018 and will reach

125 BILLION

in 2030

In 2018 there were

5.2 BILLION

connected CONSUMER DEVICES growing with 13.8% CAGR 2013-30

Source: IHS Markit

THE PROBLEM

- Products are built to a functional / cost / time-to-market target
  - Security is not considered, or an after-thought
  - How to secure by design?
- Security is opaque to customers –
  - Why build security in, if it's not part of the purchase decision?
  - How to measure and differentiate for security?
- Security is an *every* point-in-time concept –
  - How to provide ongoing security assurance?

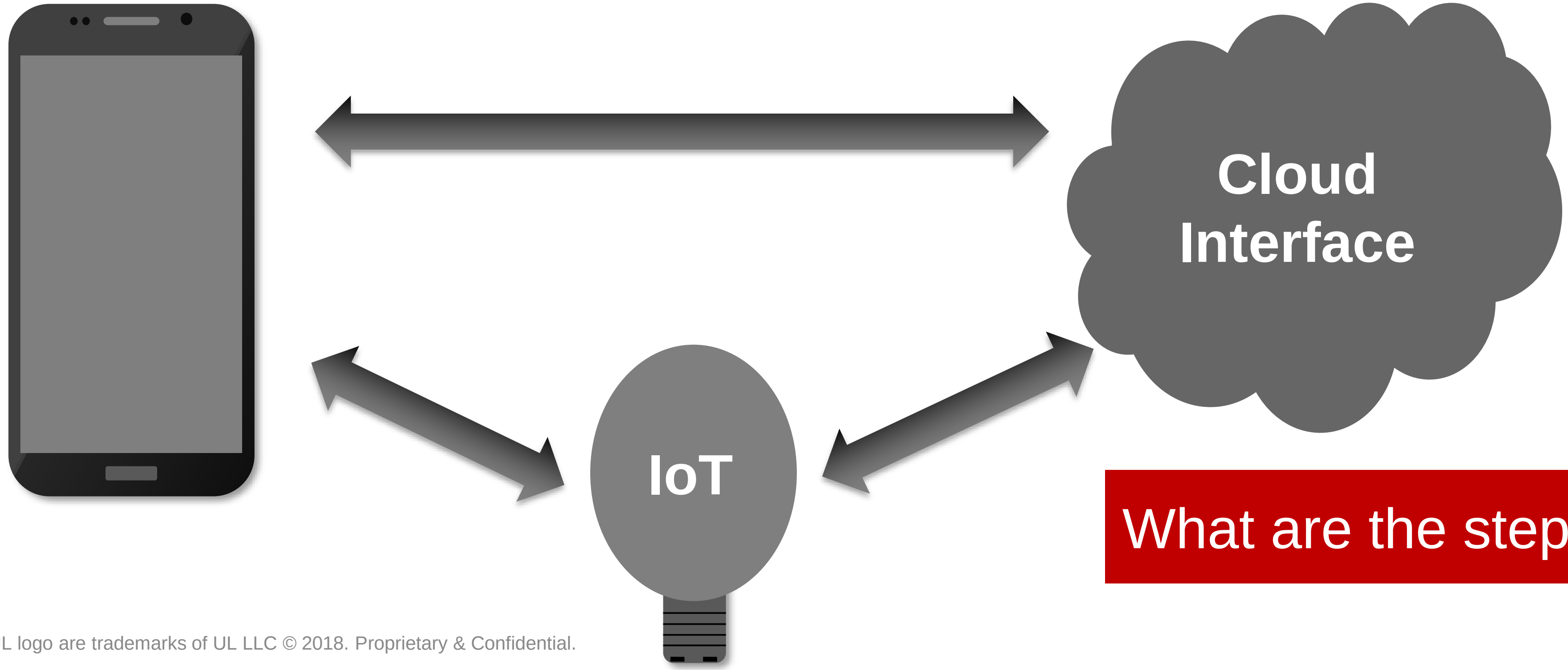
IoT security primarily is a commercial problem

AND… IT'S NOT JUST ABOUT THE THINGS

Increasingly, product functionality is distributed

The 'end point' device often requires functionality and control provided by remote systems – such as gateways, cloud systems, or mobile apps

Security issues at any one end can affect the entire solution



What are the steps then?

The ABC’s of UL IoT Security

Advise

Education

- Qualify risk
- Gap assessment
- Filter the noise

Benchmark

Support

- Pentest and security assessment
- Prepare for verification / certification
- Secure Development Lifecycle

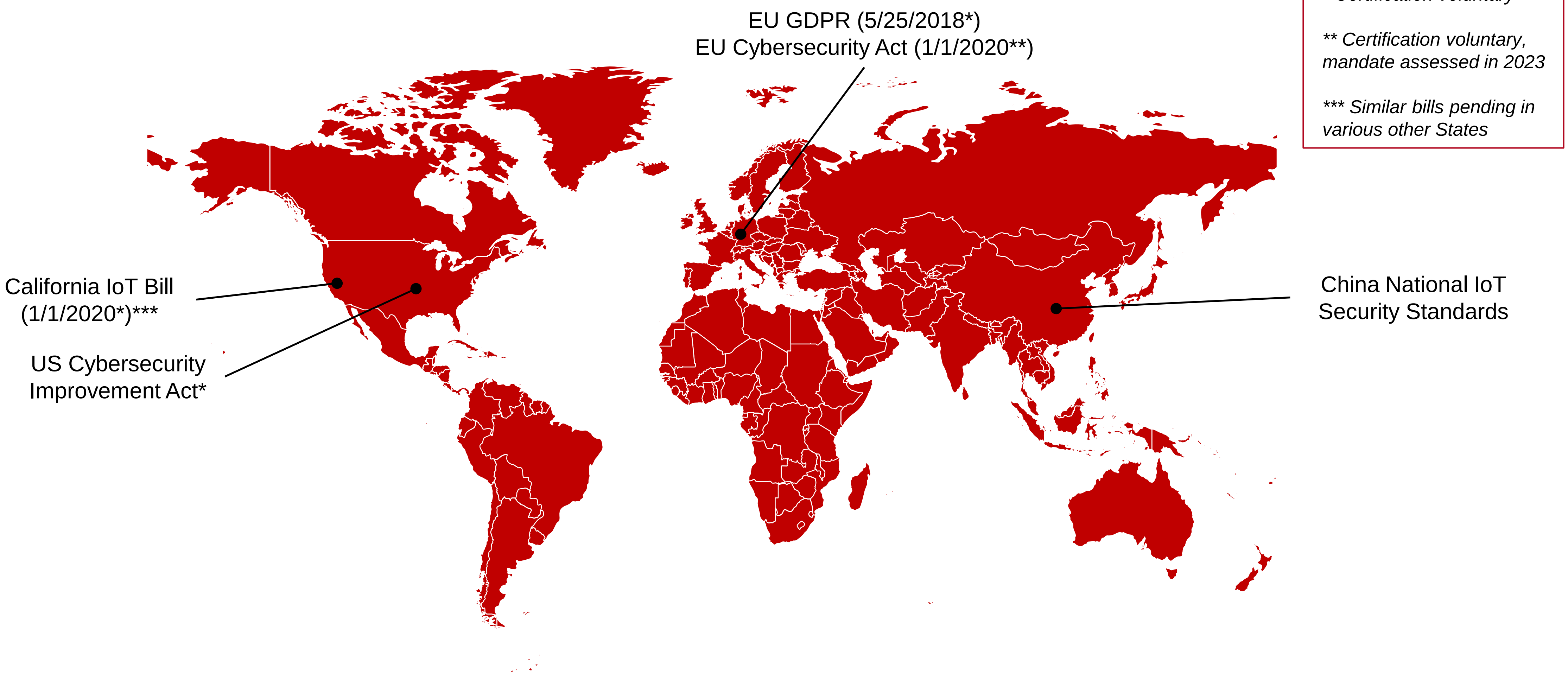
Certify

Partnership

- Differentiate early adopters
- Validate ROI
- Brand reputation

CYBERSECURITY MATURITY

REGULATORY DEVELOPMENTS



EU GDPR (5/25/2018*)
EU Cybersecurity Act (1/1/2020**)

California IoT Bill (1/1/2020*)***

US Cybersecurity Improvement Act*

China National IoT Security Standards

** Certification voluntary*

*** Certification voluntary, mandate assessed in 2023*

**** Similar bills pending in various other States*

Governments are moving, but will look upon industry initiatives to lead the way

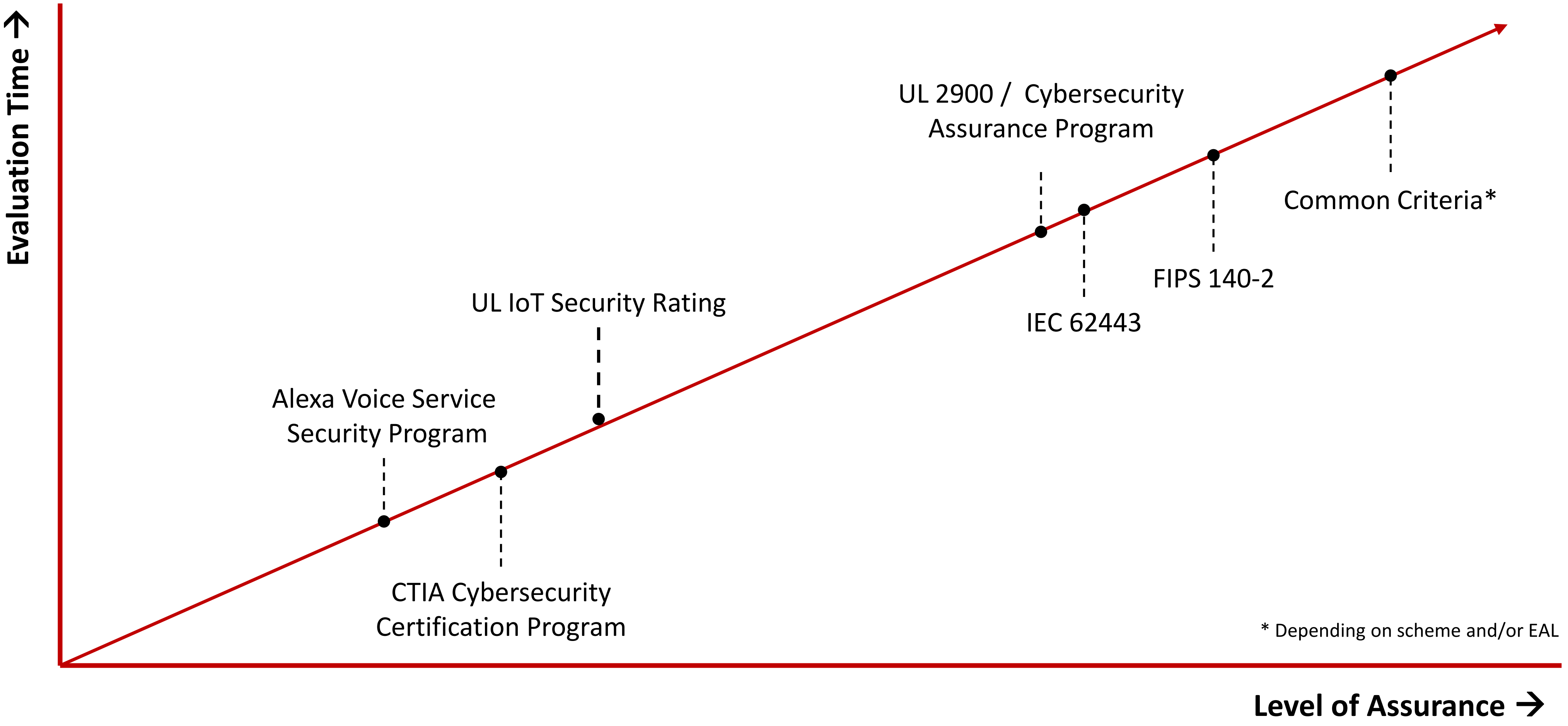
REGULATORY & INDUSTRY INITIATIVE EXAMPLES

- California IoT Bill
- EU Cybersecurity Act
- US Cybersecurity Improvement Act
- UK Code of Practice for Consumer IoT Security/ETSI TS 103 645
- NIST Core Baseline Cybersecurity Capabilities
- DoC/DHS Botnet Report
- CSDE/CTA Anti-Botnet Guide

- IEC 62443
- UL 2900 Series of Standards / UL Cybersecurity Assurance Program (CAP)
- UL IoT Security Rating Program
- Common Criteria (ISO 15408)
- FIPS
- ARM PSA
- CTIA Cybersecurity Certification Program
- Amazon Alexa Voice Service Security Program
- GSMA IoT Security Guidelines
- IoT Security Foundation Best Practices Guidelines
- Other

TIME VS SECURITY ASSURANCE

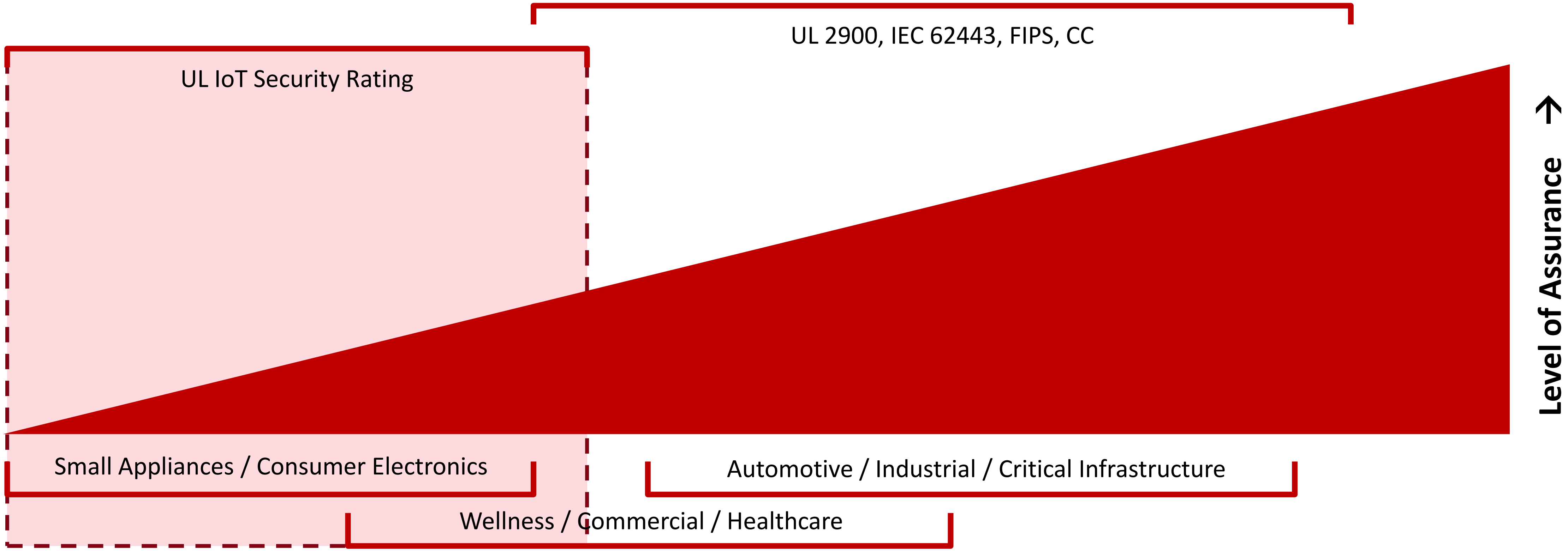
~ ILLUSTRATIVE ~



* Depending on scheme and/or EAL

TIME VS SECURITY ASSURANCE

~ ILLUSTRATIVE ~



UL 2900, IEC 62443, FIPS, CC

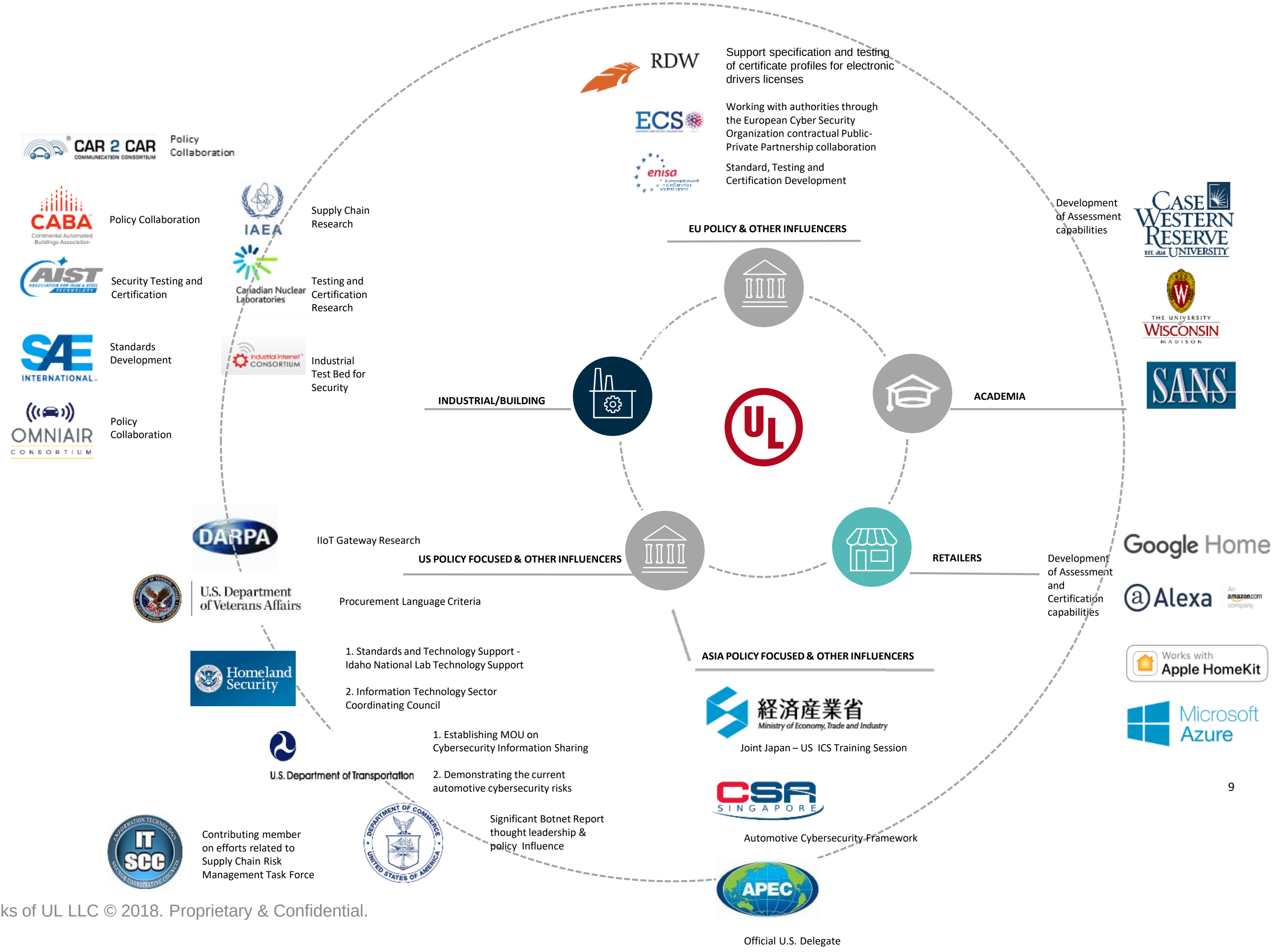
UL IoT Security Rating

Small Appliances / Consumer Electronics

Automotive / Industrial / Critical Infrastructure

Wellness / Commercial / Healthcare

A COLLABORATIVE APPROACH



EU POLICY & OTHER INFLUENCERS

RDW — Support specification and testing of certificate profiles for electronic drivers licenses

ECS — Working with authorities through the European Cyber Security Organization contractual Public-Private Partnership collaboration

enisa — Standard, Testing and Certification Development

ACADEMIA

Development of Assessment capabilities — Case Western Reserve University, The University of Wisconsin Madison, SANS

RETAILERS

Development of Assessment and Certification capabilities — Google Home, Alexa (an amazon.com company), Works with Apple HomeKit, Microsoft Azure

9

ASIA POLICY FOCUSED & OTHER INFLUENCERS

経済産業省 Ministry of Economy, Trade and Industry — Joint Japan – US ICS Training Session

CSR Singapore — Automotive Cybersecurity Framework

APEC — Official U.S. Delegate

US POLICY FOCUSED & OTHER INFLUENCERS

DARPA — IIoT Gateway Research

U.S. Department of Veterans Affairs — Procurement Language Criteria

Homeland Security — 1. Standards and Technology Support - Idaho National Lab Technology Support

2. Information Technology Sector Coordinating Council

U.S. Department of Transportation — 1. Establishing MOU on Cybersecurity Information Sharing

2. Demonstrating the current automotive cybersecurity risks

Department of Commerce, United States of America — Significant Botnet Report thought leadership & policy Influence

IT SCC — Contributing member on efforts related to Supply Chain Risk Management Task Force

INDUSTRIAL/BUILDING

CAR 2 CAR Communication Consortium — Policy Collaboration

CABA Continental Automated Buildings Association — Policy Collaboration

AIST Association for Iron & Steel Technology — Security Testing and Certification

SAE International — Standards Development

OMNIAIR Consortium — Policy Collaboration

IAEA — Supply Chain Research

Canadian Nuclear Laboratories — Testing and Certification Research

Industrial Internet Consortium — Industrial Test Bed for Security

SUPPLY CHAIN SECURITY

Problem

- Tier 1 OEMs and asset owners struggle with understanding the security maturity of their suppliers
- Existing SLAs with suppliers are ineffective because most suppliers don't understand security
- OEMs and asset owners don't have the time and may not have the resources to validate each one of their suppliers' security maturity

Solution

- An independent evaluation of suppliers with focus on suppliers' security processes and/or product testing
- An independent evaluation that provides transparency to OEMS and asset owners for supplier security
- An independent 3rd party that can work with suppliers to improve their security maturity over time

Complexity is the problem

TRUST

IS THE SOLUTION

- Powers smarter decisions
- Makes brands easier to choose
- Makes supply chains simpler to manage
- Makes differentiation quicker to achieve

THANK YOU

Empowering Trust™