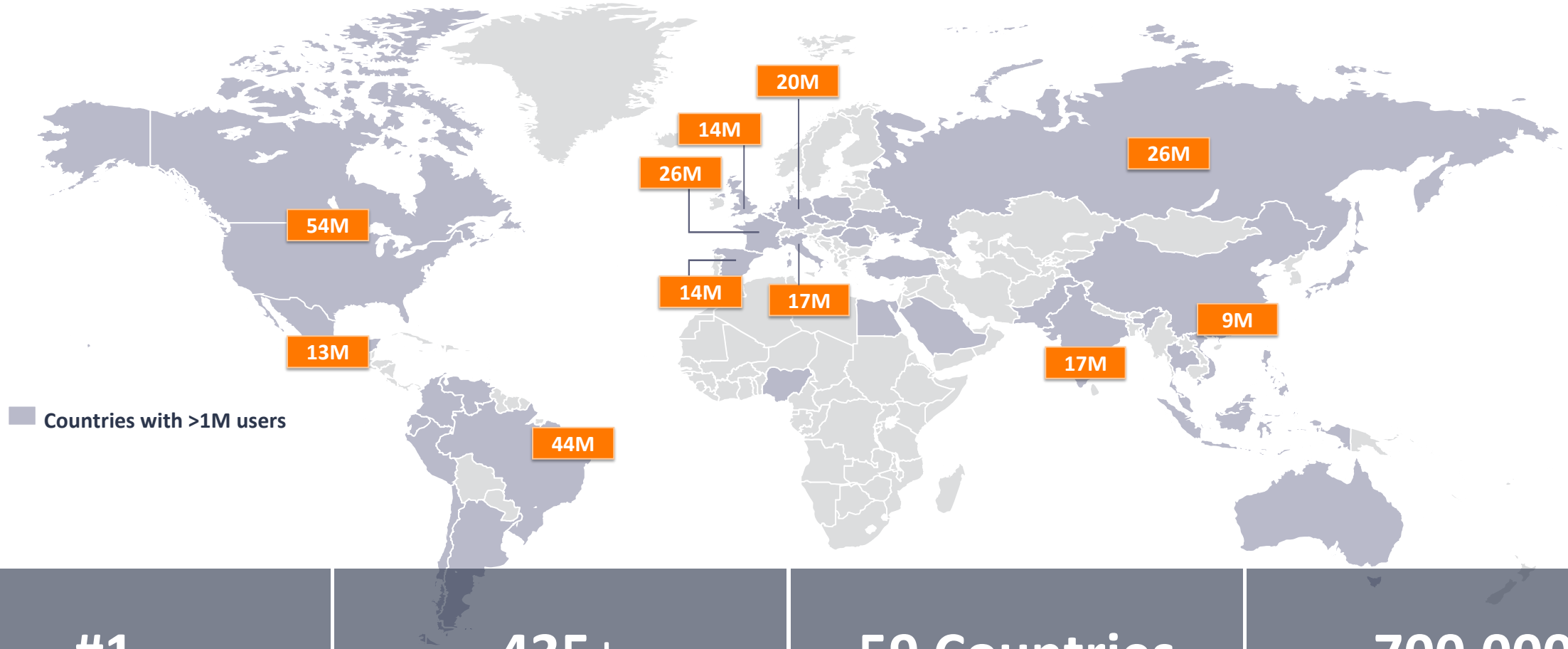
RSAConference2019
San Francisco | March 4–8 | Moscone Center

Shadow IoT Hacking the Corporate Environment: Office as the New Smart home

Ondrej Vlcek
President and Chief Technology Officer
Avast
@avastvlk

World's largest provider of Consumer Protection, Privacy, and Performance Products



#1
Downloaded Consumer Security Product

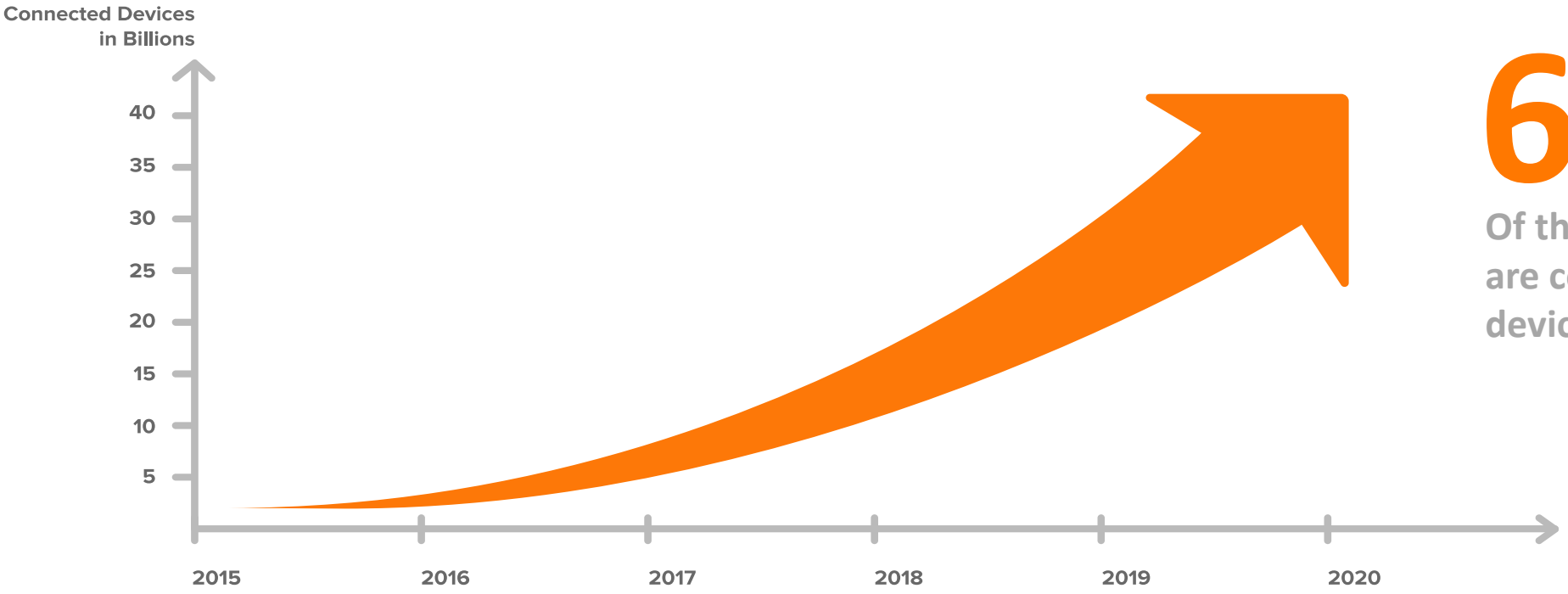
435+
Million Global Users

59 Countries
With >1M Active Users

700,000
Businesses Protected

The Number of Connected Devices Is Growing Exponentially

The types of connected devices are expanding broadly



64%

Of these devices are consumer devices

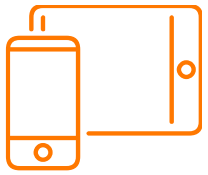
- TVs
- Toys
- Lighting
- Game Consoles
- Home Climate
- Car Infotainment
- Healthcare
- Car Safety
- VR Displays
- Self-Driving Cars
- AR Displays
- Smart Meters
- Delivery Drones
- Personal Wellness / Quantified Self
- Security Sensors

What does the smart home of today look like?

Analyzed Avast data for December 2018

15.5M

HOMES



83M

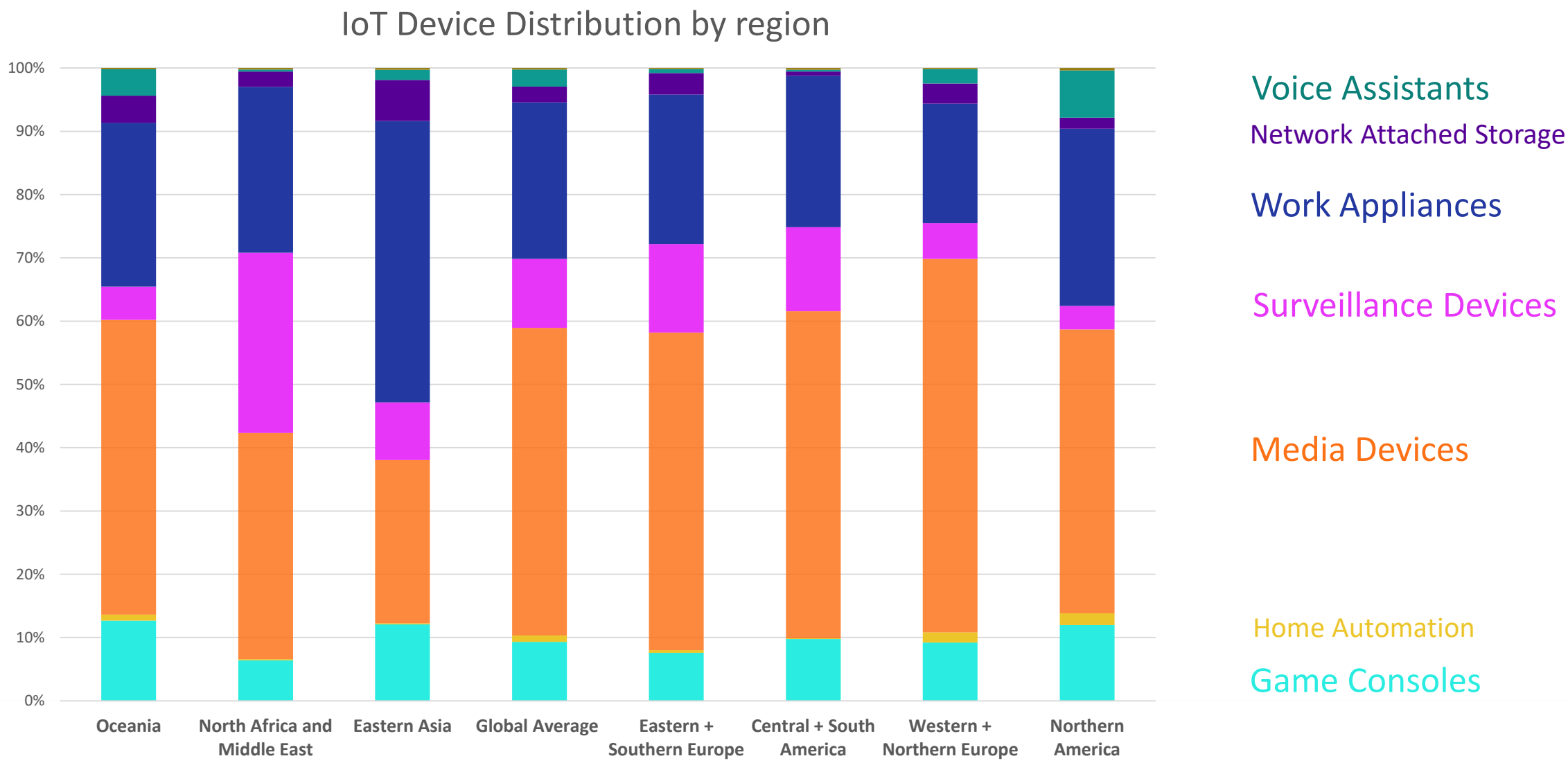
DEVICES

Research Collaboration:

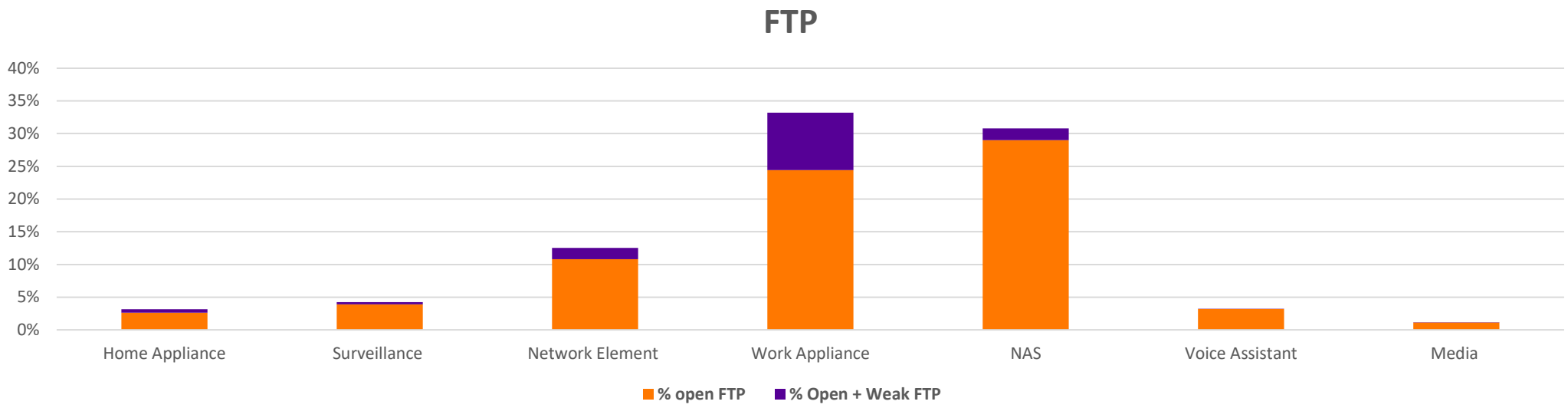
Stanford University

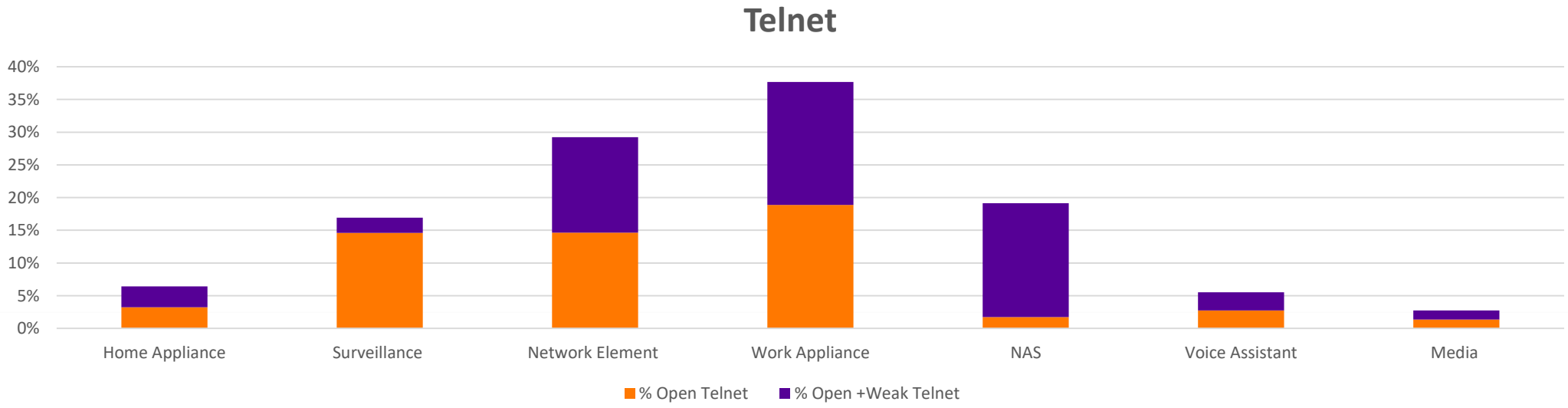
avast

Device distribution by region



Weak credentials and protocols





Survey of IT Directors: IoT in the enterprise

35%

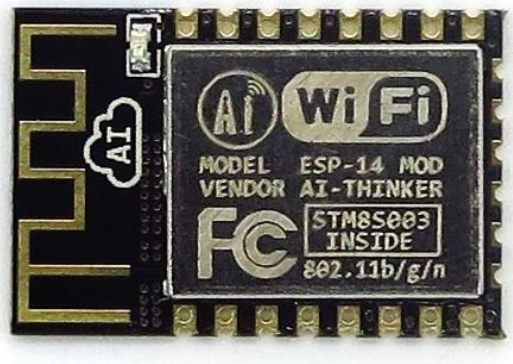
>1,000 Shadow IoT Devices on Corporate Network

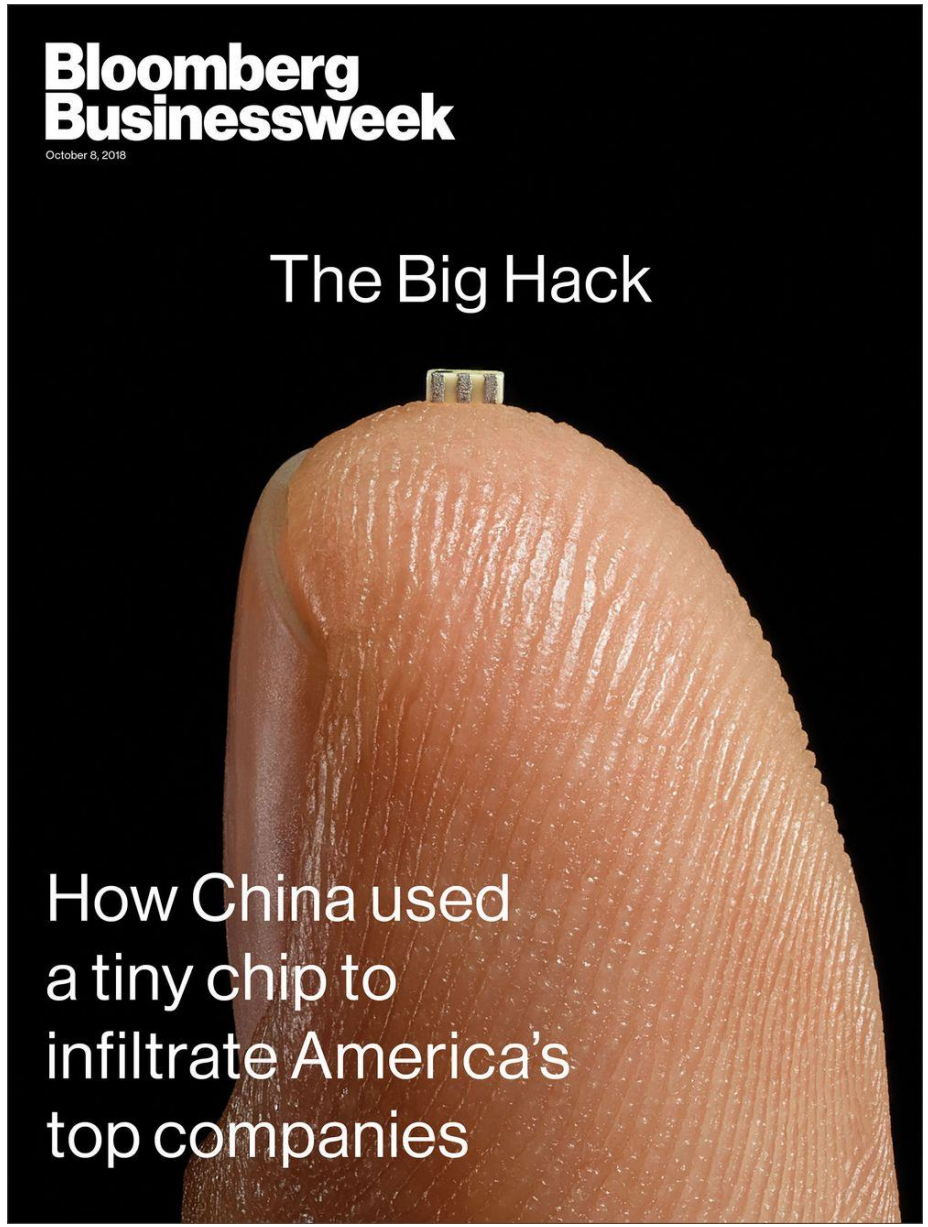
39%

used personal devices connected to the enterprise network

The problem of protecting IoT

Weak Embedded Security | Unprotected Supply Chain | Common Components





You don't have to do this….

There are plenty of ways for rogue devices to get in…

IoT malware getting more and more sophisticated

TORII

Early IoT Malware

- Single purpose
- Focused on DDoS, Cryptomining
- Easily spotted and stopped

Evolving IoT Malware

- More persistent
- Sophisticated obfuscation
- Can deliver any kind of malware
- Gathers extensive information about the network

RSAConference2019

Demo: Eyes and ears in the enterprise

Recommended Enterprise Approach to IoT security

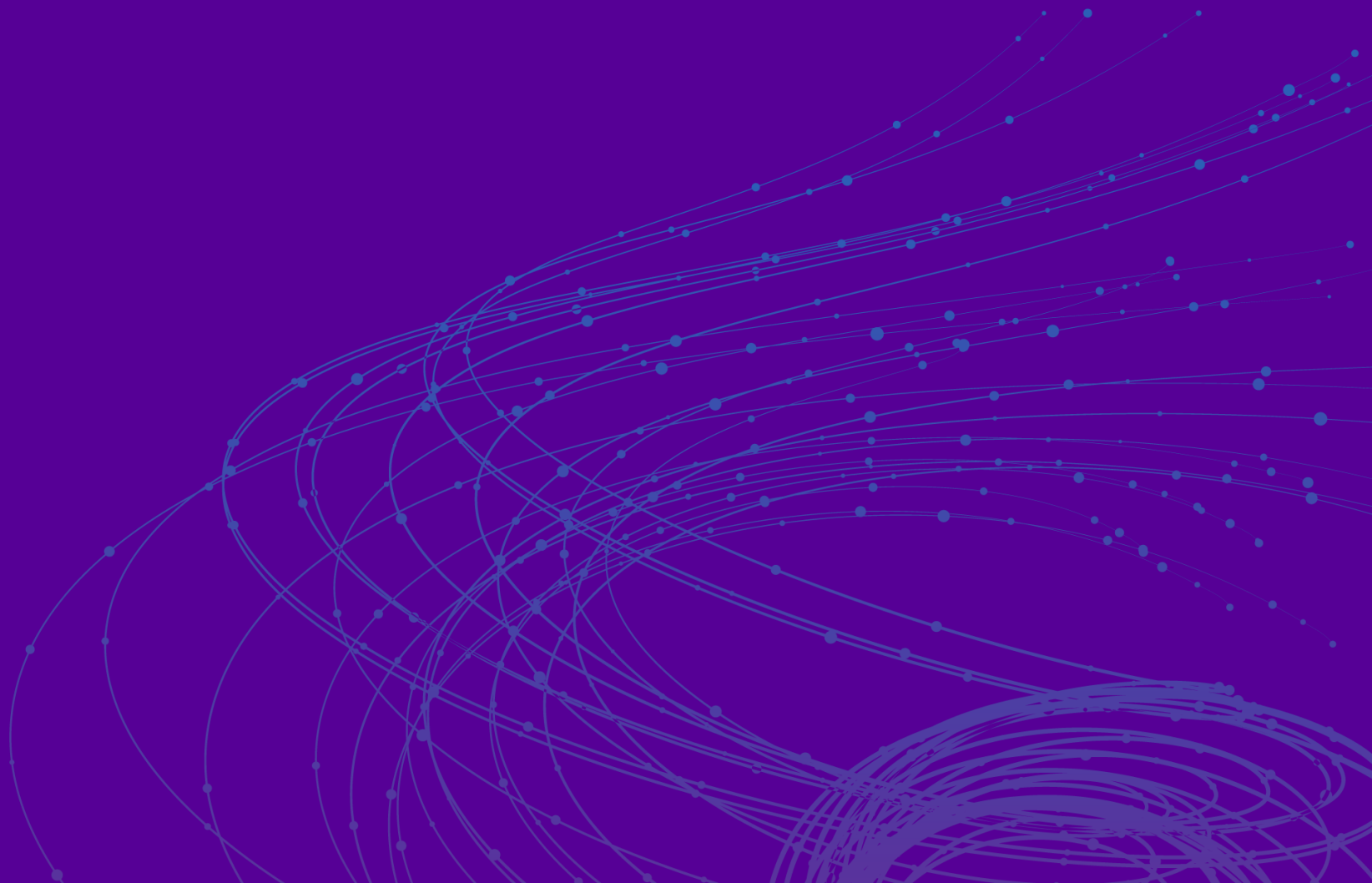
- Device cataloging
- Network Segmentation
- Network traffic analysis
- Patch management
- Enforcing internal network policies
- Remember, it’s not about the perimeter anymore

Script for Demo

Go to
https://docs.google.com/document/d/10bwdHEDJUFbd7BxFk_cBMoyMs8lQSMCGQRvq1RkZh6Y/edit

RSAConference2019

Thank you

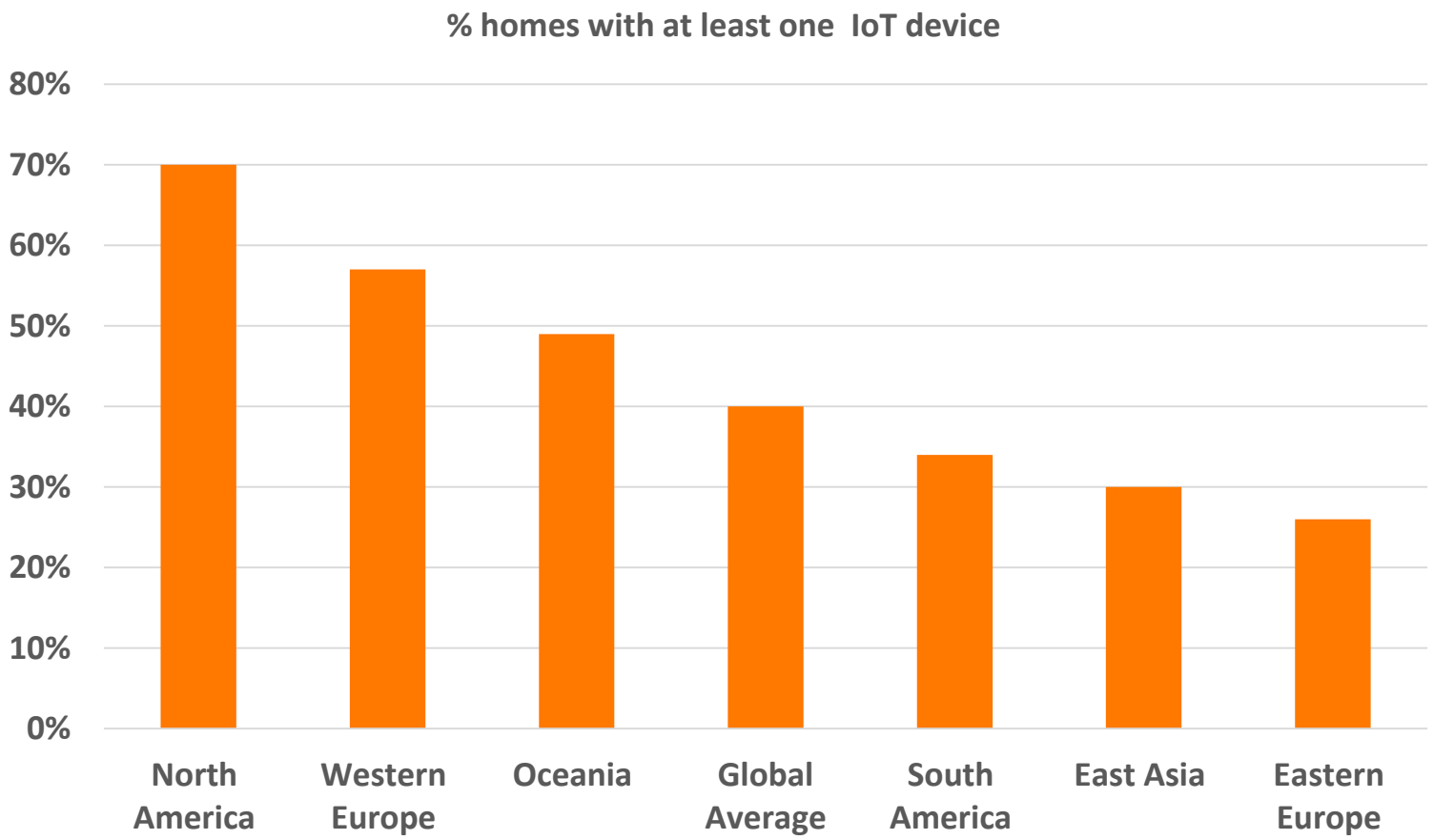


Weak Routers at ISPs causing downstream infections

Mikrotik Router Fiasco

- XXX detected infections
- Again, more persistent and sophisticated obfuscation
- Capable of being controlled and repurposed – cryptomining, scanning networks, etc.
- Powerful mesh network of enslaved routers

Device distribution by region



While 70% of homes in North America have a device, fewer than 10% in South East Asia do.

In all regions, 100 vendors account for more than **90%** of devices.

400 vendors account for **99%**.