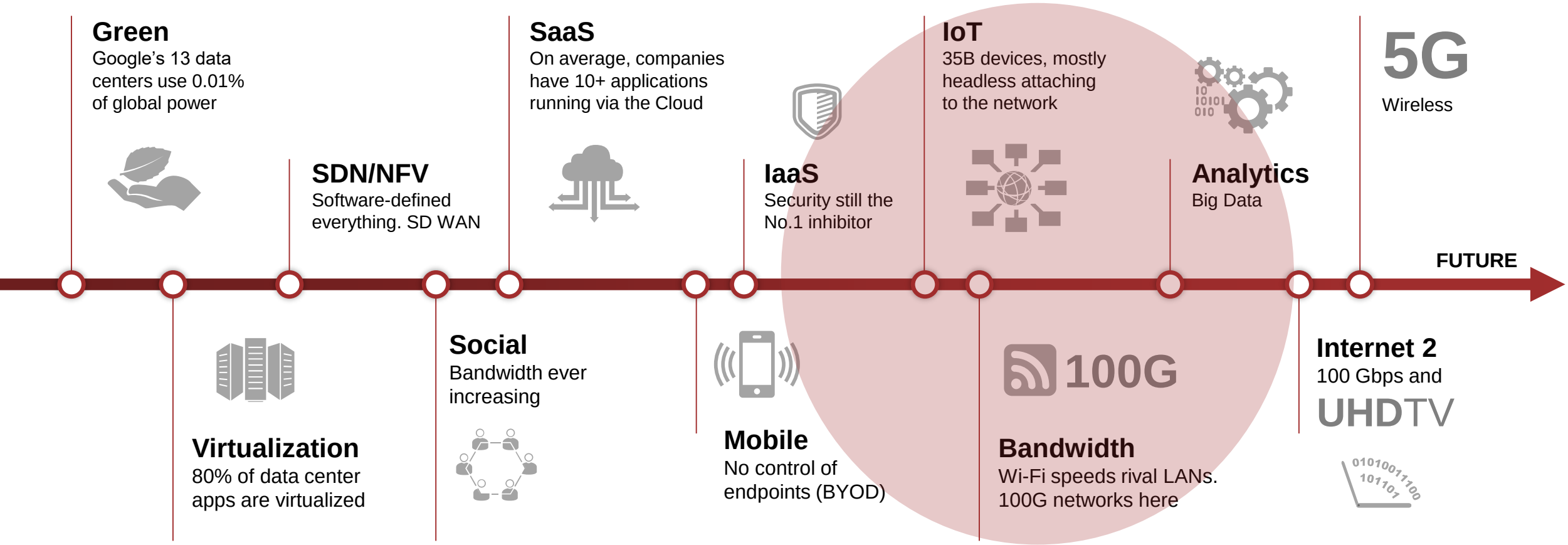
Securing the IoT

Eric Wu 吳章銘
ericwu@fortinet.net

永不停止的改變與演進


Green
Google's 13 data centers use 0.01% of global power
SDN/NFV
Software-defined everything. SD WAN
SaaS
On average, companies have 10+ applications running via the Cloud
IaaS
Security still the No.1 inhibitor
IoT
35B devices, mostly headless attaching to the network
Analytics
Big Data
5G
Wireless
FUTURE
Virtualization
80% of data center apps are virtualized
Social
Bandwidth ever increasing
Mobile
No control of endpoints (BYOD)
100G
Bandwidth
Wi-Fi speeds rival LANs. 100G networks here
Internet 2
100 Gbps and
UHDTV

A World of “SMART THINGS”

The ‘Internet of Things’ will generate $14.4 trillion of value over the next decade

Healthcare

CREDIT SUISSE

Total sales of clothing and accessories that incorporate computer technology are on target to grow to $42.5 billion by 2019

Cars

EMEA IoT revenues are estimated at a total of $2.4 trillion by 2020

Agriculture

IDC

IoT Examples – the Daily Stuff

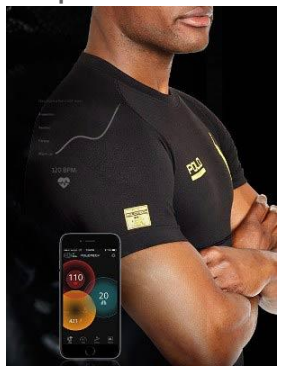
Smart Thermostats

Apple Watch

Smart TV

Mimo Monitor

Ralph Lauren Shirt



Google glasses

Smart Phones

Smart Fridge

Key Foundations for the IoT Ecosystem

Security
Access and threats

Trust
"Trust" ecosystem:
users, partners, suppliers

Privacy
Data confidentiality
and control

Update on SFMTA Ransomware Attack

這下子，還要一直IoT嗎？

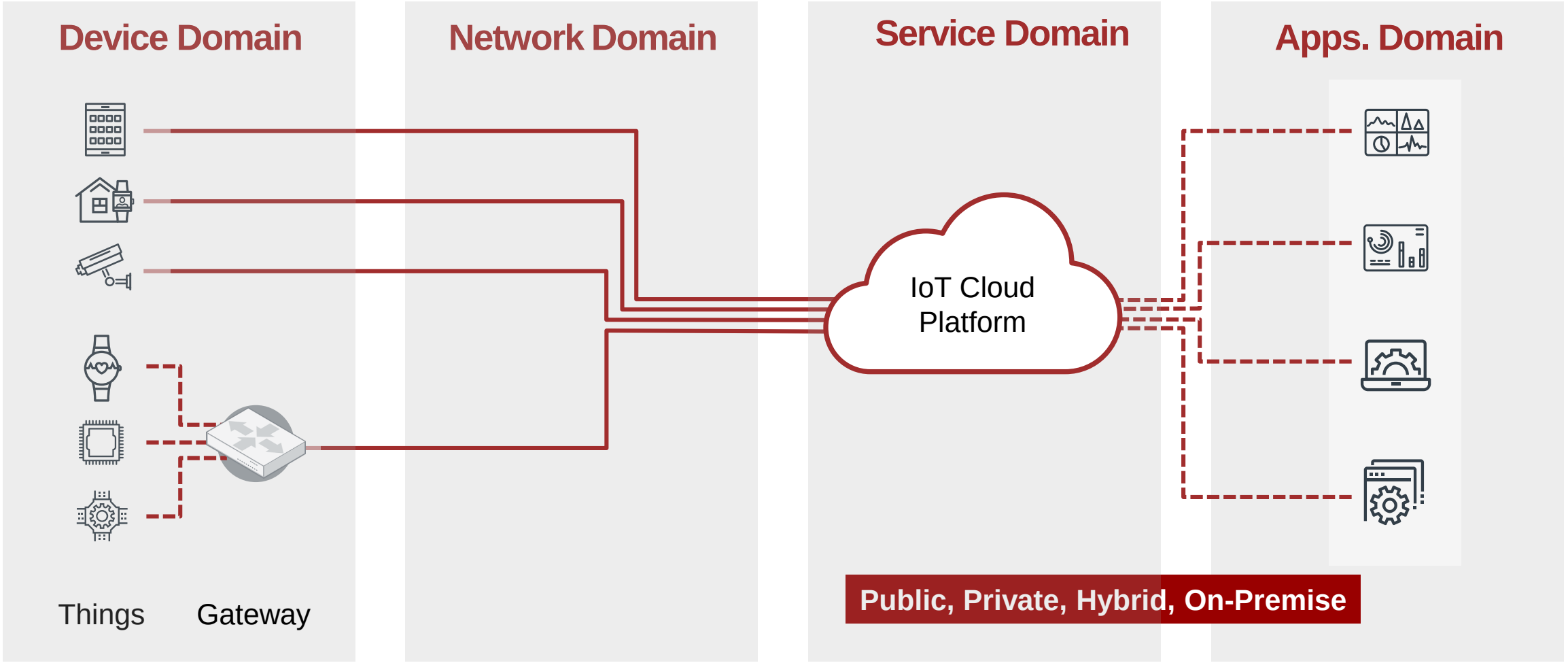
by Kristen Holland
Monday, November 28, 2016

Updated 5:22 p.m., Monday, Nov. 28:

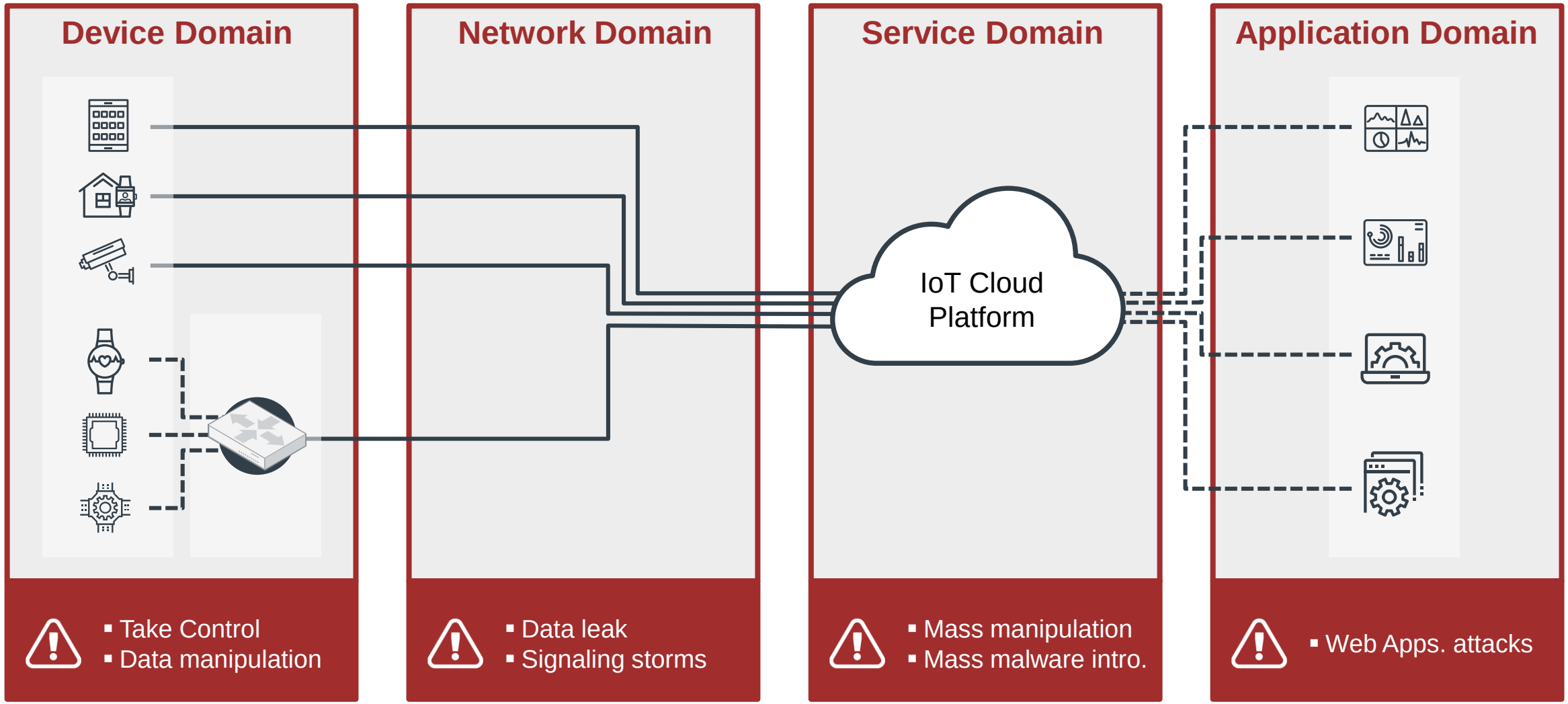
Thank you for your at… …re our office computers from this weekend's ransomware attack. W… …rmation as possible. To that end, below is a summary of the effects of the … …stand them.

…y, Nov. 25 we became aware of a potential security issue with our computer systems, including email. The malware used encrypted some systems mainly affecting office computers, as well as access to various systems. However, the SFMTA network was not breached from the outside, nor did hackers gain entry through our firewalls. Muni operations and safety were not affected. Our customer payment systems were not hacked. Also, despite media reports - no data was accessed from any of our servers.

The IoT (Distributed) Ecosystem



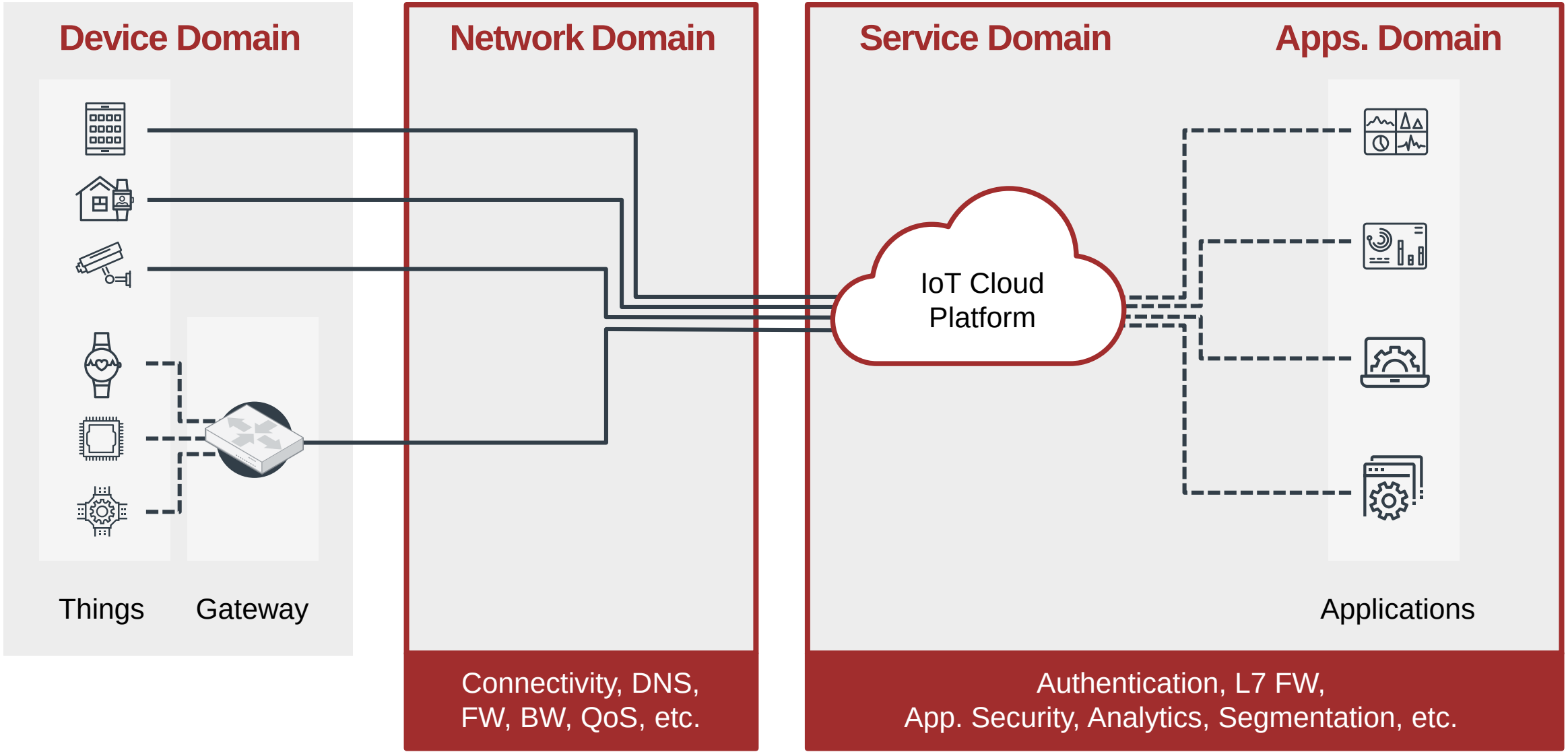
Security Concerns in the IoT Ecosystem



Device Domain – Where Vulnerability Starts

SECURITY MUST START at the Network Domain and Continue in the Service and Application Domains

The CSP IoT Business Model



IoT Security Strategy

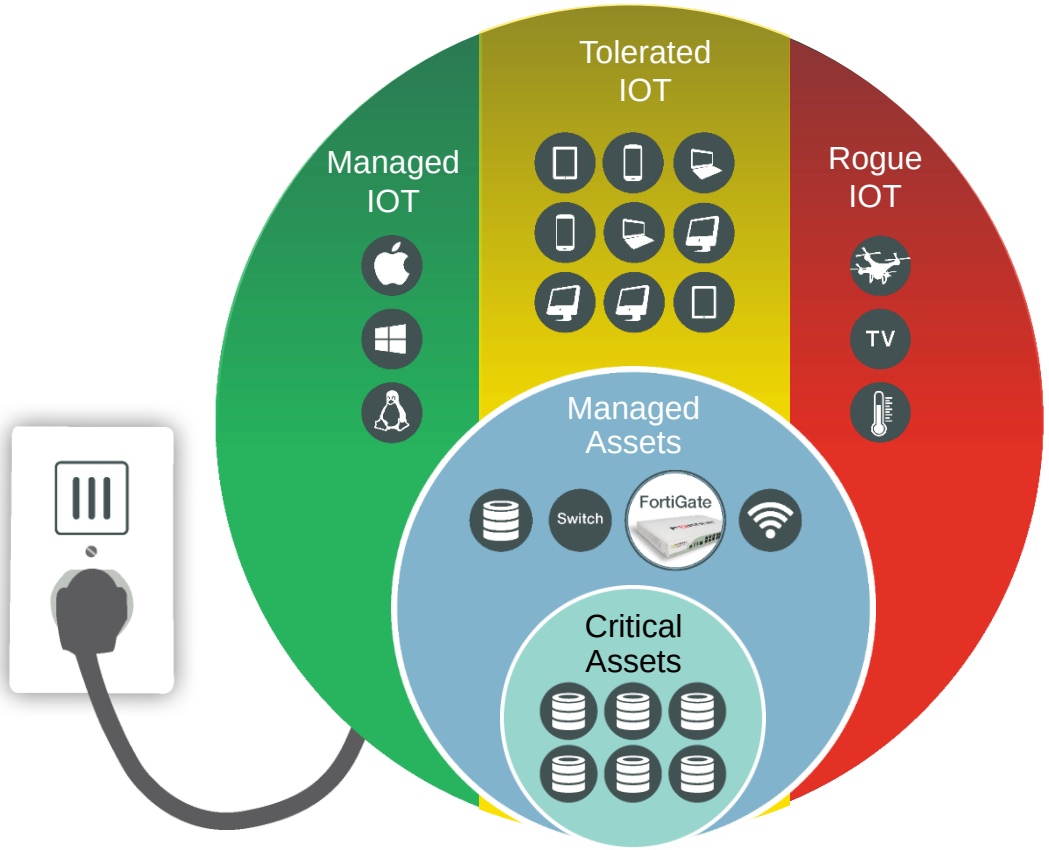
What IoT Problem?

Your attack surface changes every time…

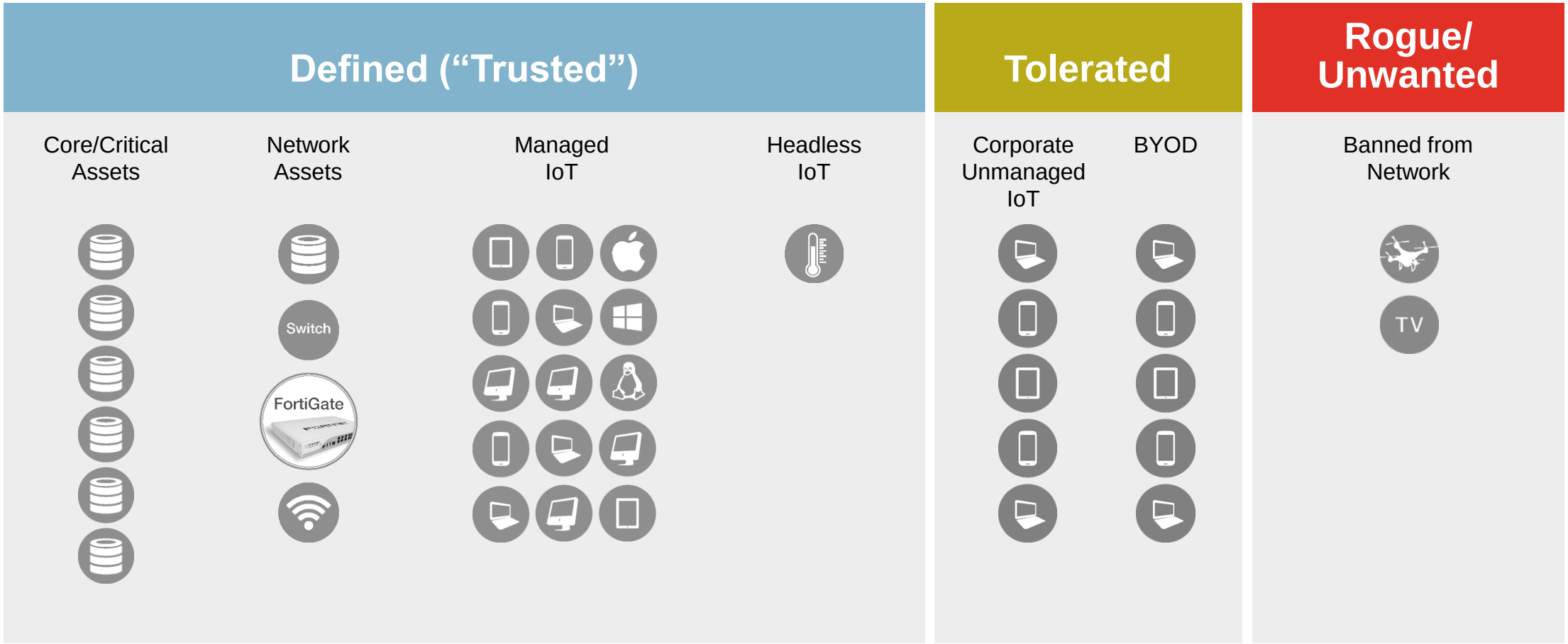
- A new application is installed
- A new device enters your network
- A new VM service is connected
- A user signs up for a new social account

Security Fabric…

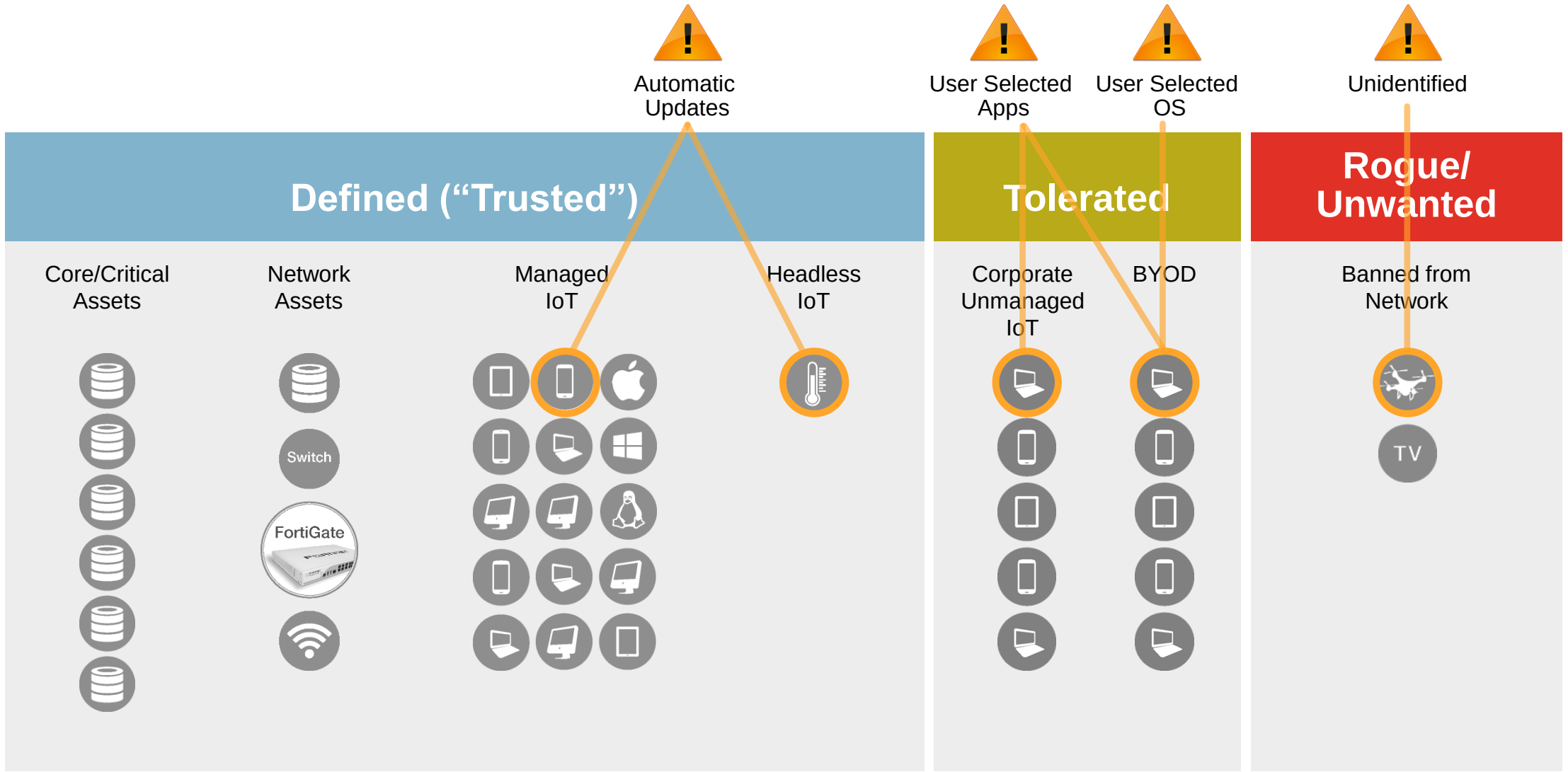
- Learns every change across the network
- Audits the changes for best practices & anomalies
- Analyzes the attack surface against the configuration, real-time data and business rules



IoT : Where Do I Start?

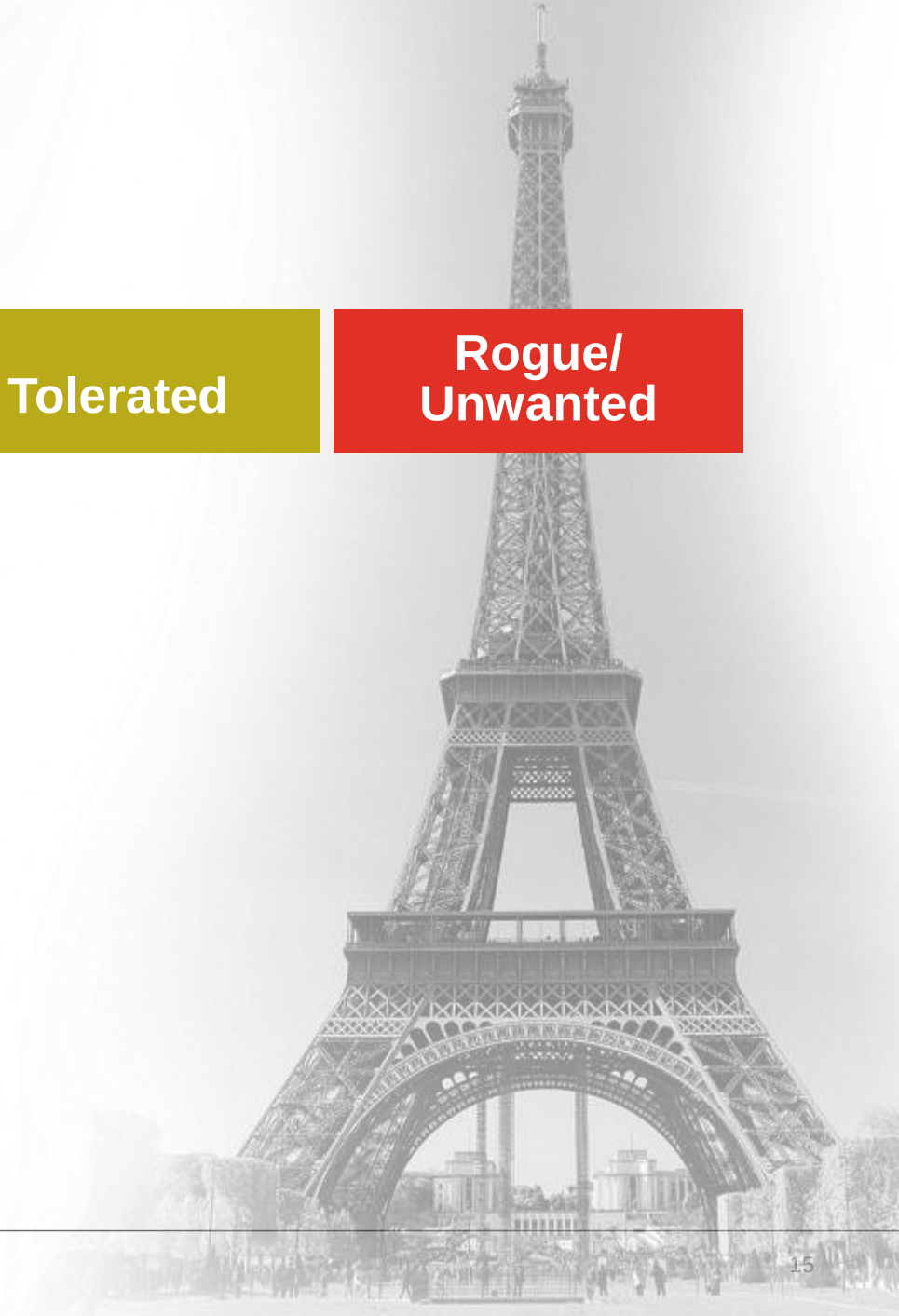


IoT : Where are The Unknowns?

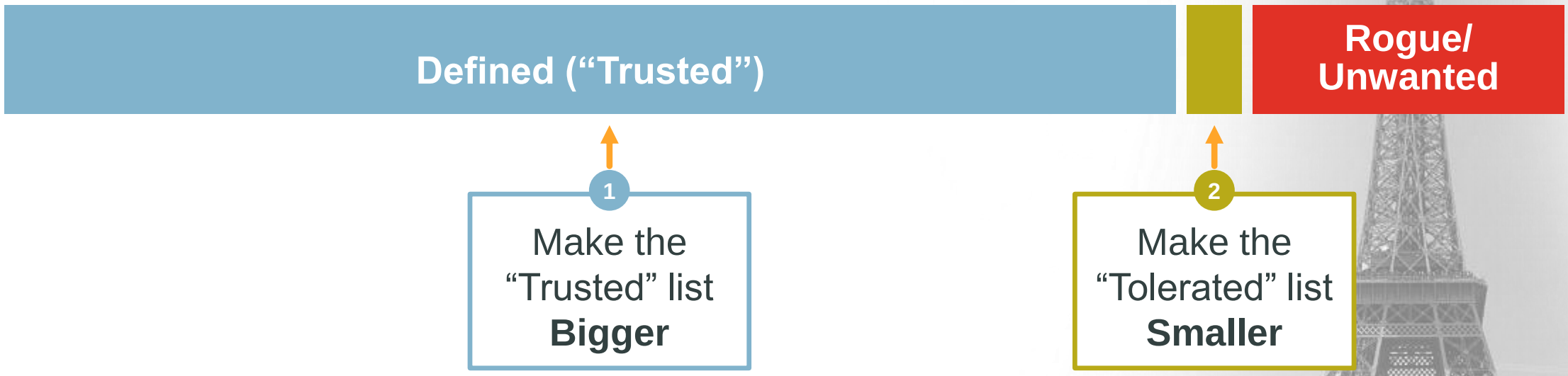


How to Mitigate the Risks?

Defined (“Trusted”)	Tolerated	Rogue/ Unwanted

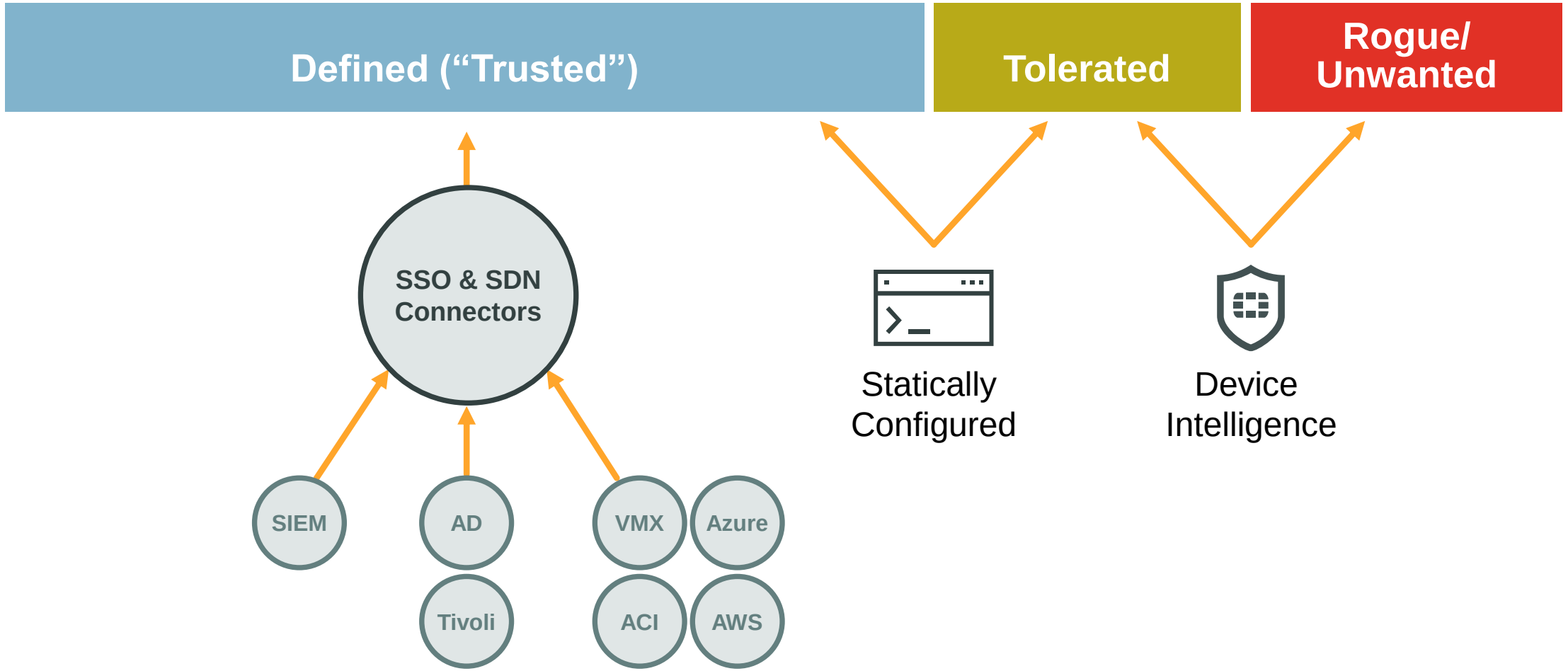


How to Mitigate the Risks?



Building Trust

Knowledge Builds Trust



IoT Manage Capabilities

Reducing the Attack Surface

Learn

Trusted or Not Trusted

Segment

Define a Policy

Protect

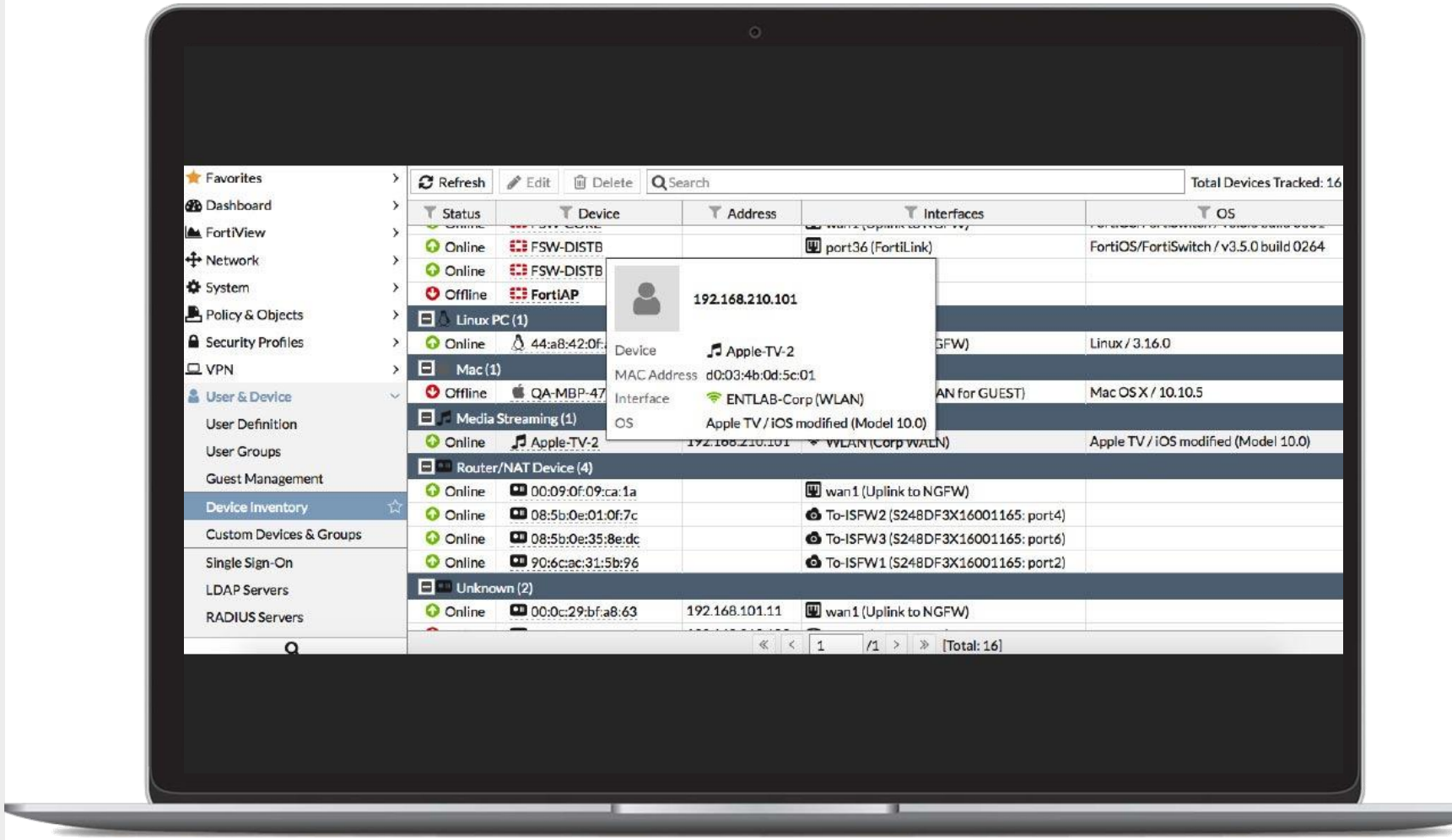
Everything

Step 1 - Learn

Reducing the Attack Surface

Headless Device Auto Detection

- 20+ new categories & New Devices be added added continually and classified

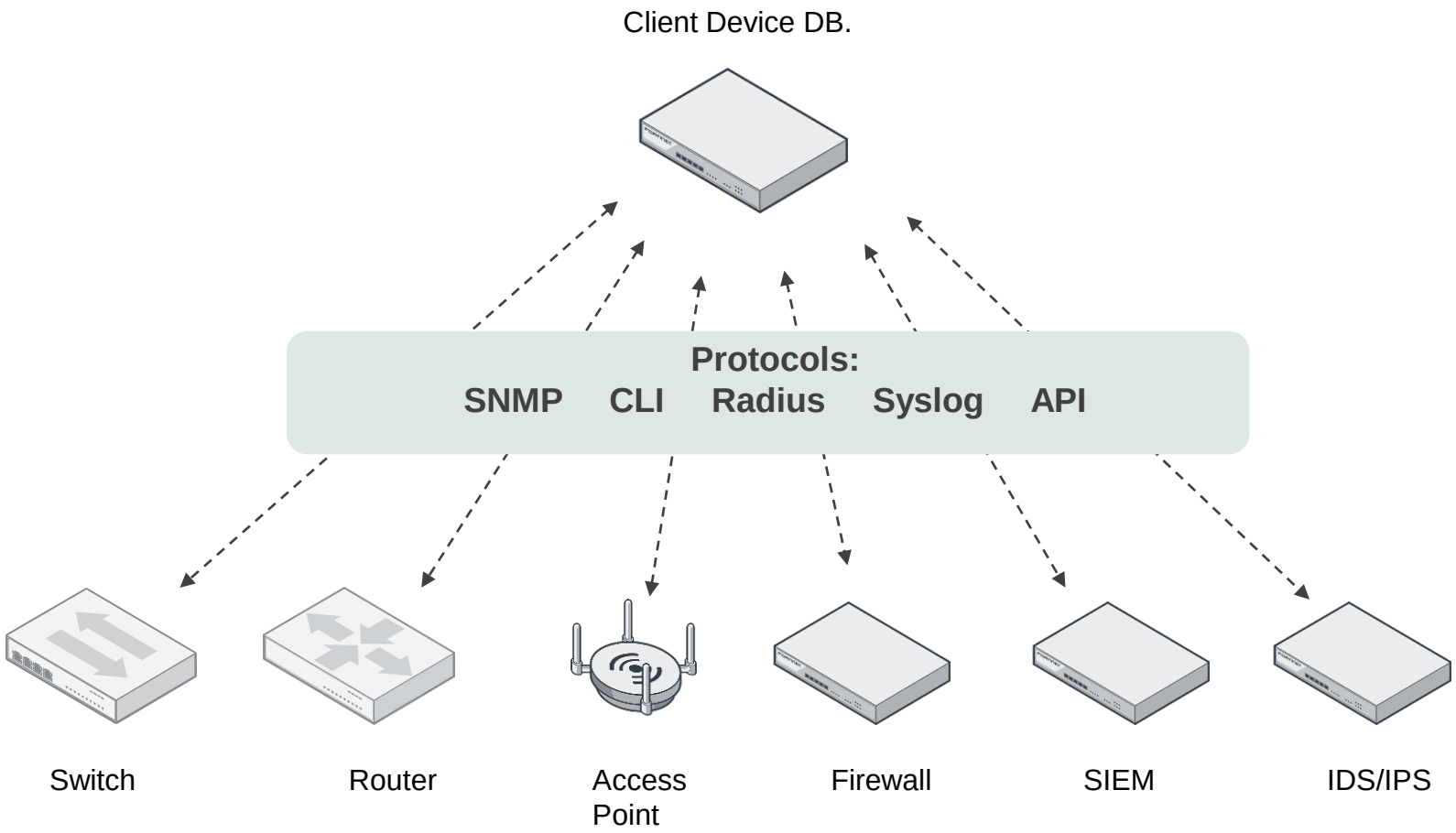


Discovery and Visibility

- Discover all endpoints, IoT devices, users, and applications
  - » Inputs from RADIUS, CLI, SNMP, Syslog, MDM, DHCP, LDAP
  - » Can identify more than 1,500 device types
- Multi-vendor wired & wireless connectivity
  - » Inputs from virtually all vendors and models
- Identify and profile every endpoint
  - » Enables policy rules created by granular device type
  - » Extends vulnerability and patch management to client users
- Self-registration to simplify guest management

Agentless Data Collection

Information gathered from multiple sources



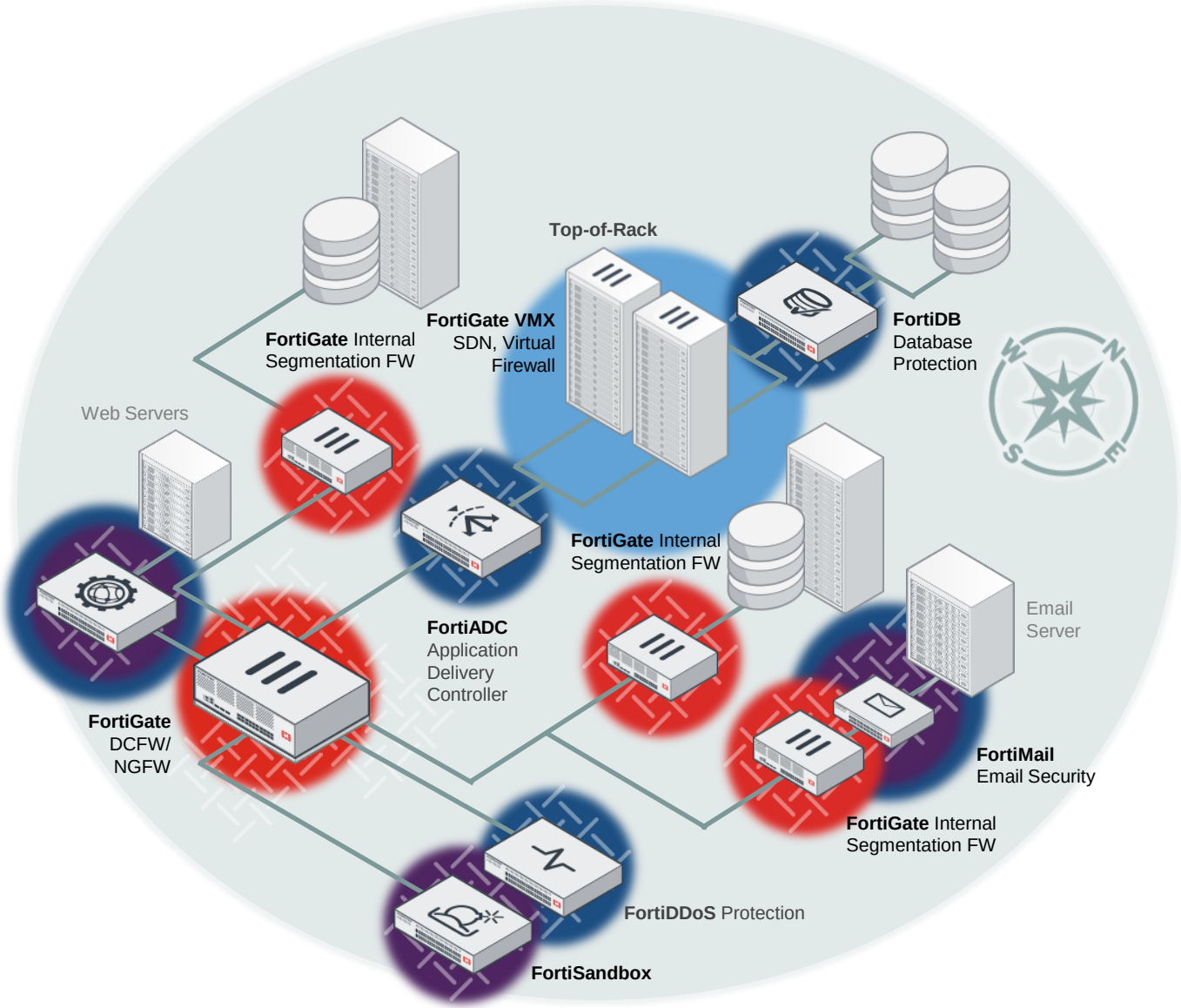
Know everything in your networks

Step 2 – Segment

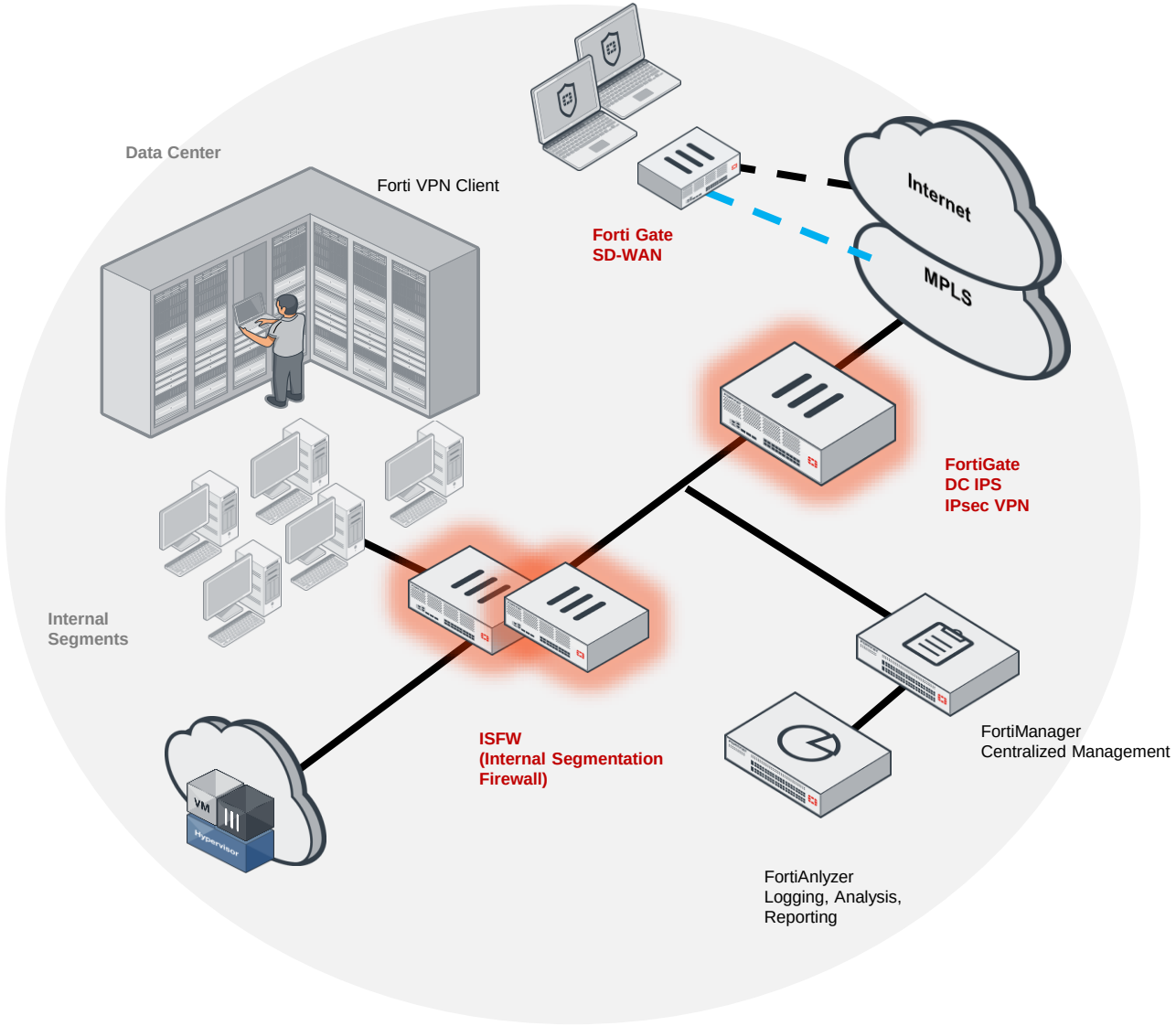
Internal Segmentation

More Firewalls

- Easy to say
- Avoid adding complexity



Why Internal Segment Firewall?



Customer Problem

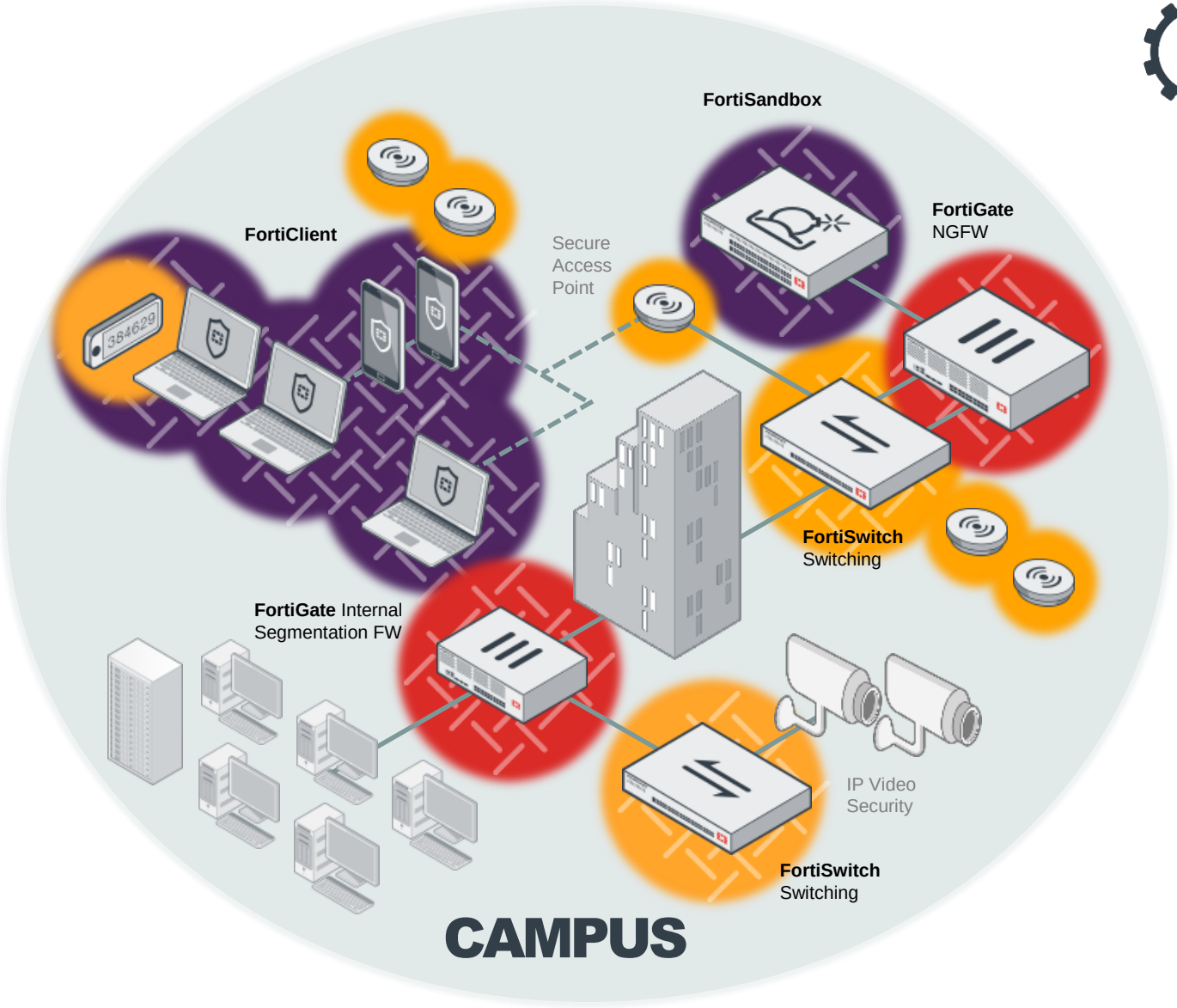
- Internal networks need protection from advanced threats
  - Many ways into the network
  - Lateral movement of malware
- Edge firewalls do not work on internal networks (LAN speeds are 10X WAN speeds)
  - Cost prohibitive
  - Complex to deploy
  - Lacking port density

Step 3 – Protect

Security Template

Enforce

- Within the fabric
  - » Wi-Fi AP
  - » Ethernet Switch
- Block Rogue Devices
- Block traffic not matching security template at the switch or access point
- Generate alert within the fabric – new rogue device?



Step 3 – Protect

Security Template

Define

- Reduce Attack Surface
- Pre-Defined Templates
  - » Ports, protocols
  - » Devices
    - – Voice
    - – Camera
    - – Recorder
      etc
  - » Recognized IoT Devices
    - – Printers
    - – Smart TVs
  - » Popular End Points
    - – Passive Browse
    - – Server
    - – Multiple applications

Step 3 – Protect

Security Template

Discover

- Vulnerability Discovery
- Scan End Point
  - » Weak Passwords
  - » Software Versions
  - » Management Port
- Remediation
  - » Report
  - » Block Ports
- Client Scanning
  - » Managed end points

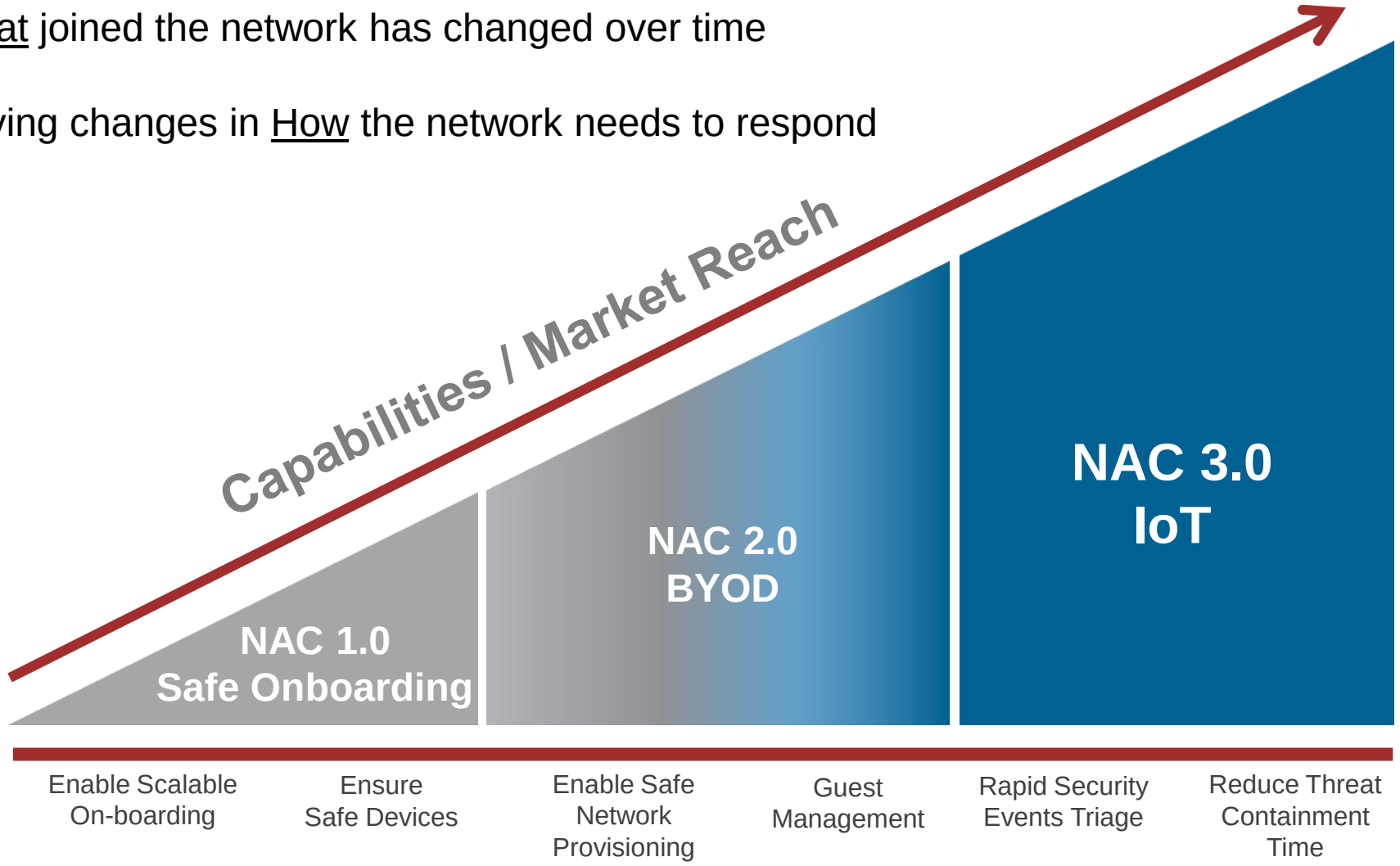
Automated Response

- Bridge the SOC & NOC
  - » Security events move from detection to remediation immediately
- Rapid security event triage
  - » Automated rules can respond in seconds to bad behavior
- Accelerate threat investigations
  - » Device history compiled from multiple sources instantly available
- Granular containment options
  - » E.g., Quarantine or Internet-only connectivity

The Evolution of Network Security

What joined the network has changed over time

Driving changes in How the network needs to respond



How does this improve the Security Fabric?

Visibility

- Agent-less scanning of all devices
  - » Provide FortiClient-type information for even headless devices
- Identify vulnerable devices pre-connect or post-connect
  - » On-going scanning with deep information provides continuous evaluation
  - » Vulnerability and patch management for non-FortiClient devices

Control

- Dynamically control every user and device's level of access
  - » With better device visibility, we can apply profiling policies via FGT
- Ability to configure 3rd party network devices for traffic segmentation

Automated Response

- Reduce containment time from days to seconds
  - » Automated rules in Network Sentry trigger containment settings in FGT, FSW, FAP
  - » More options than current automation stitches in FOS 6.0

THANK YOU

Eric Wu 吳章銘
ericwu@fortinet.net