A Internet das Coisas Muito Ruins

Vitor Vale, Systems Engineer Brazil.

FORTINET

33 bilhões de EndPoints estarão conectados até 2020

Novos tipos de dispostivos se conectando a rede

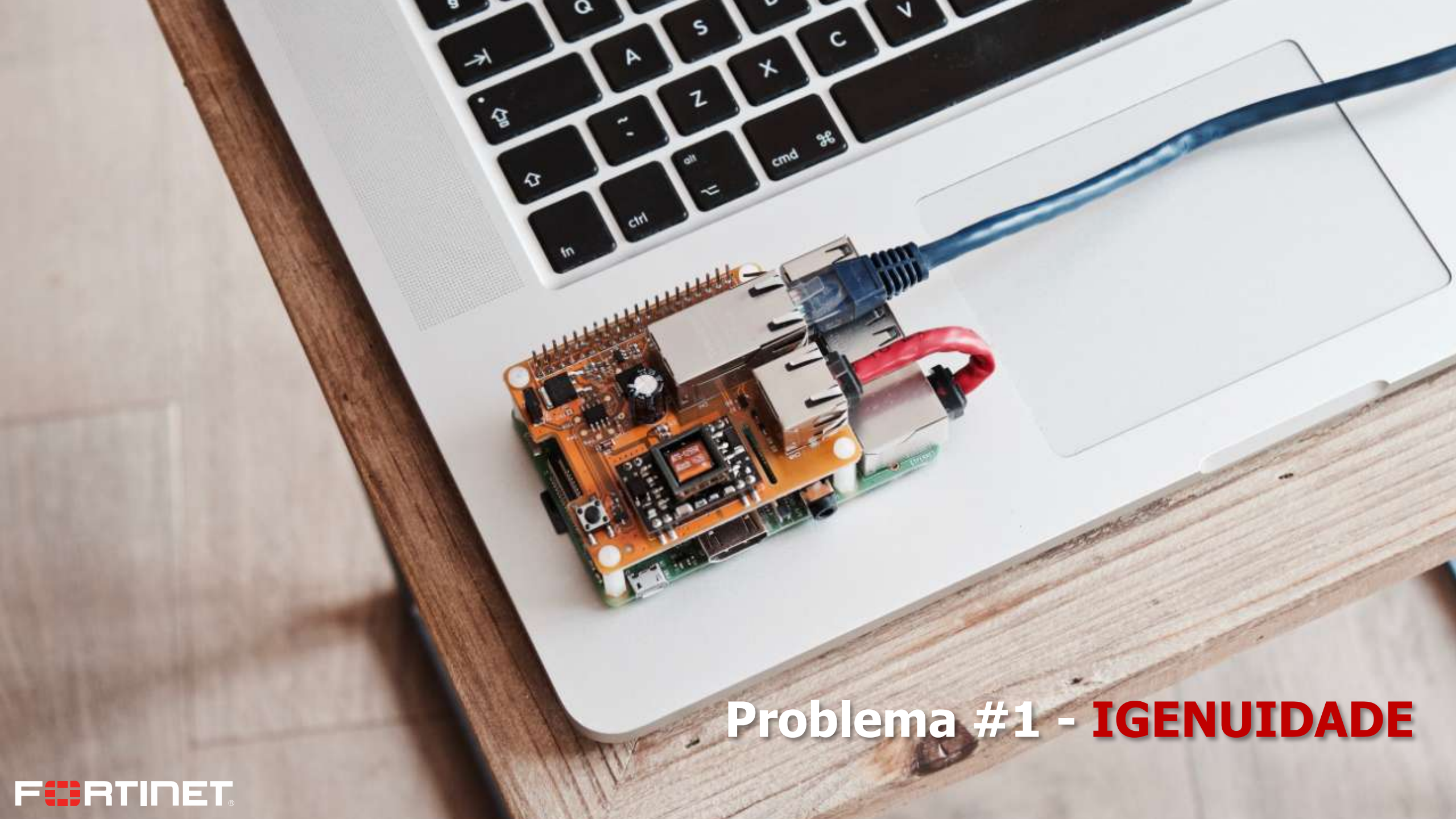
O que é IoT?

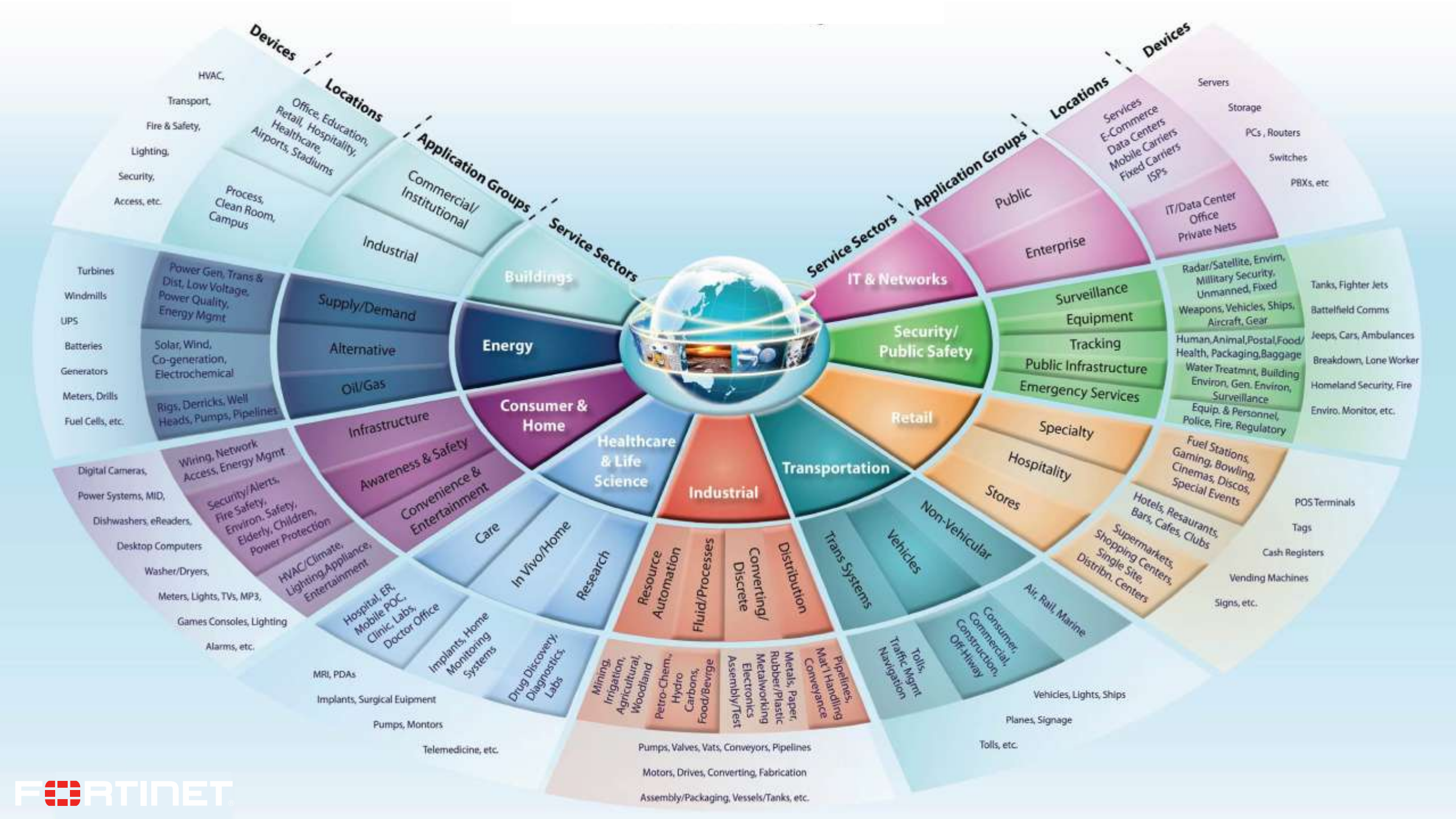
O que as pessoas pensam ...

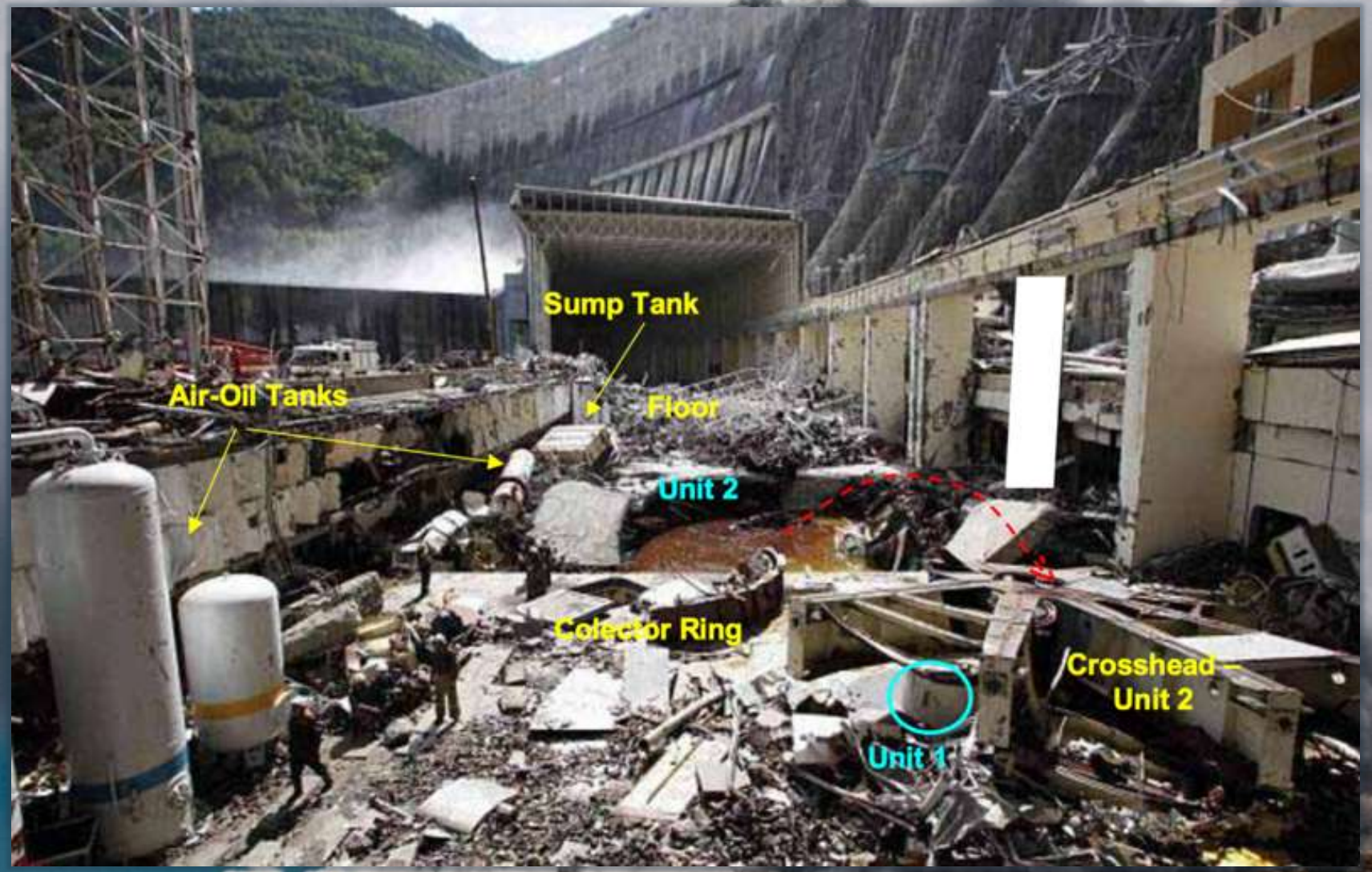
FORTINET

As coisas sérias ...

FORTINET


Problema #1 - IGENUIDADE


Devices
Locations
Application Groups
Service Sectors
HVAC,
Transport,
Fire & Safety,
Lighting,
Security,
Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Energy
Consumer & Home
Healthcare & Life Science
Industrial
Transportation
Retail
Security/ Public Safety
IT & Networks
Public
Enterprise
Services
E-Commerce
Data Centers
Mobile Carriers
Fixed Carriers
ISPs
IT/Data Center
Office
Private Nets
Servers
Storage
PCs , Routers
Switches
PBXs, etc
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Infrastructure
Awareness & Safety
Convenience & Entertainment
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting,Appliance, Entertainment
Digital Cameras,
Power Systems, MID,
Dishwashers, eReaders,
Desktop Computers
Washer/Dryers,
Meters, Lights, TVs, MP3,
Games Consoles, Lighting
Alarms, etc.
Care
In Vivo/Home
Research
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
MRI, PDAs
Implants, Surgical Euipment
Pumps, Montors
Telemedicine, etc.
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Mining, Irrigation, Agricultural, Woodland
Petro-Chem., Hydro Carbons, Food/Beverge
Electronics Assembly/Test
Metals, Paper, Rubber/Plastic Metalworking
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.
Trans Systems
Vehicles
Non-Vehicular
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hiway
Air, Rail, Marine
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.
Specialty
Hospitality
Stores
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Radar/Satellite, Envirn, Military Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets
Battelfield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.


Sump Tank
Air-Oil Tanks
Floor
Unit 2
Colector Ring
Crosshead –
Unit 2
Unit 1

Problemas #2 – Os Dispositivos

FORTINET

IoT como o elo mais fraco

FORTINET

IoT e DDoS

1.35 Tbps (2018)

FORTINET

Problema #3 – Rede Acadêmica

Superfície de Ataque Única

Research Branch

Academic Branch

Administrative Branch

A tempestade perfeita

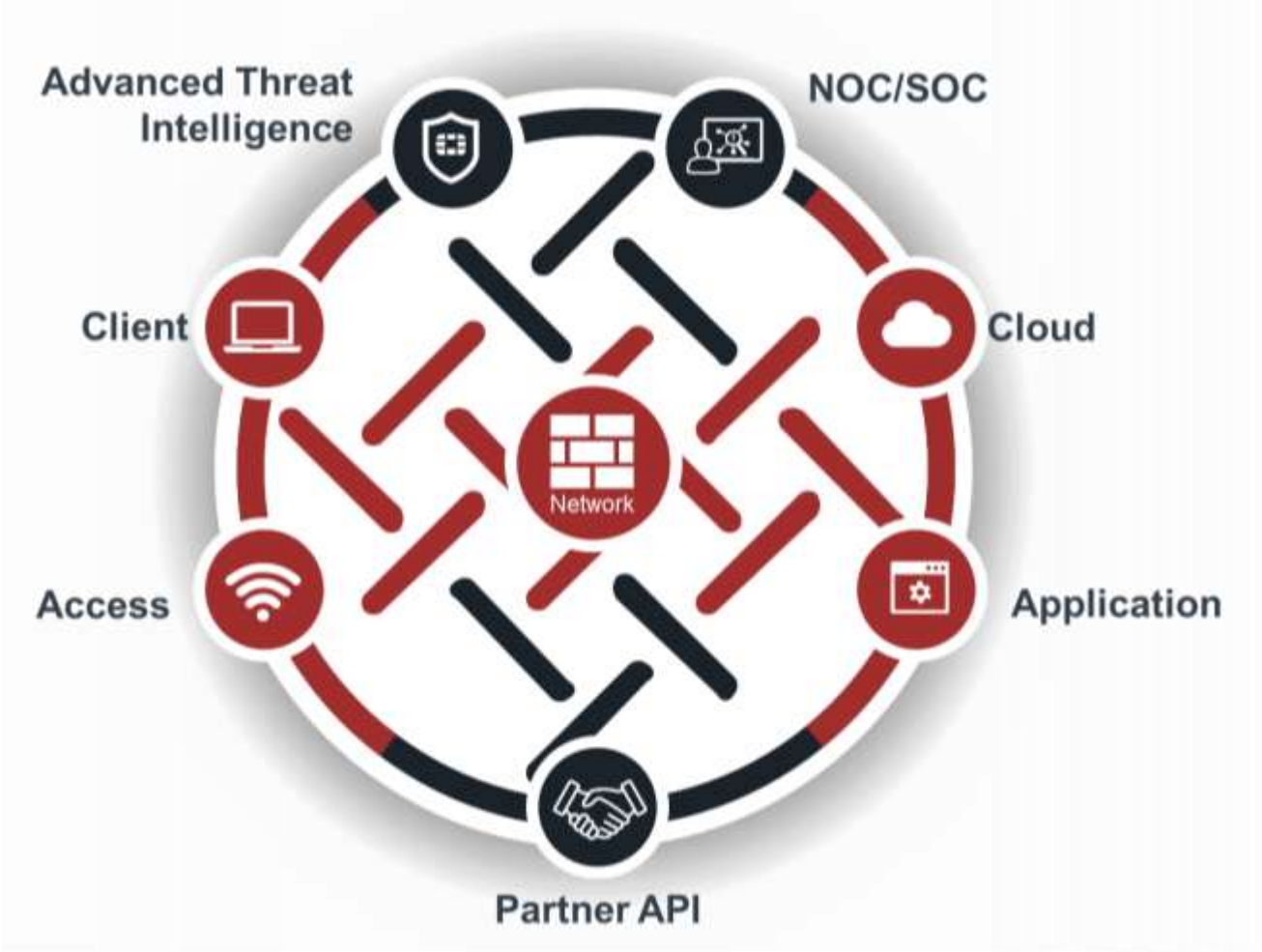
Aberto
Dinâmico
Heterogênio

Exposto
Propagação de Malware
Muitos Pontos de Entrada

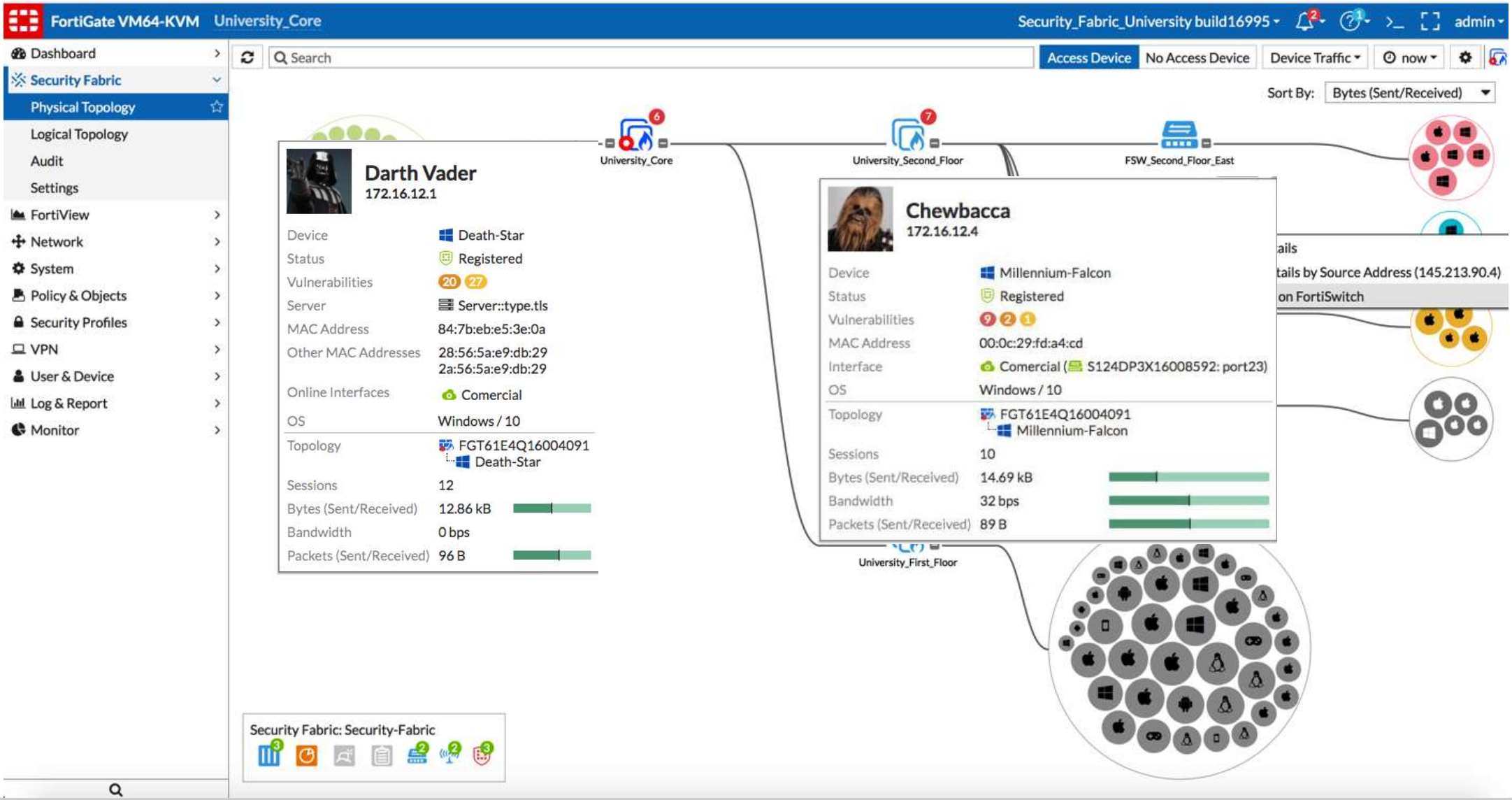
O Papel da Fortinet na Proteção do Ecossistema de IoT

Security Fabric

Conjunto interconectado de Elementos de Segurança que abrange o ecossistema em rede para proteger toda a superfície de ataque do IoT até a Nuvem

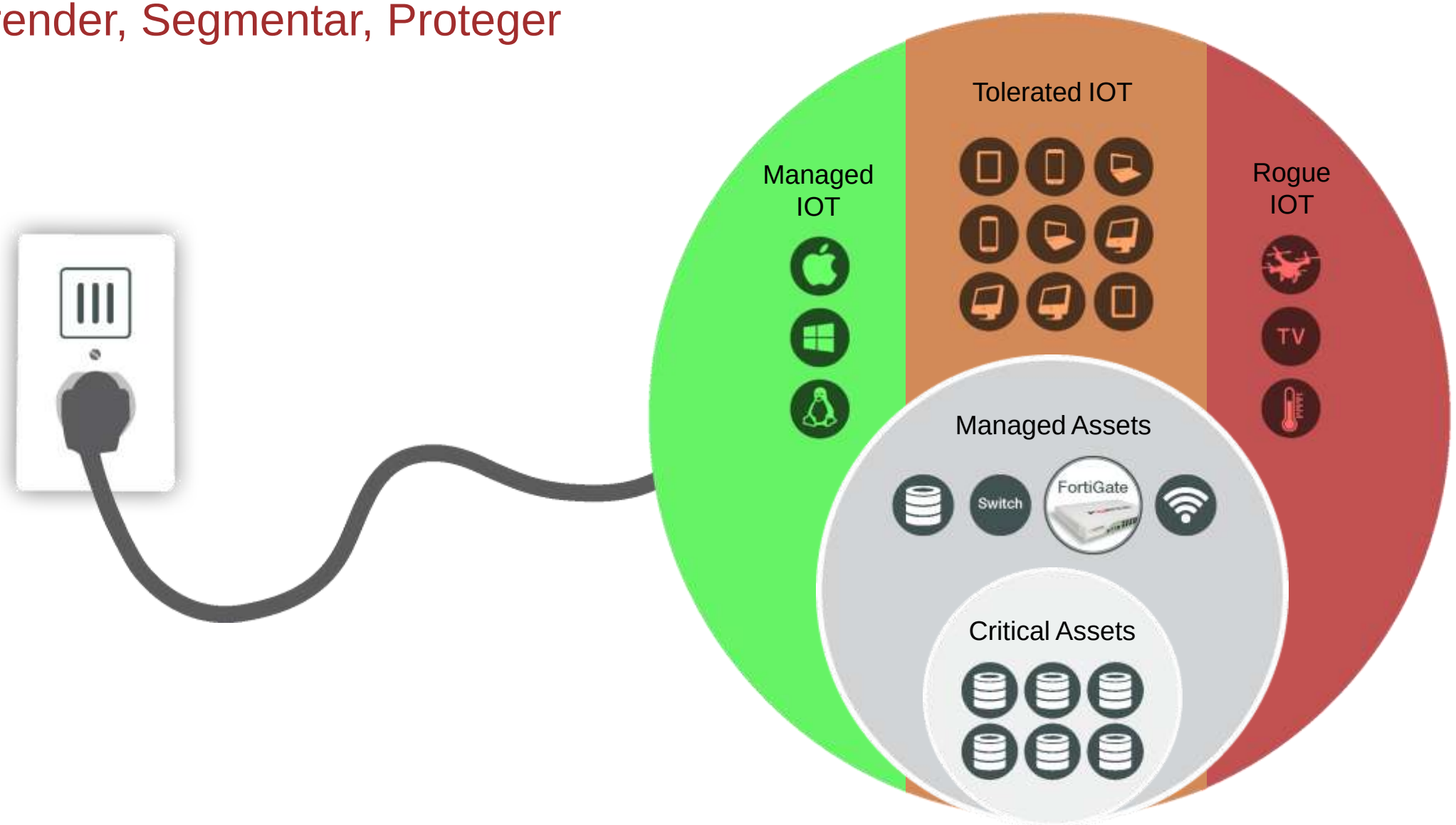


Uma Postura de Segurança Única Para Toda a Rede



Estratégia de Segurança de IoT

Aprender, Segmentar, Proteger

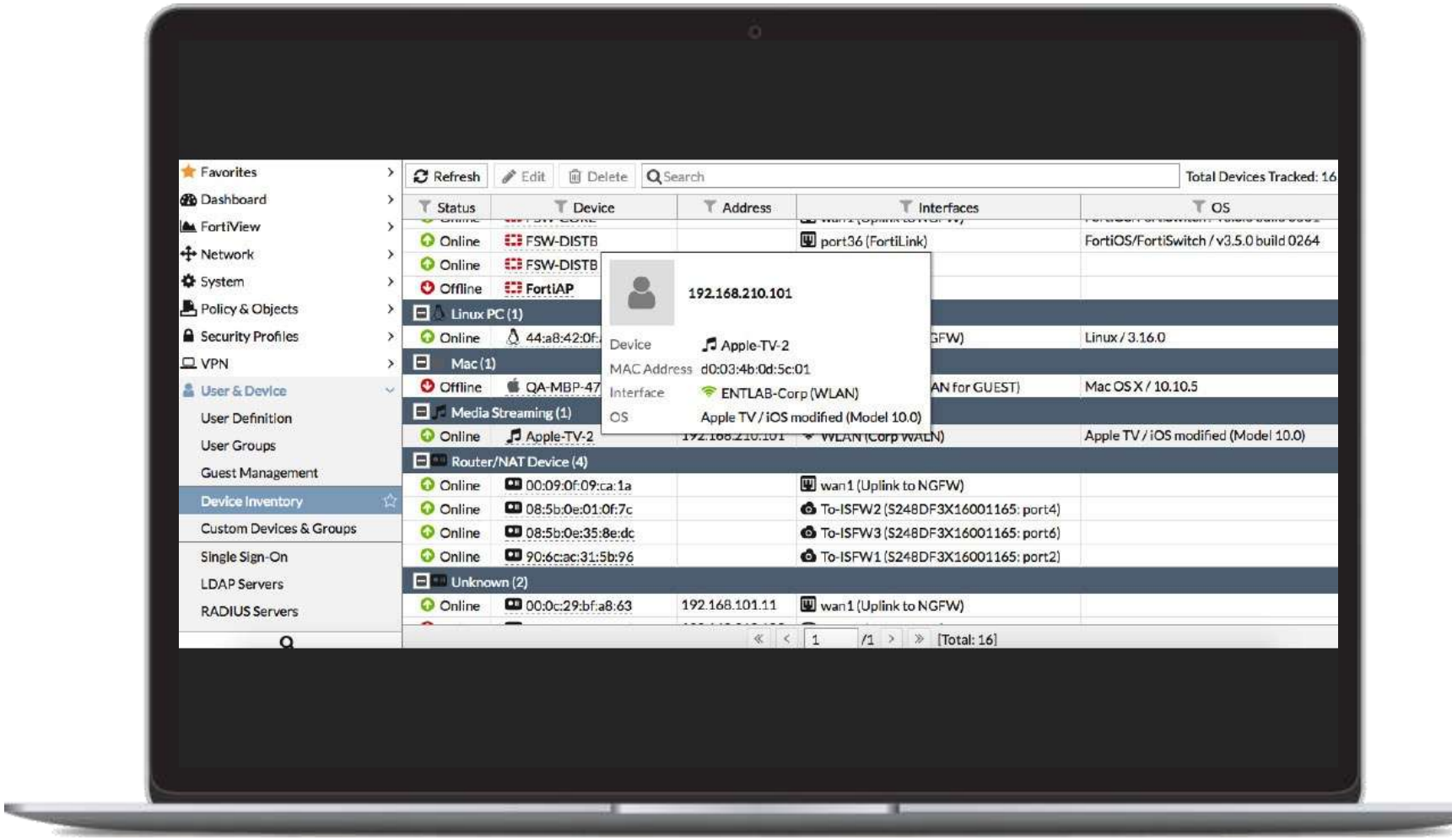


Passo 1 - Aprender

Descoberta e Identificação

Descoberta de Dispositivo
Detecção Automática

- Dispositivos devem ser adicionados e continuamente classificados
- Perfil do dispositivo
- Marcação de dispositivos

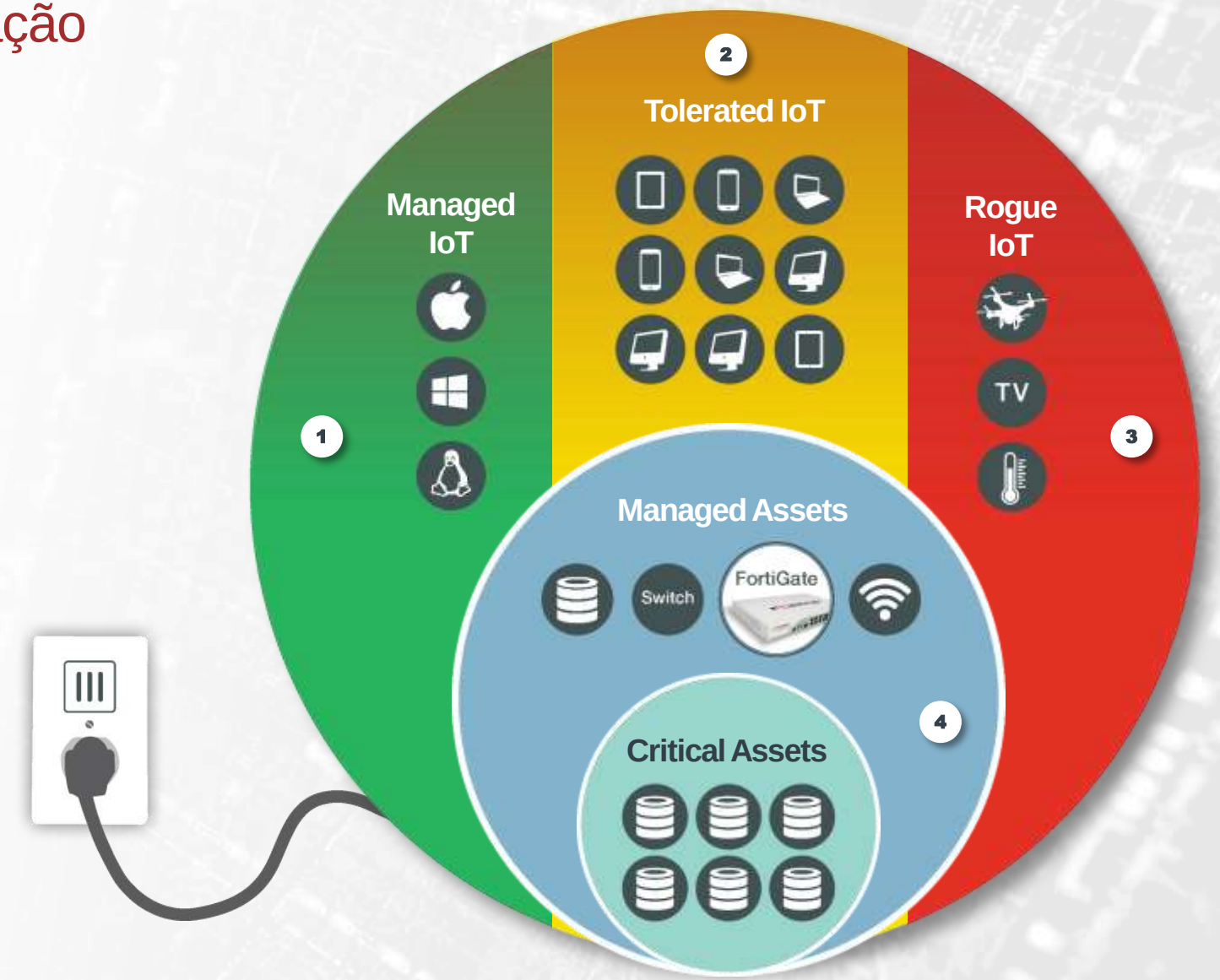


Passo 2 - Segmentar

Security Fabric – Segmentação

Segmentar Rede IoT

1. Gerenciado Centralizadamente
   - Acesso Amplo
2. Não Gerenciado
   - Acesso Restrito
3. Não Permitido
4. 3rd Party DBs
   - Tivoli
   - AD
   - SIEM
   - VM Tools

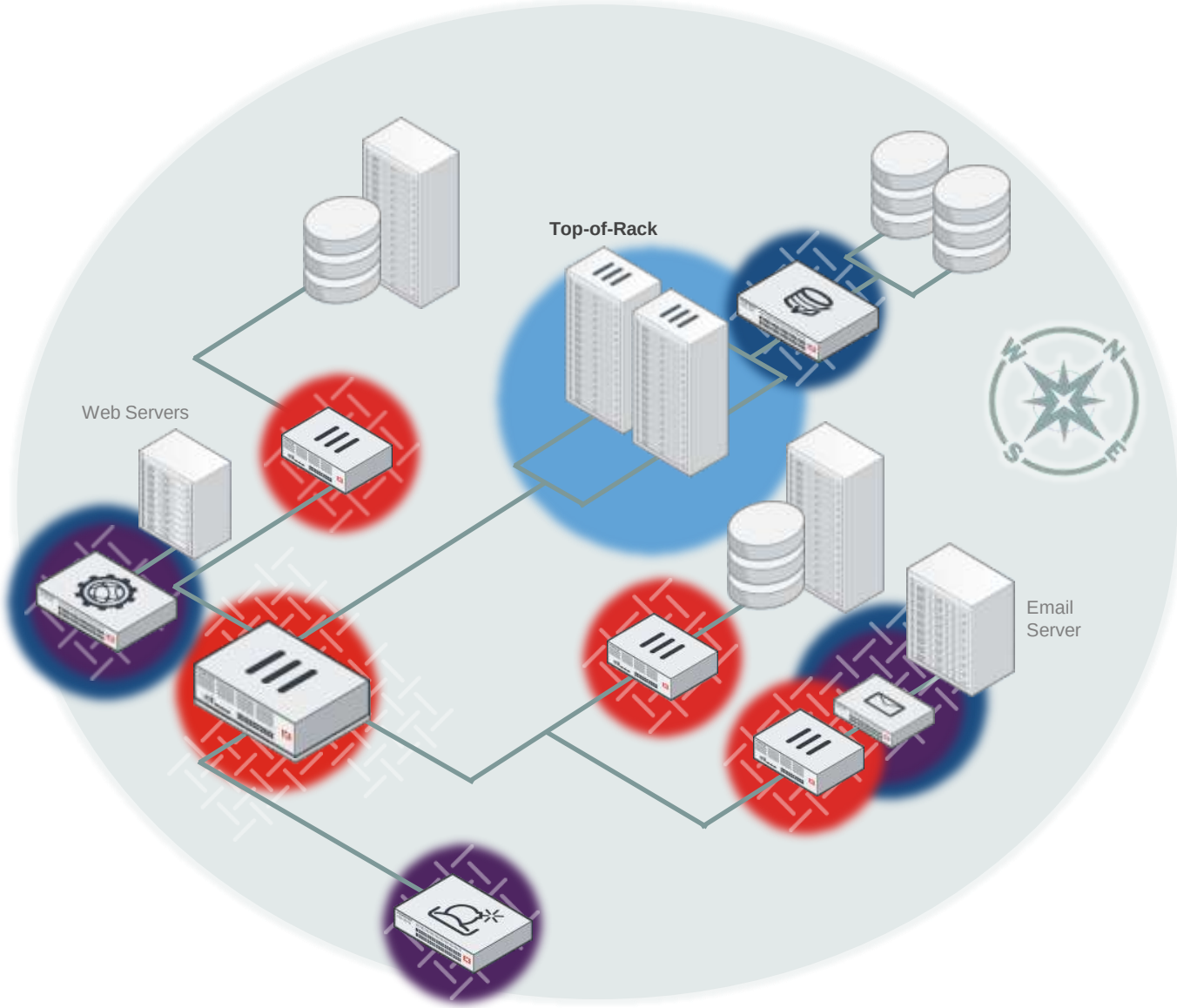


Passo 2 – Segmentar

Segmentação Interna

Segmentar baseado no Perfil de Risco

- Firewall de Segmentação Interna (Físico e Virtual)
- Políticas podem ser aplicacadas para restringir a comunicação com redes e aplicativos específicos
- Regras de autenticação para controlar o acesso
- Diminuir a Complexidade



Passo 3 – Proteger

Modelo de Segurança

Defina

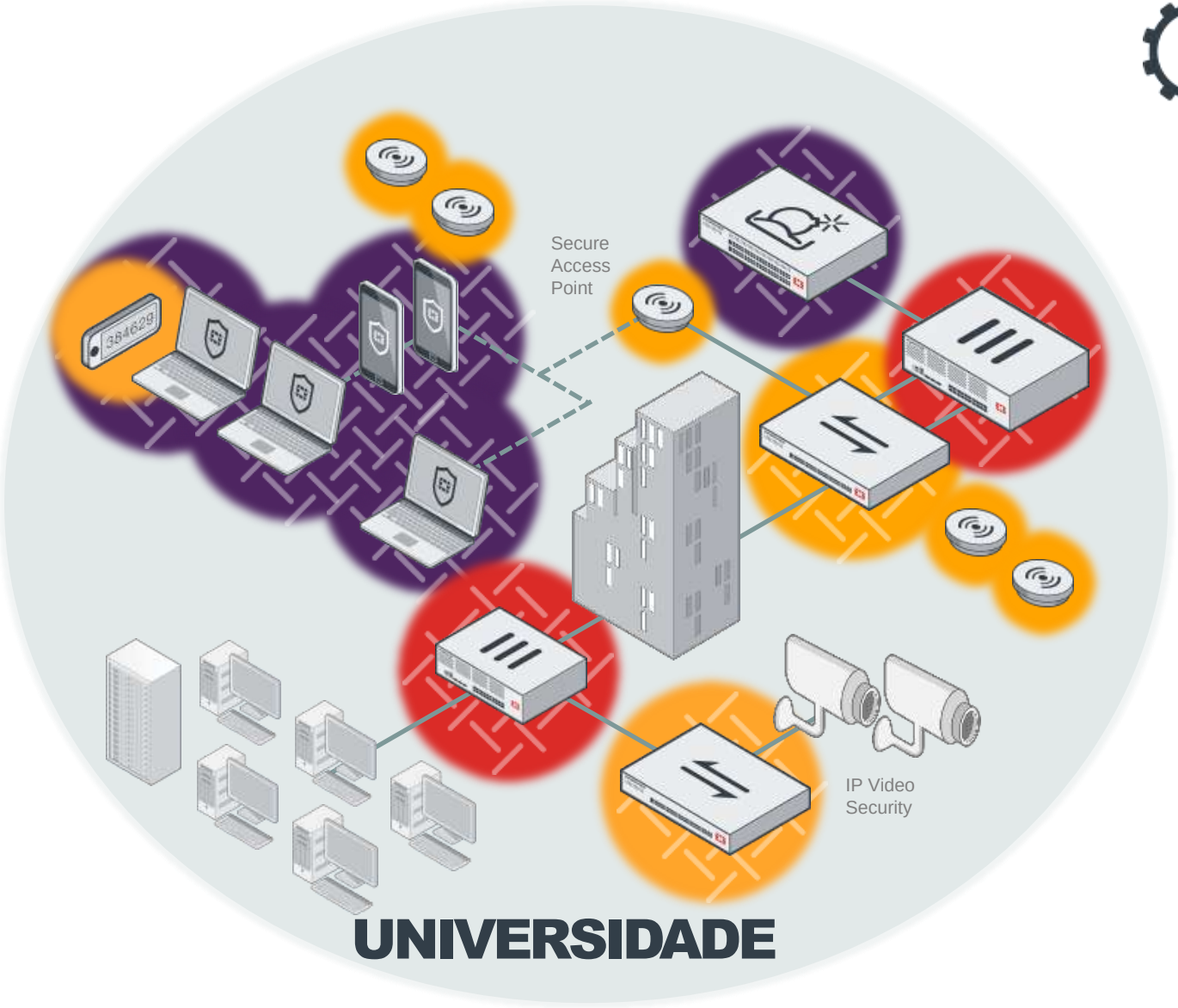
- Política de segurança adaptativa baseada em inteligência
- Modelos pré-definidos
  - » Portas, protocolos
  - » Dispositivos de Rede
  - » Dispositivos IoT Reconhecidos
    - Impressoras
    - Smart TVs
  - » End Points Populares
    - Browse Passivo
    - Servidor
    - Múltiplas Aplicações

Passo 3 – Proteger

Modelo de Segurança

Enforce

- Bloqueio/Quarentena de dispositivos não autorizados
- Bloquear tráfego de rede que não combina com o modelo de segurança no switch ou AP
- Gerar alerta na console de gerenciamento – dispositivo não autorizado?



FORTINET