Powerful Forces Impacting the Enterprise – Can Your Network Withstand Them?

Patrick Grillo, Senior Director Security Strategy

© Copyright Fortinet Inc. All rights reserved.

What's Going On With The Enterprise?

Change, Change and Some More Change

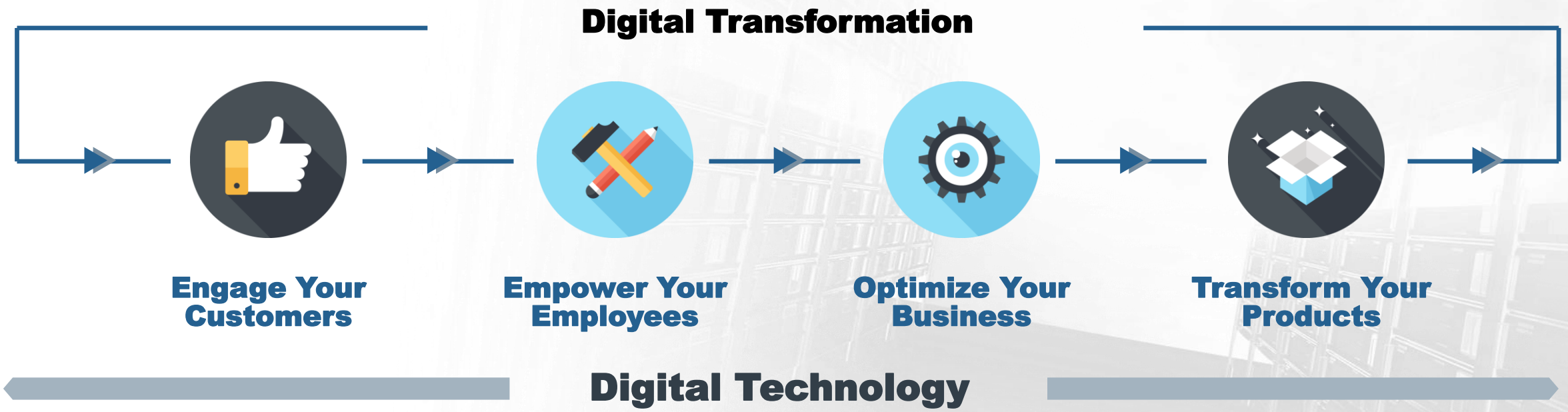
Three Out of Many Concerns

DIGITAL TRANSFORMATION

CYBER THREATS

COMPLIANCE

Digital Transformation



Securing the Digital enterprise

"…in the digital era, [security] focus needs to shift from securing network perimeters to safeguarding data spread across systems, devices, and the cloud."

MIT Technology Review, 2017

Mobile Devices

Augmented Reality/Wearables

IoT Platforms

Cloud Computing

Bid Data Analytics and Advanced Algorithms

Multi-level Customer Interaction and Customer Profiling

3D Printing

Location Detection Technologies

Smart Sensor

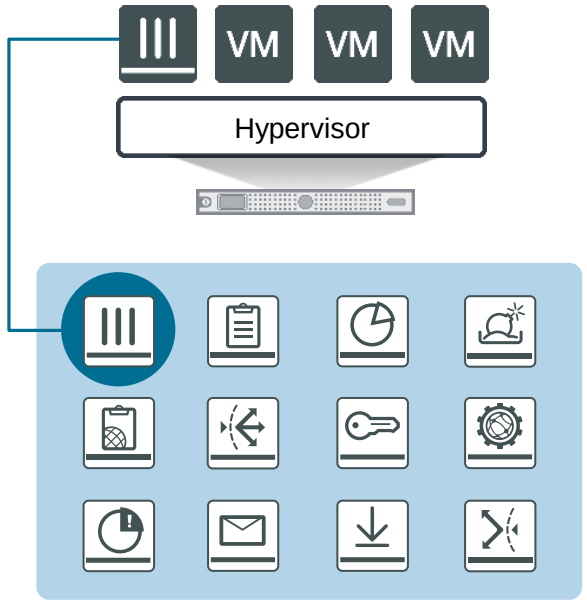
Advanced Human-machine Interfaces

FOCUS #1
VIRTUALIZATION AND CLOUD

Putting the “S” in Virtualisation

Virtualization

Hypervisor Port



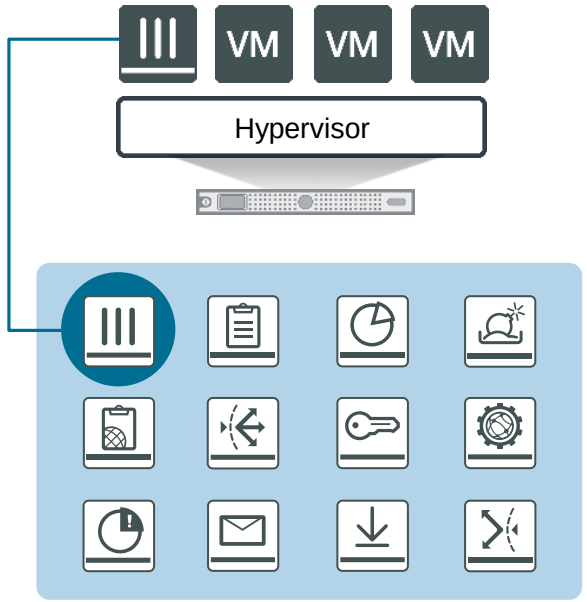
From Virtualization to Private Cloud and Beyond

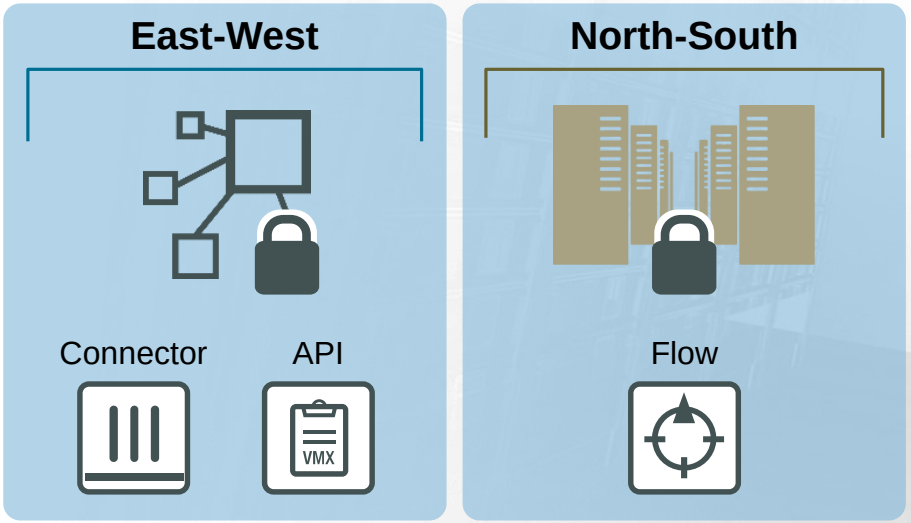
Micro Segmentation and Managing Volume

Virtualization → Private Cloud

Hypervisor Port

SDN / Orchestration





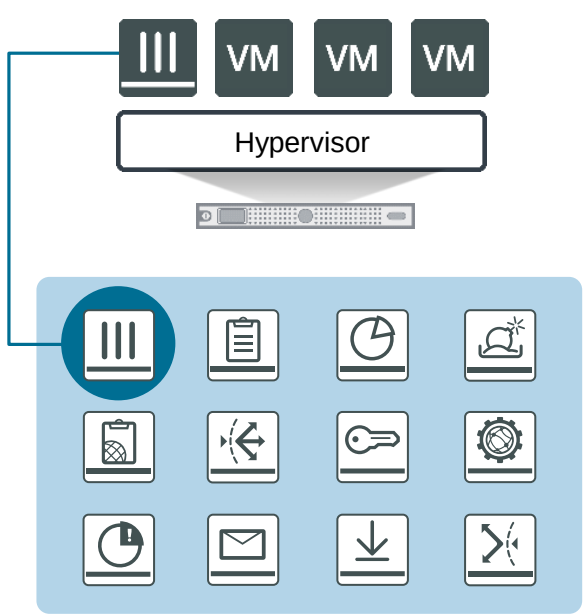
Continuing the Journey - Maybe

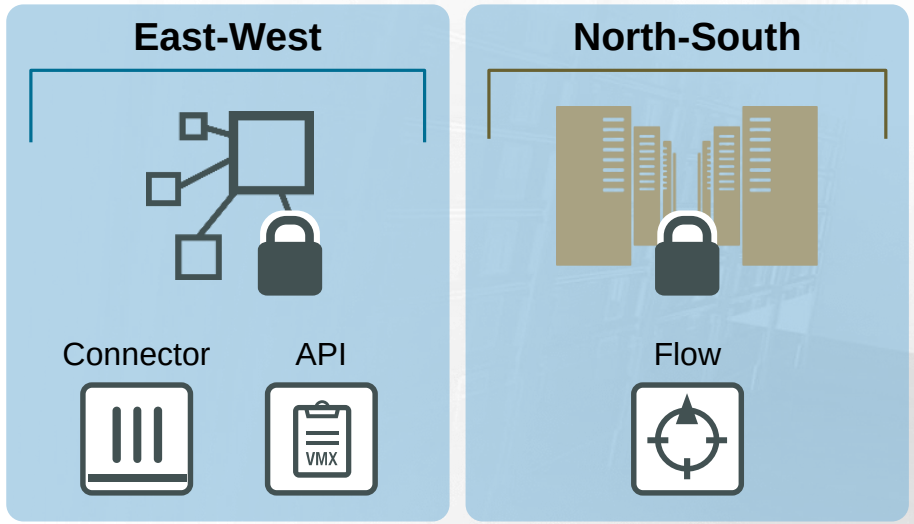
Virtualization → Private Cloud ↔ Hybrid ↔ Public Cloud

Hypervisor Port

SDN / Orchestration

On-Demand





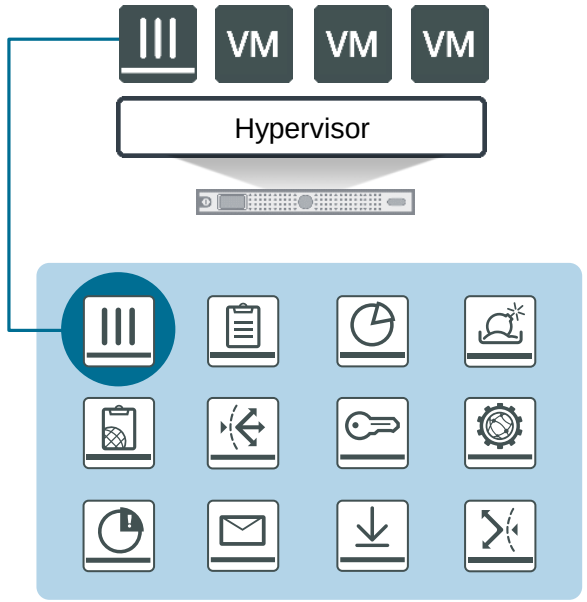
Continuing the Journey - YES

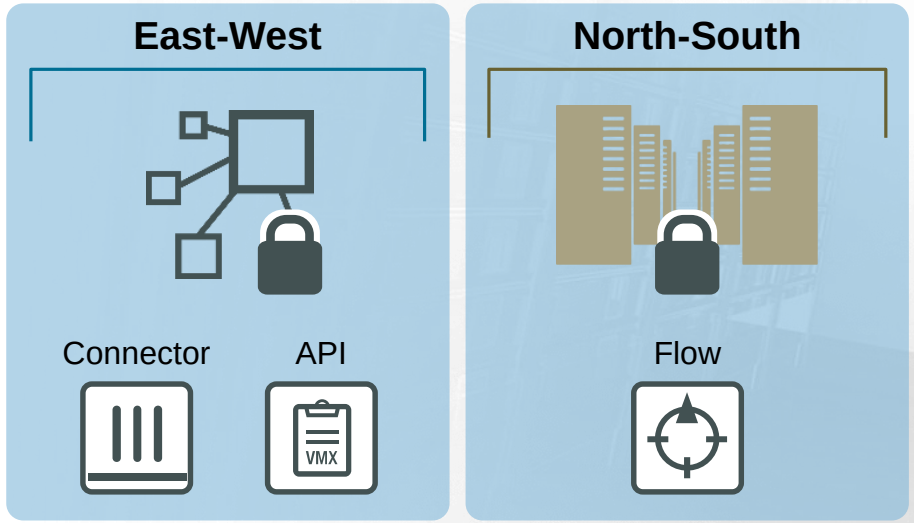
Virtualization → Private Cloud ↔ Hybrid ↔ Public Cloud

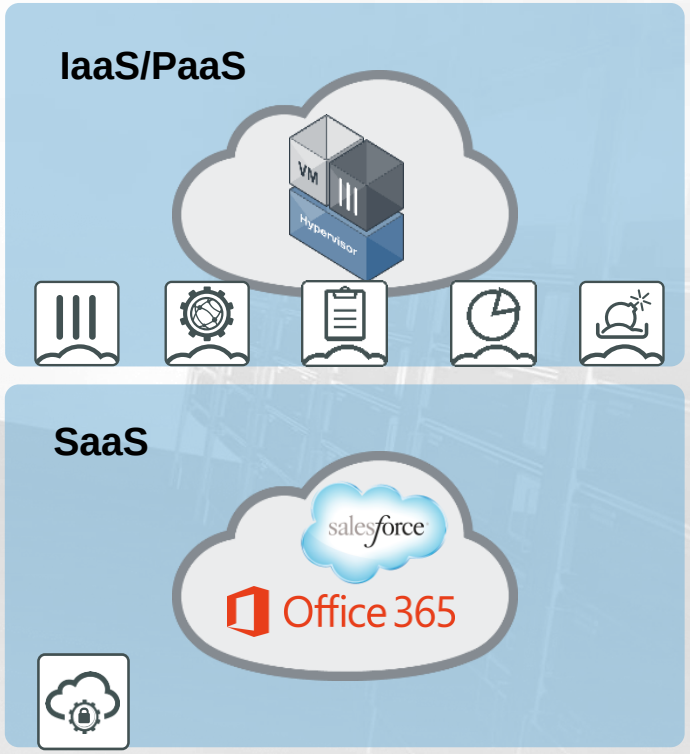
Hypervisor Port

SDN / Orchestration

On-Demand

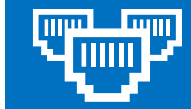






FOCUS #2
SOFTWARE DEFINED OUTSIDE OF THE DATA CENTER – SD WAN

The Problem…



70%

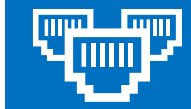
Of customers mentioned existing WAN is brittle, slow, expensive and

not effective for cloud adoption

Gartner

Market guide for SDWAN, 2017

The Problem…And the Solution



70%

Of customers mentioned existing WAN is brittle, slow, expensive and

not effective for cloud adoption

Gartner

Market guide for SDWAN, 2017

SD-WAN

- **WAN transport agnostic**
- **Load sharing across multiple WANs**
- **Simplified management**
- **Integration of additional network services.**

Gartner

Market guide for SDWAN, 2017

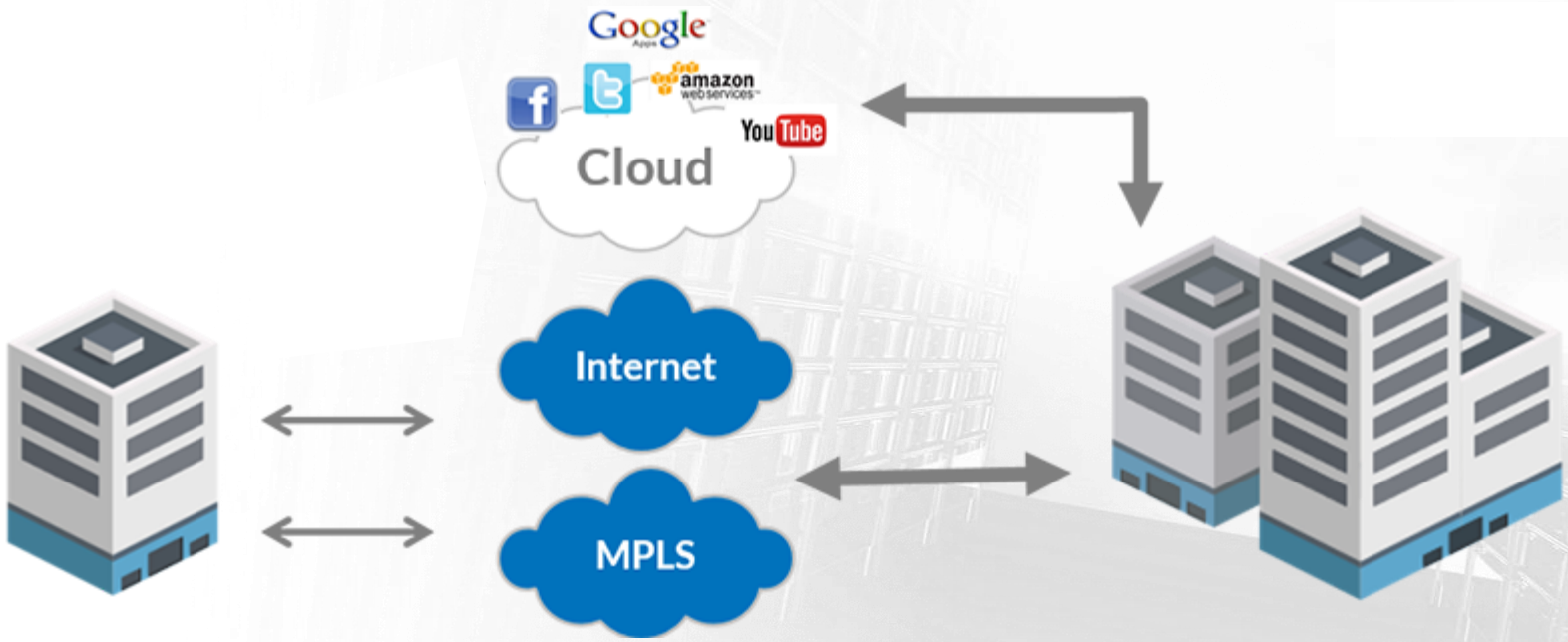
Rapidly Growing SD-WAN Market

By the end of 2019, 50% of enterprises will use SD-WAN technology in all their branches, up from less than 5% today - **Gartner (October 2017)**

SD-WAN market is highly disruptive force expected to grow 76.2% through 2020 to become $1.2B Market - **Gartner (March 2017)**

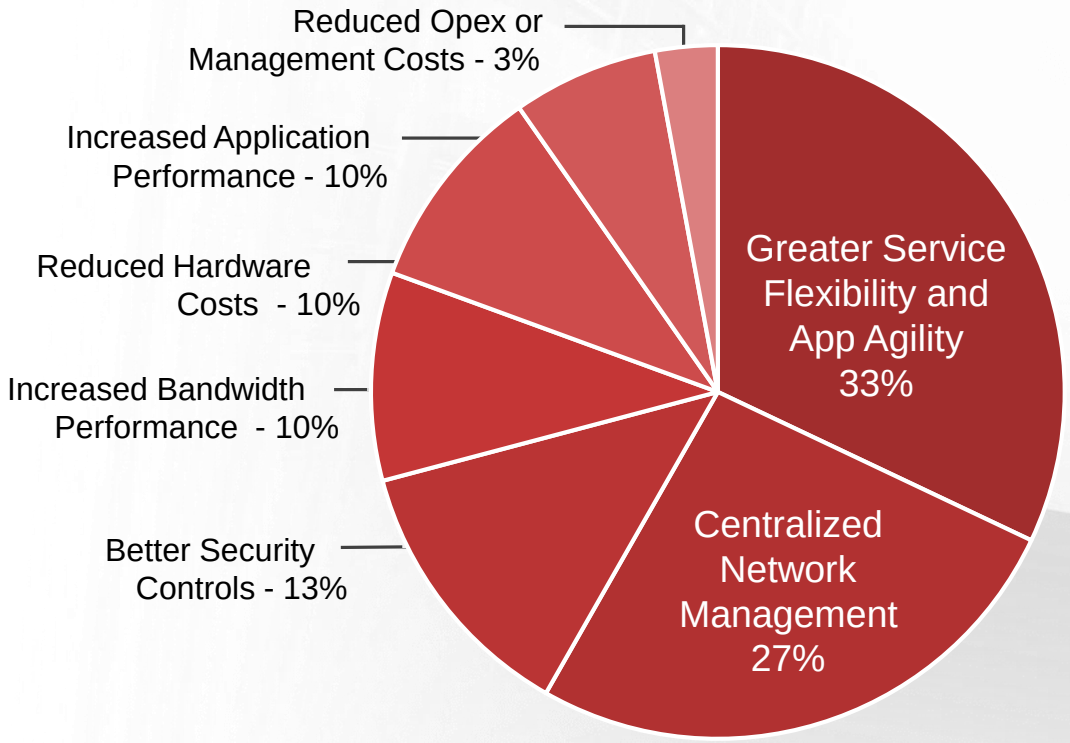
90% of the SD-WAN vendors do not offer Security. Integrated security is a key requirement for customers enabling direct Internet access — **Gartner (October 2017)**

But What is an SD-WAN?



The Drivers Behind SD WAN

Enterprise Primary Drivers



SDWAN survey, 2016

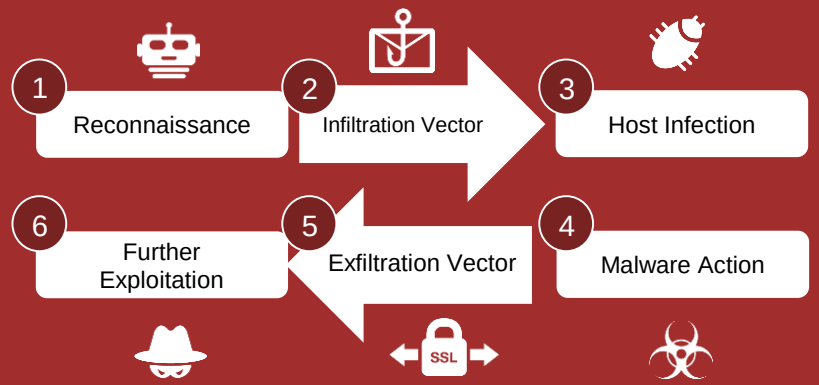
Security is Critical for Direct Internet Access

Volume

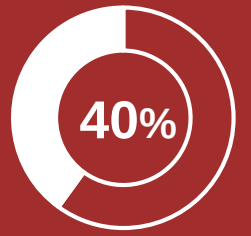
500,000
IPS attacks per minute

Advanced

Kill Chain



SSL Traffic

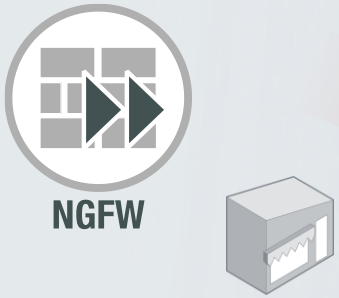


Over 40%
of browsing done in HTTPS (SSL)

The Argument for Secure SD-WAN

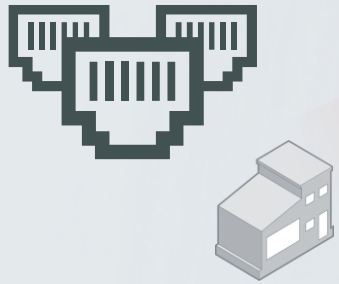
Branch Security

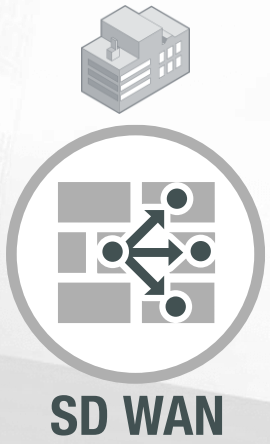
- NGFW Security
- Better Visibility
- Scalable Management



Branch WAN

- Multiple WAN Links
- Direct Internet Access
- Easy to deploy





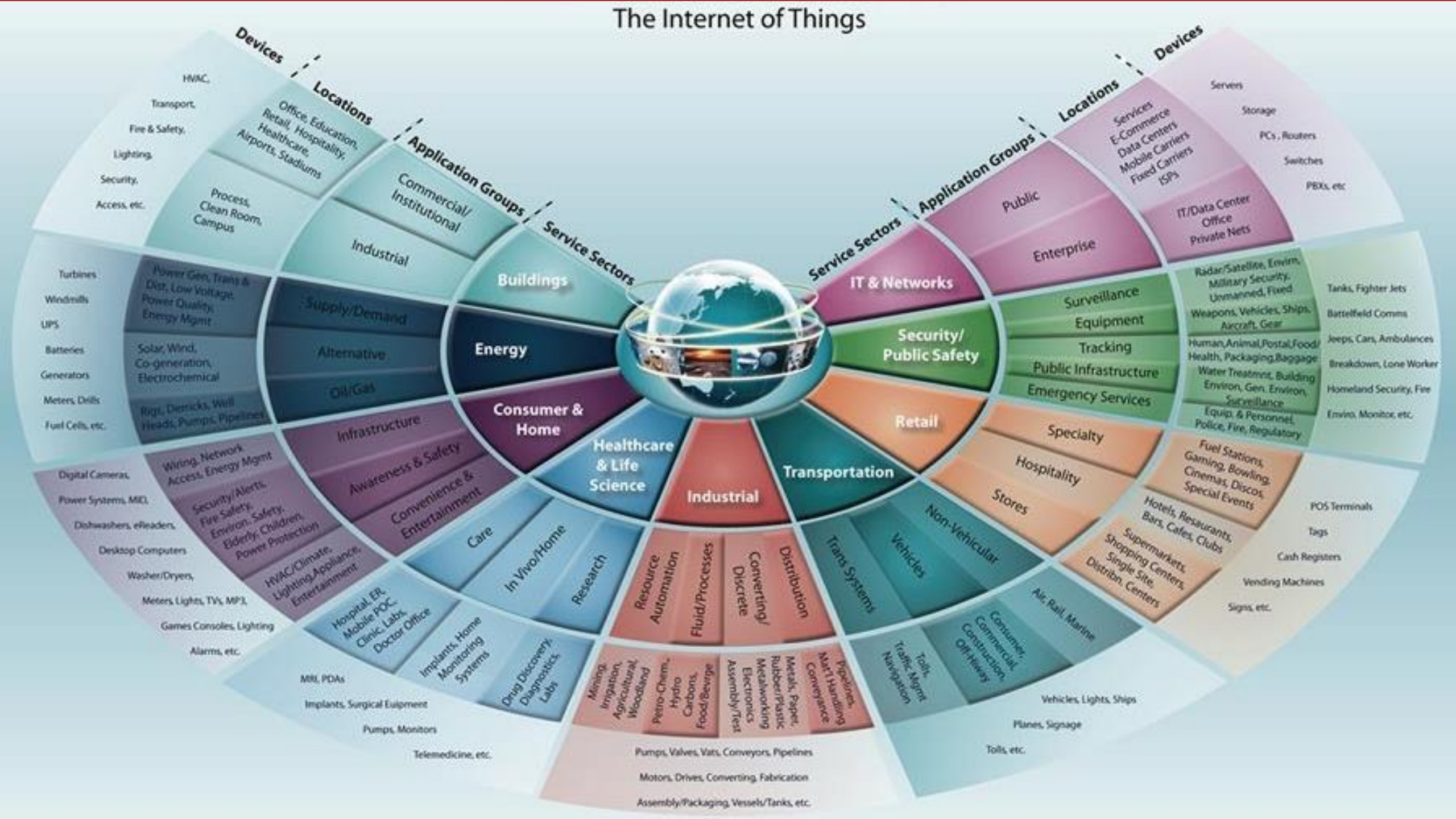
Secure SD-WAN

- NGFW Security
- Efficient SaaS adoption
- Reduce WAN cost
- Zero-touch Deployment

FOCUS #3
THE INTERNET OF THINGS

www.jklossner.com
©14 c'world klossner
"WE HAVE TO GO OUT FOR DINNER. THE REFRIGERATOR ISN'T SPEAKING TO THE STOVE."

The Internet of Things



Did You Also Know*?

- Nuclear Facilities (US)
  - » More than 150 successful cyber attacks between 2010 & 2014
- Building Infrastructure
  - » Temperature and fire control systems
- Oil Rigs
  - » Hacker induced instability
- Firearms
  - » Smart weapons with WiFi
- Airplanes
  - » Access flight control via entertainment system
- Kitchen (UK)*
  - » Toaster refusing to toast white bread
  - » Freezer shutting down when ice cream detected

*The 10 Most Terrifying IoT Security Breaches you aren't aware of (so far) LinkedIn September 2015

IoT – The Ever Changing Attack Surface

- 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
- Your network should..
  - » Learn every change across the network
  - » Audit the changes for best practices & anomalies
  - » Analyze the attack surface against the configuration, real-time data and business rules

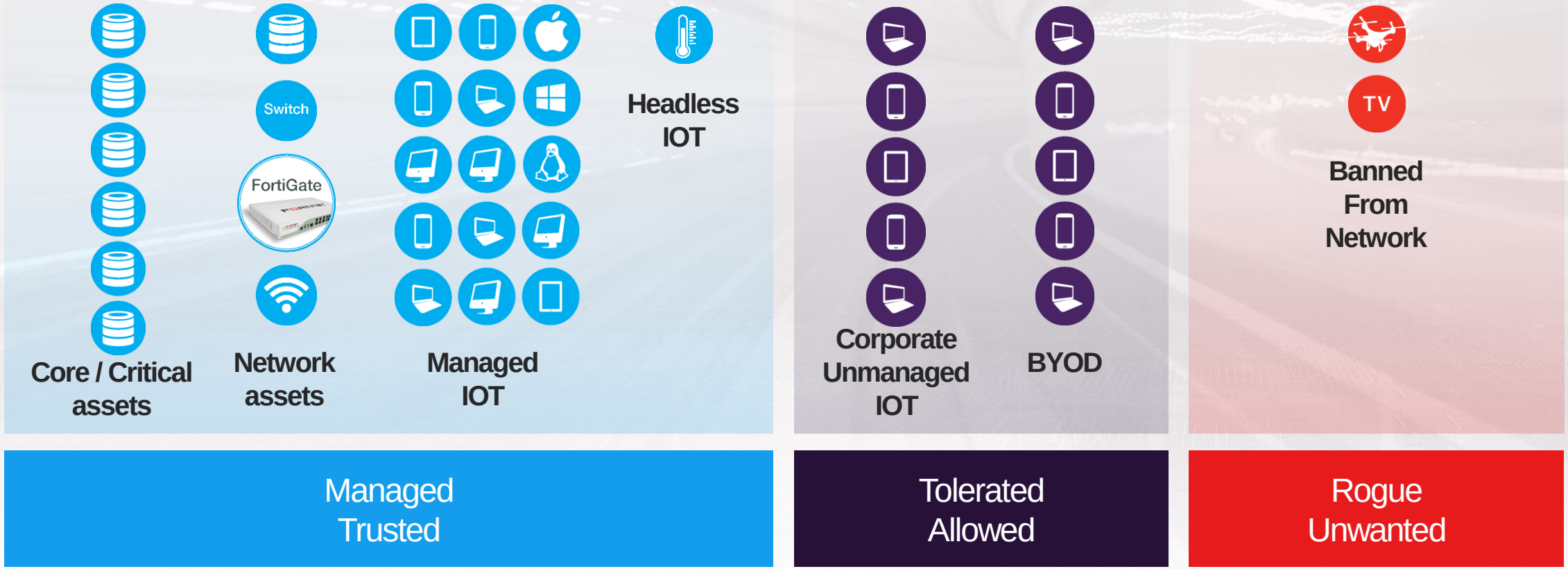
The Watchwords of IoT

LEARN
Trusted or Not

SEGMENT
Define a Policy

PROTECT
Everything

IoT – Where do I start?



Three Out of Many Concerns

DIGITAL TRANSFORMATION

CYBER THREATS

COMPLIANCE

Q2 2017 by the Numbers*

Exploits

- 184 billion exploit detections
- 1.8 billion average daily volume
- 6,298 unique exploit detections
- 69% of firms saw severe exploits

Malware

- 62 million malware detections
- 677,000 average daily volume
- 16,582 variants in 2,534 families
- 18% of firms saw mobile malware

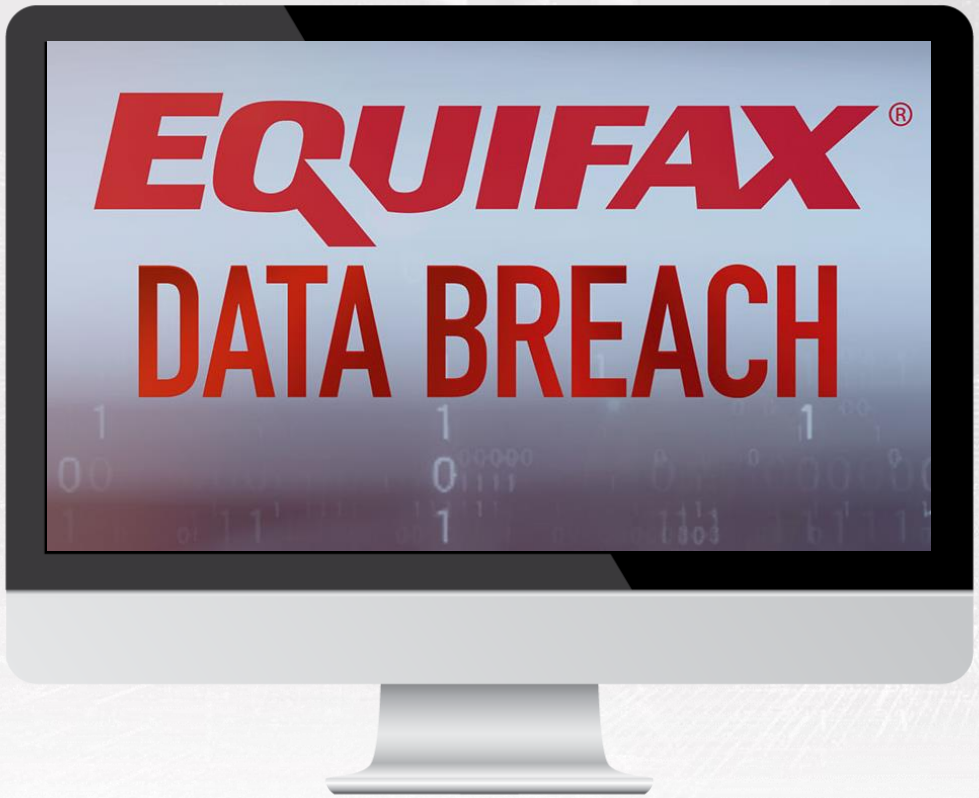
Botnets

- 2.9 billion botnet detections
- 32 million average daily volume
- 243 unique botnets detected
- 993 daily communications per firm

The State of the Threat Landscape

We’re Suffering From the YEAH Syndrome

Yet Another Headline



Paradise Papers

Too Soon to Tell But Don't Forget Panama

ELDERLY VULNERABILITIES ARE STILL DANGEROUS

90% OF ORGANIZATIONS
saw exploits for vulnerabilities
that were at least **3 YEARS OLD**

60% saw ones that were
10 OR MORE YEARS OLD

Prevention and Detection Working Together

- Network Firewall
- Antivirus
- Intrusion Prevention
- End Point Protection
- Secure Email Gateway
- Web Application Firewall
- Two Factor Authentication

- Botnet Detection
- IP & Client Reputation
- Sandbox

Supported by Integrated Threat Intelligence Ecosystem

Three Out of Many Concerns

DIGITAL TRANSFORMATION

CYBER THREATS

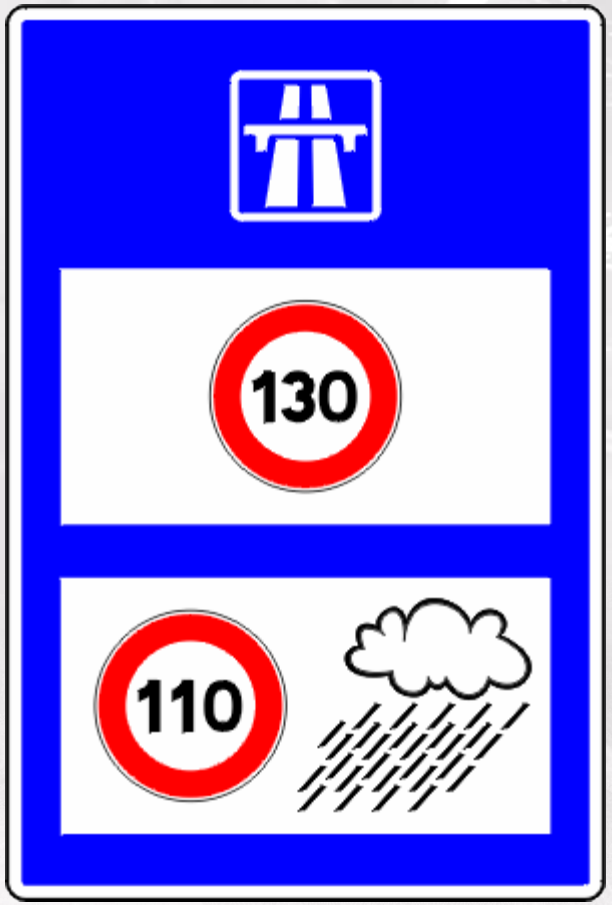
COMPLIANCE

GDPR

“WE DON’T KNOW WHAT WE DON’T KNOW.”

DONALD RUMSFELD
FORMER US SECRETARY OF DEFENSE

What Do They Have in Common?



Preparing for GDPR*

12 Steps To Take Now

1 Awareness
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data
You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

8 Children
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

9 Data Breaches
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

11 Data Protection Officers
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International
If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

*ico.org.uk

Two Key Aspects of GDPR

1. Consequences for GDPR violations

- Empowers supervisory authorities to assess fines that are “effective, proportionate and dissuasive.”
- Two tiers of maximum fines depending upon severity of violation
  - **»2% or €10M, whichever is higher**
  - **»4% or €20M, whichever is higher**
- Allows data subjects to seek monetary damages in court from controllers who violate their rights and from processors as well.

Two Key Aspects of GDPR

2. Data Breach notifications

- A personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- Data controllers must notify the supervisory authority "competent under Article 55"
- Notice must be provided "without undue delay and, where feasible, **not later than 72 hours** after having become aware of it."

- Notification to the authority must consist of at least:
  - Describe the nature of the personal data breach, including the number and categories of data subjects and personal data records affected;
  - Provide the data protection officer's contact information;
  - Describe the likely consequences of the personal data breach
  - Describe how the controller proposes to address the breach, including any mitigation efforts
  - If data processor experiences a [illegible] must notify the controller
- Notice **is not** required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons,"

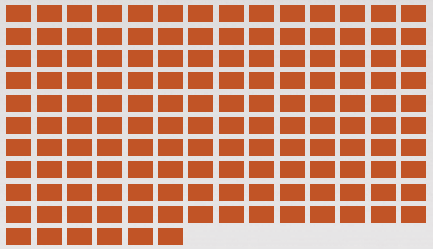
Looking to the Future - What GDPR Requires

JANUARY 2019

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

What Your Network Requires

Average time between intrusion and detection =



146 DAYS*

The Hacker's Advantage:

Window of Opportunity

Change the Playing Field:

Close the Window of Opportunity

- KNOW SOONER
- REACT FASTER

Three Out of Many Concerns

DIGITAL TRANSFORMATION

CYBER THREATS

COMPLIANCE

Multiple Issues, One Vision

The Fortinet Security Fabric

EVOLVING AS THE MARKET, AND YOUR NEEDS, EVOLVE

Provides A Single Security Posture Across the Whole of the Network - Physical, Virtual and Cloud

Integrates Security with Connectivity

Protects Against the "Things"

Supports Your Compliance Requirements

FORTINET