Protecting High-Performance Data Centers

Antonis Proimadis, Senior Presales Engineer

November 2015, Infocom

Data Center Trends detailed

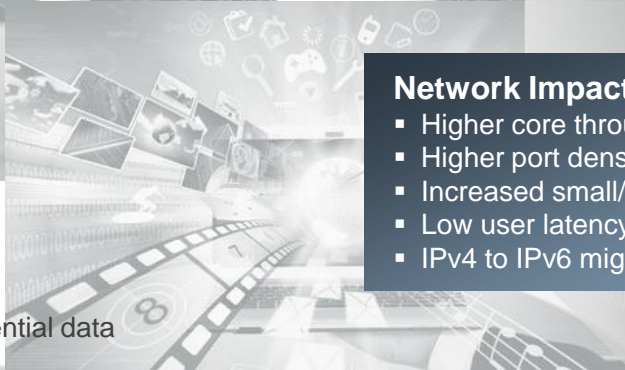**BYOD, Mobility & SaaS**
- Anytime, anywhere access
- User-centric apps & services
- Customer/client responsiveness

Data Center Transformation
- Server & network virtualization
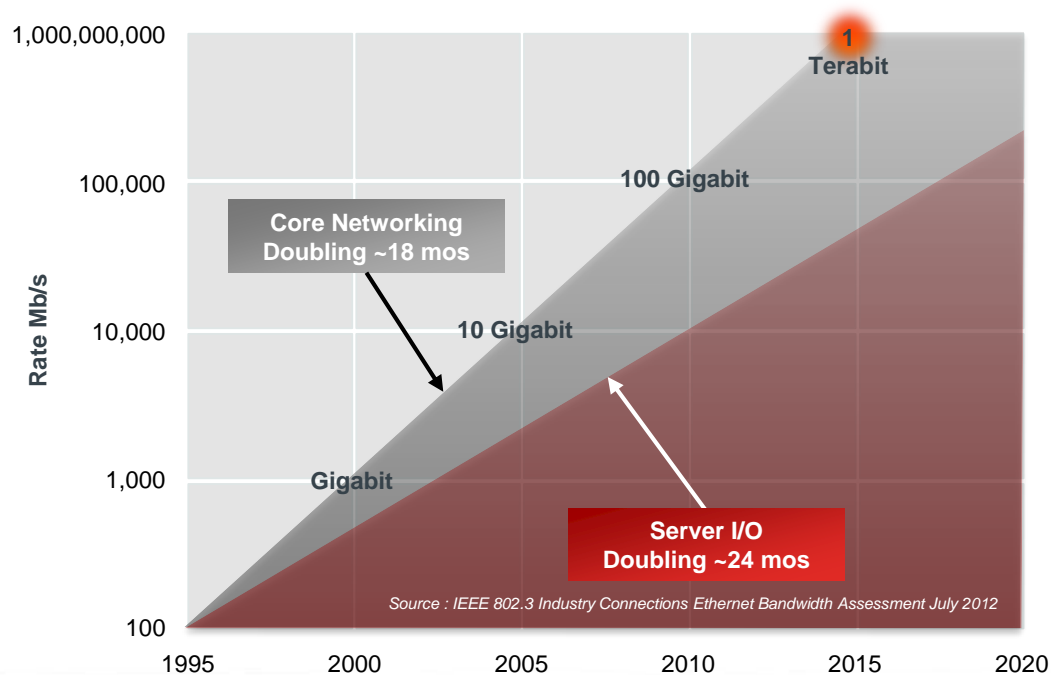- Multi-tenant public clouds
- Elasticity & agility

Network Impact
- Higher core throughput & scalability
- Higher port density
- Increased small/mixed packet traffic
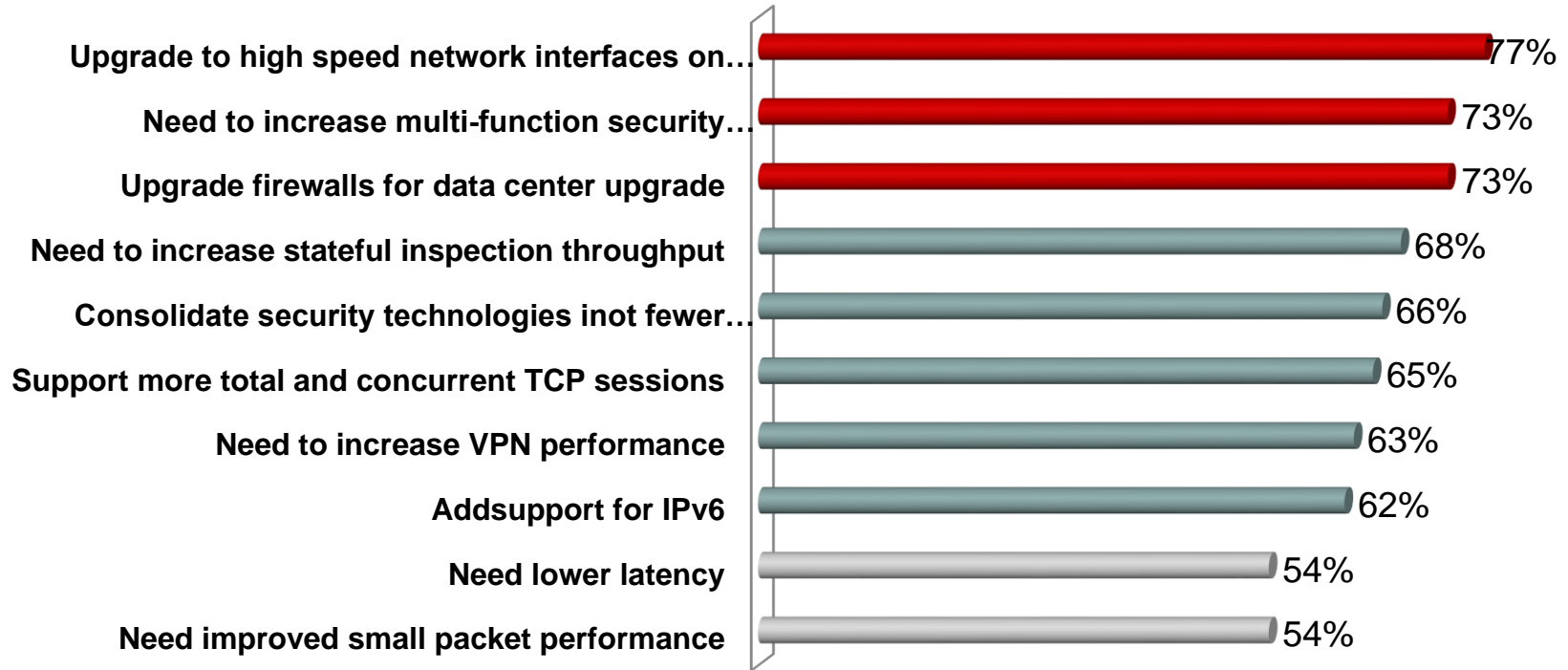- Low user latency
- IPv4 to IPv6 migration

Big Data & Internet of Things
- Billions of connected devices
- Continuous data aggregation
- Warehousing of petabytes of confidential data

Data Center Trends: Moore's Law Effect Continues to Drive Higher Network Speeds and Interfaces

Upgrade to high speed network interfaces on…	77%
Need to increase multi-function security…	73%
Upgrade firewalls for data center upgrade	73%
Need to increase stateful inspection throughput	68%
Consolidate security technologies inot fewer…	66%
Support more total and concurrent TCP sessions	65%
Need to increase VPN performance	63%
Addsupport for IPv6	62%
Need lower latency	54%
Need improved small packet performance	54%

Source : Infonetics High End Firewall Survey

FURTINET. FAST. SECURE. GLOBAL.
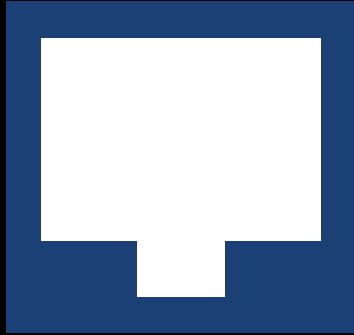
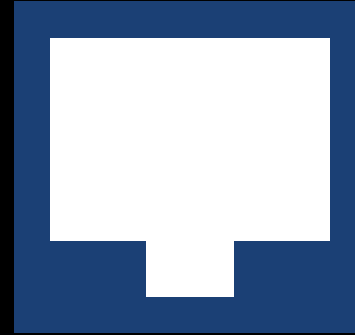# Data Center and Core Bandwidth Requirements
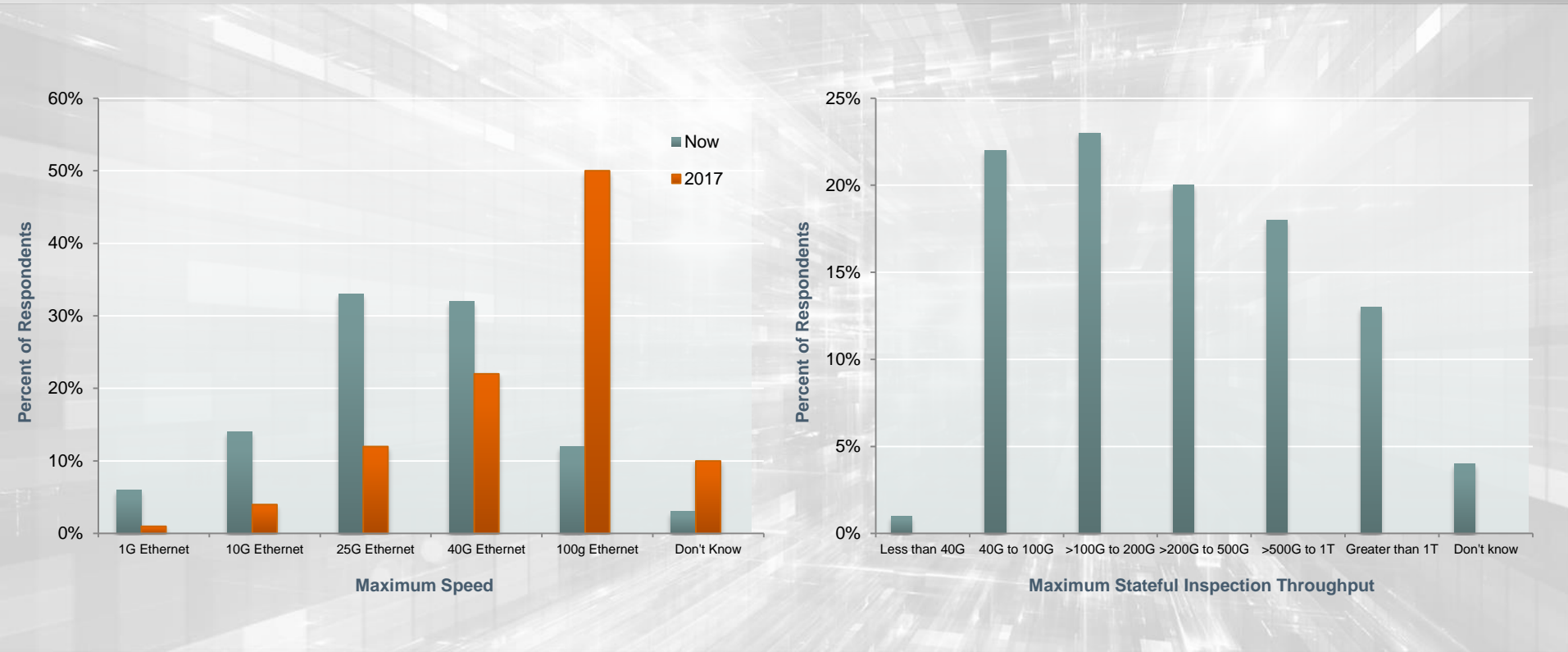
Software-Defined Networks (SDN)
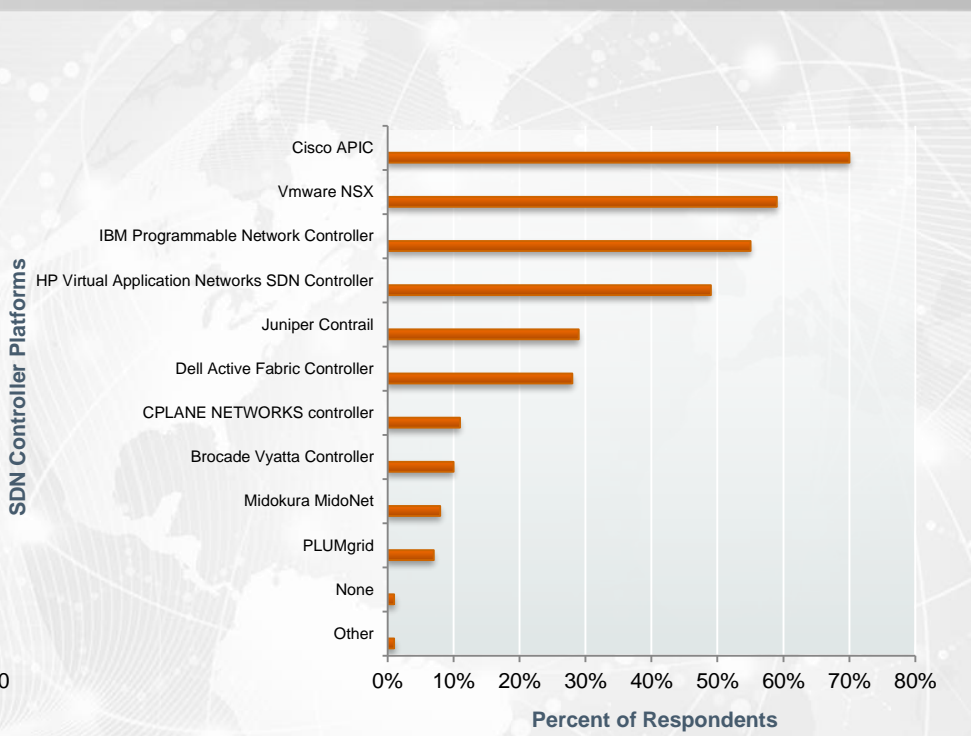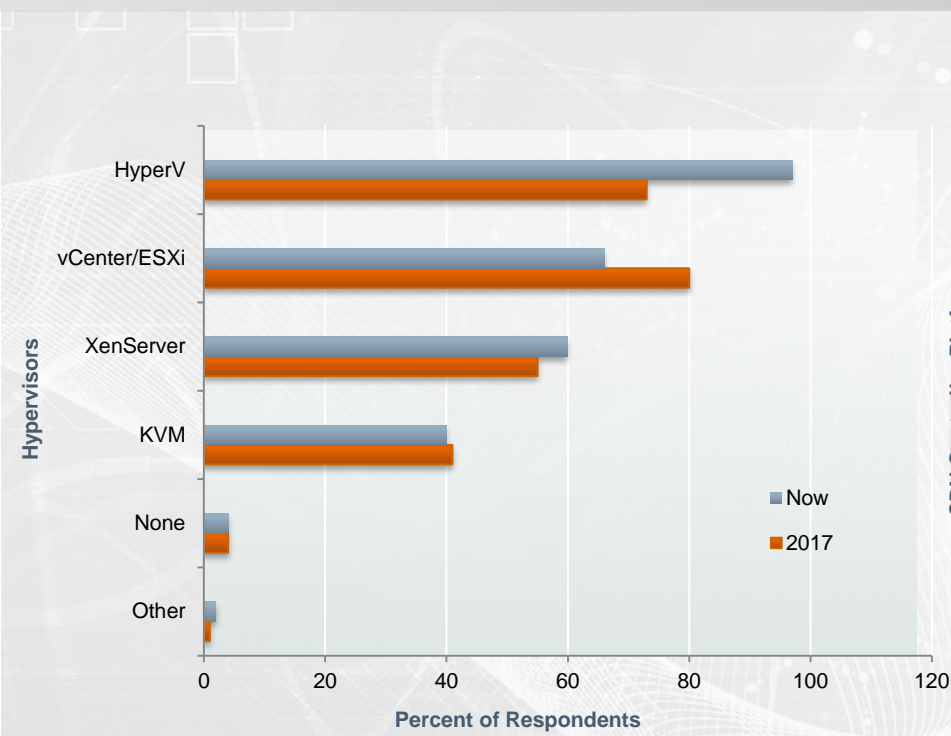
Fact – Trust & Verify Security Model

UNTRUSTED   TRUSTED

Fact – The Internal Network is Open
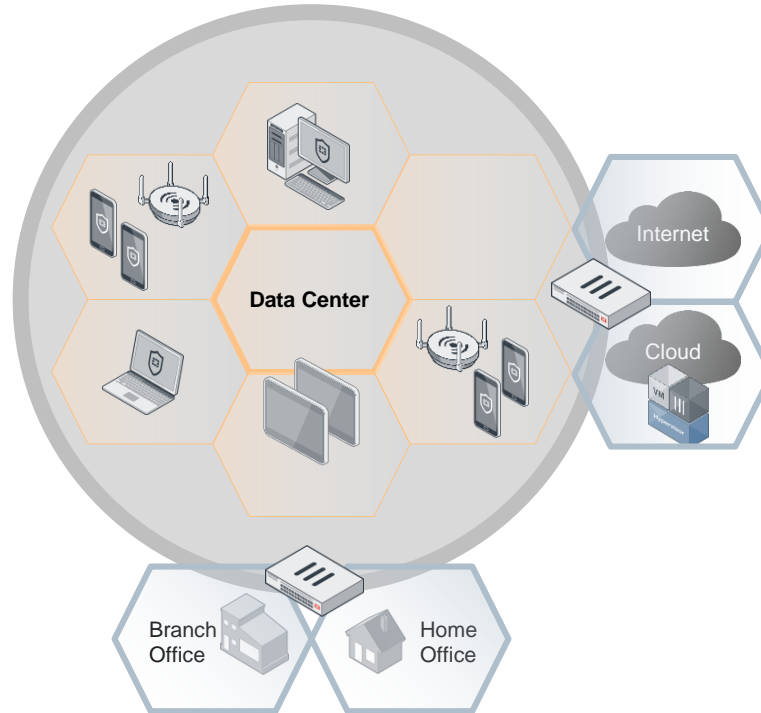
Fact – Attack Surface & Vectors Evolution
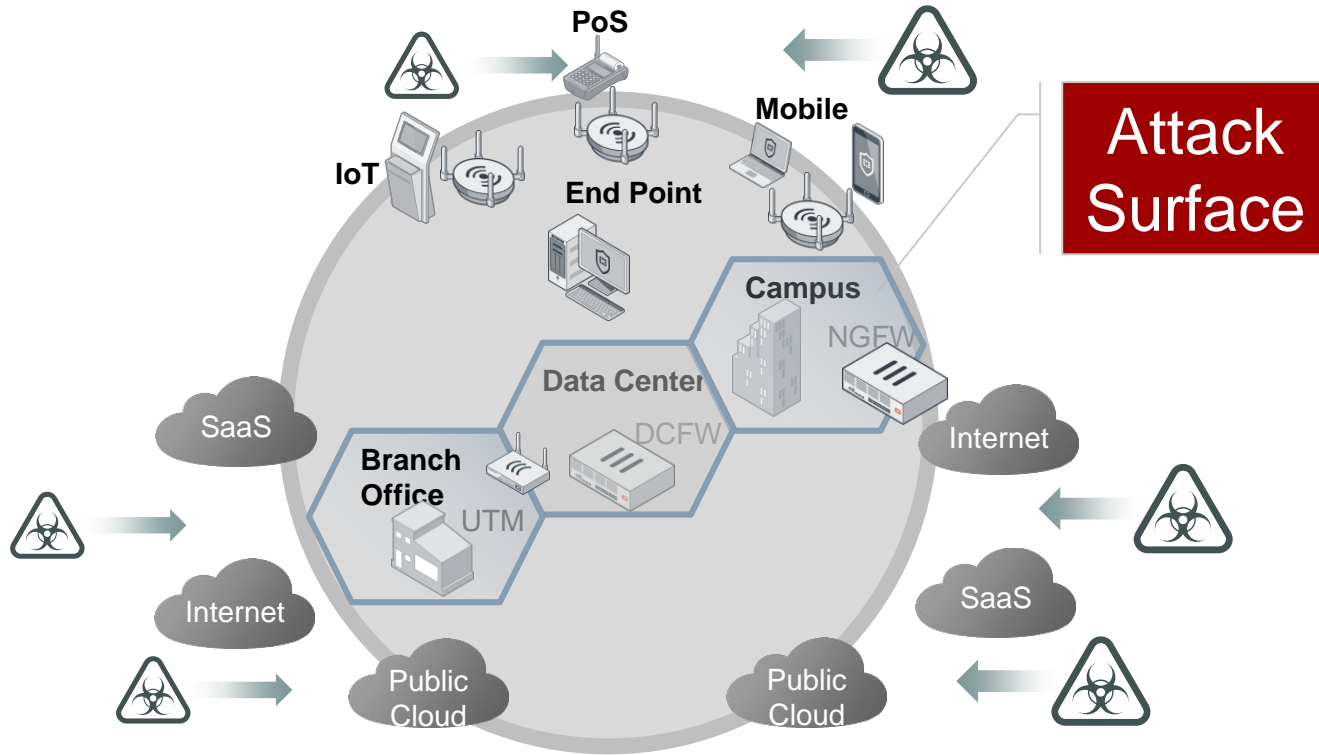
Wireless Networks Ranked as the Most Vulnerable IT Infrastructure

How vulnerable you believe each is from a security standpoint?

	Endpoint	Core network infrastructure	Wireless	Databases	Applications	Storage	Email
Worldwide	45%	29%	49%	25%	17%	11%	25%
EMEA	47%	27%	52%	22%	17%	10%	24%
UK	48%	23%	53%	21%	22%	13%	20%

FAST. SECURE. GLOBAL.

F=RTINET.
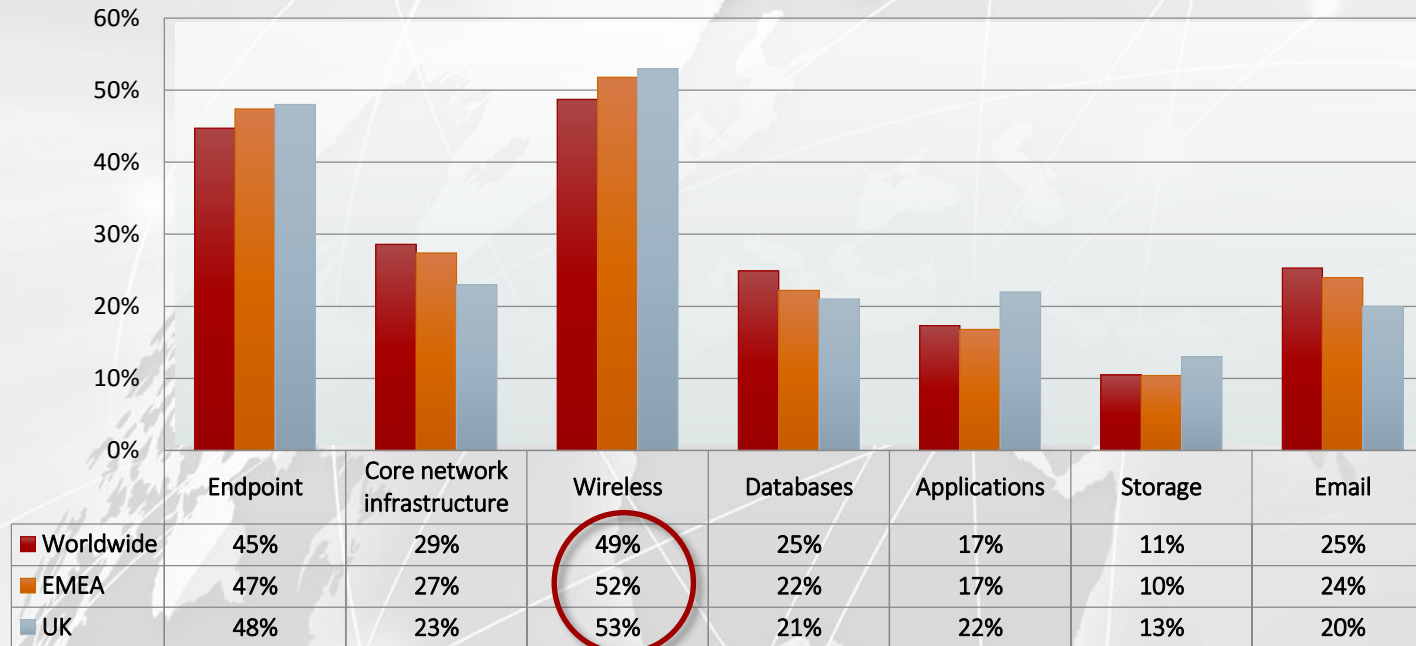
Advanced Threats Take Advantage of the "Flat Internal" Network

- Existing Firewalls focused on the **Border**

- Internal network no longer "trusted"

- Many ways into the network

- Once inside threats can spread quickly

Border

EXTERNAL | INTERNAL

Email (Phishing) Vulnerabilities Web Downloads | Social Engineering Exploits (Zero Days)

Threat Production + Recon

1 Threat Vector → Infection 2

4 Extraction ← Communication 3

Package Encrypt Stage

Disposal

Hide, Spread, Disarm, Access, Contact Botnet CC, Update

FAST. SECURE. GLOBAL.
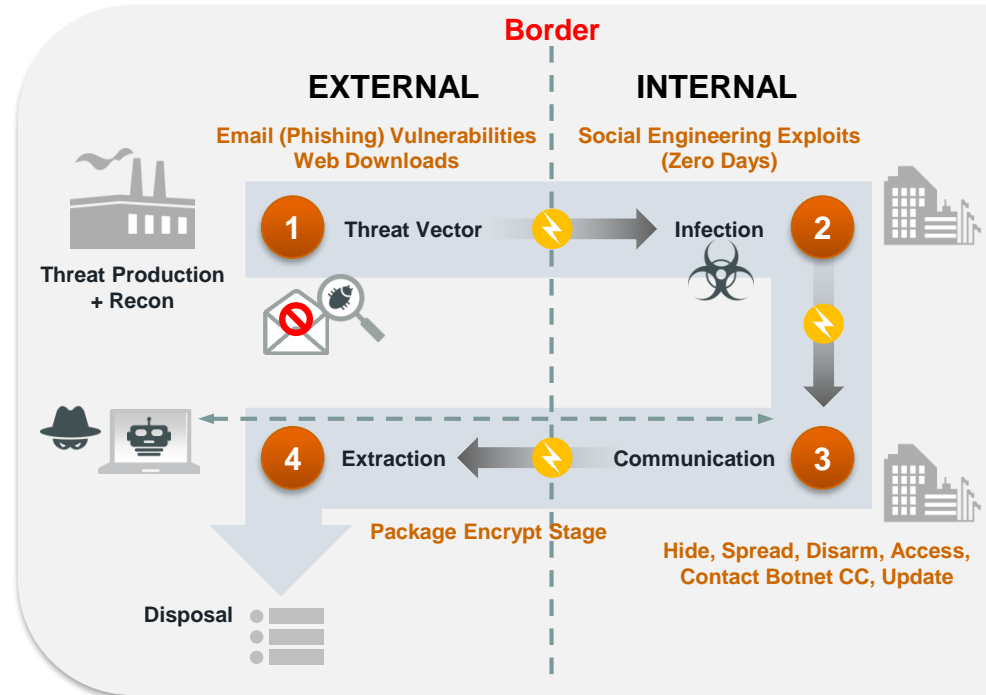
Key Breach Report Trends

95%

OF MALWARE TYPES
SHOWED UP FOR LESS
THAN A MONTH, AND
FOUR OUT OF FIVE
DIDN'T LAST BEYOND
A WEEK.

70–90%

OF MALWARE SAMPLES
ARE UNIQUE TO AN
ORGANIZATION.

50%

NEARLY 50% OPEN
E-MAILS AND CLICK ON
PHISHING LINKS WITHIN
THE FIRST HOUR.

23%

OF RECIPIENTS NOW
OPEN PHISHING
MESSAGES AND
11% CLICK ON
ATTACHMENTS.

60%

IN 60% OF CASES,
ATTACKERS ARE ABLE
TO COMPROMISE AN
ORGANIZATION
WITHIN MINUTES.
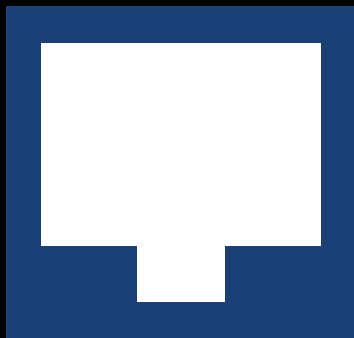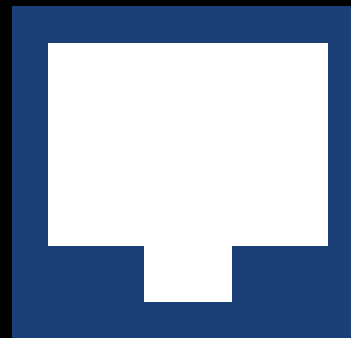
Fact – A Breach Can't Be Avoided

"All organizations should now assume that they are in a state of continuous compromise." (Gartner)

"There are two types of companies: those that have been hacked, and those that will be."
(Robert Mueller, FBI Director)

FORTINET.   FAST. SECURE. GLOBAL.

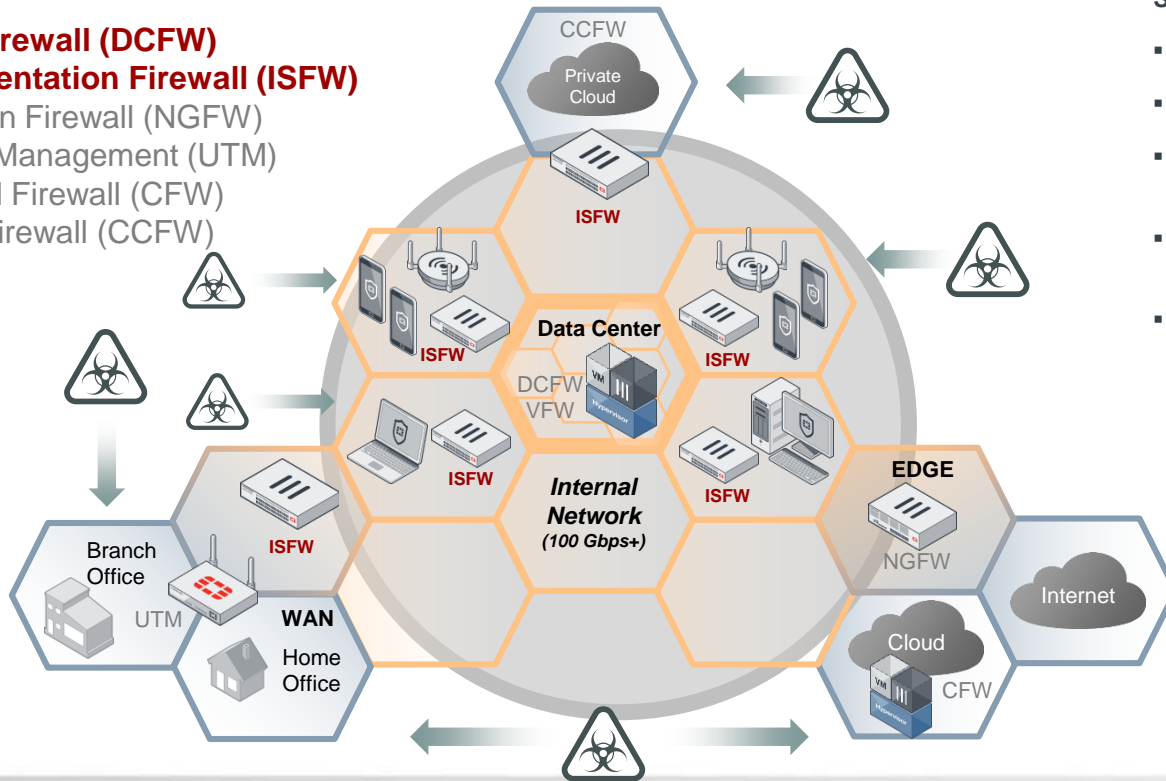# Fact – The Zero Trust Model is Gaining Traction

UNTRUSTED　　　　　　**UNTRUSTED**

Threat Landscape & Evolving IT Infrastructure

Data Center Firewall (DCFW)
Internal Segmentation Firewall (ISFW)
Next Generation Firewall (NGFW)
Unified Threat Management (UTM)
Virtual or Cloud Firewall (CFW)
Carrier Class Firewall (CCFW)

Segmentation Challenges

- *Higher internal network speeds*
- *Ultra-low latency requirements*
- *Protection required, not just detection*
- *Operational efficiency/ manageability*
- *Inspecting traffic that stays within the data center*

CCFW
Private Cloud
ISFW
Data Center
ISFW
ISFW
DCFW VFW
ISFW
ISFW
Internal Network (100 Gbps+)
EDGE
NGFW
Branch Office
UTM
WAN
Home Office
Internet
Cloud
CFW

Internal
External

FAST. SECURE. GLOBAL.

Requirement NO. 1 - **PERFORMANCE**

Data Center Firewall (DCFW)
Internal Segmentation Firewall (DCFW)

Border Firewall (NGFW)

Internet
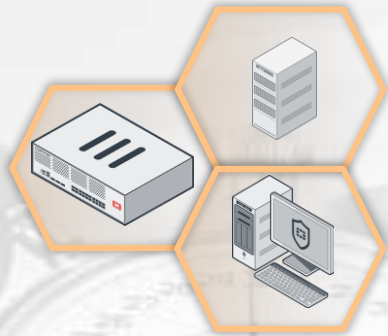
Interfaces → 10G, 40G & 100G

Ports Speeds → 1G, 10G

No. of Ports → 8 to 48 Ge/10Ge

No. of Ports → 2 to 12

Throughput → 10Gps to 1Tbps

Throughput → Mbps to 1Gbps

FAST. SECURE. GLOBAL.

CPU versus "custom" ASIC

Vendor A

CPU

Vendor B

Multi Core CPU

Off the shelf NP

FORTINET®

Optimum Path Processing (OPP)

CPU

CP8

NP6

FAST. SECURE. GLOBAL.

18
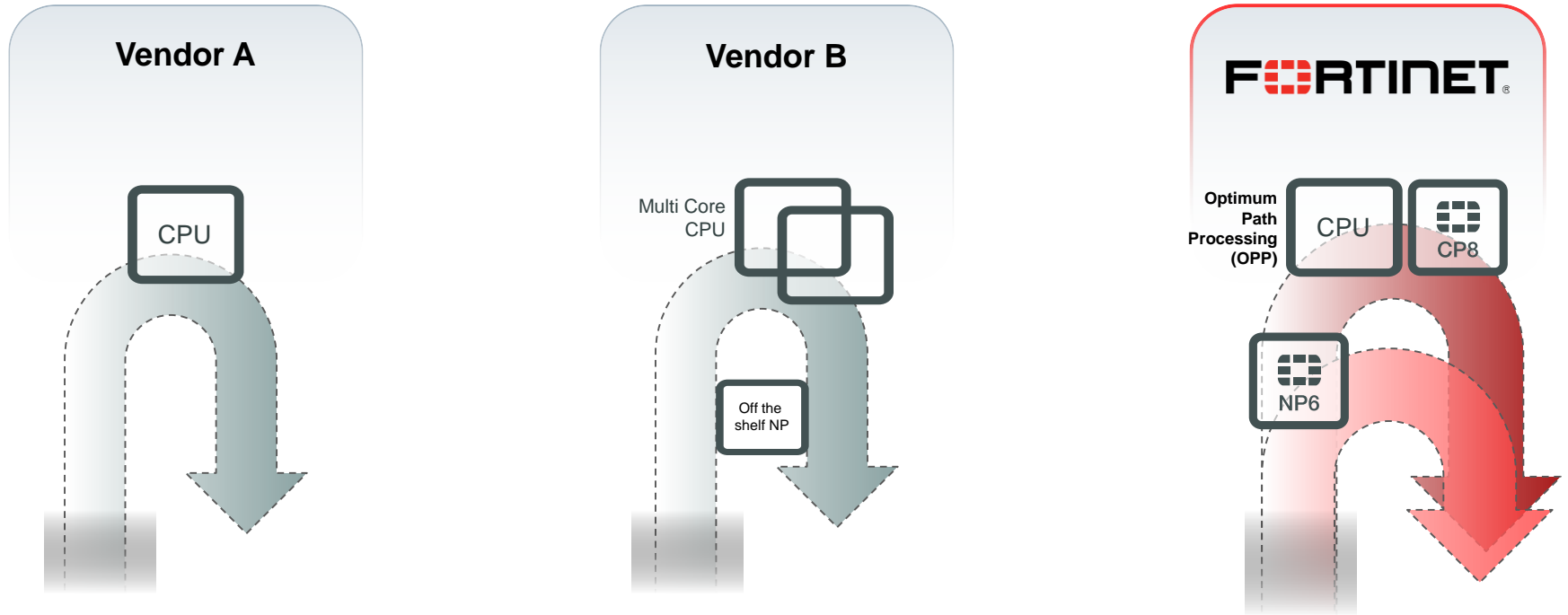
Requirement No. 2 - **PROTECTION**

Firewall
VPN
Application Control
IPS
Web Filtering
Anti-malware
WAN Acceleration
Data Leakage Protection
WiFi Controller
Advanced Threat Protection
SaaS Gateway

Management
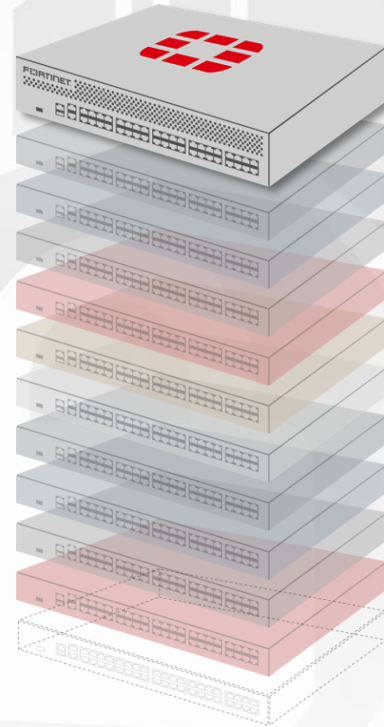
Software
Enabled
Security
Module

SECURED BY
FORTIGUARD®

FAST. SECURE. GLOBAL.

F:RTINET.

A Global Threat **Security** Service that Updates the Platform in Real time - FortiGuard

Application Control Service

Antivirus Service

Anti-spam Service

Intrusion Prevention Service

Web Security Service

Web Filtering Service

SECURED BY FORTIGUARD®

Database Security Service

Vulnerability Management Service

IP Reputation Service

Mobile Security

Global Fortinet Device Footprint

FAST. SECURE. GLOBAL.

http://threatmap.fortiguard.com

ATTACK	SEVERITY	LOCATION
HP.ProCurve.Manager.SNAC.UpdateCertificatesServlet.File.Upload	High	United States
MS.IE.Layout.Memory.Corruption	High	United States
MS.IE.Iframe.Javascript.Information.Disclosure	Medium	China
HP.ProCurve.Manager.SNAC.UpdateCertificatesServlet.File.Upload	High	India
MS.IE.Layout.Memory.Corruption	High	Thailand
CA.BrightStor.ACRserve.Message.Engine.Buffer.Overflow	High	United States
Novell.GroupWise.Messenger.Arbitrary.Memory.Corruption	High	Pakistan
Drupal.Core.xmlrpc.php.Internal.Entity.Expansion.DoS	Medium	Thailand

3rd Party Certification – The Proof

NGFW

Next Generation IPS
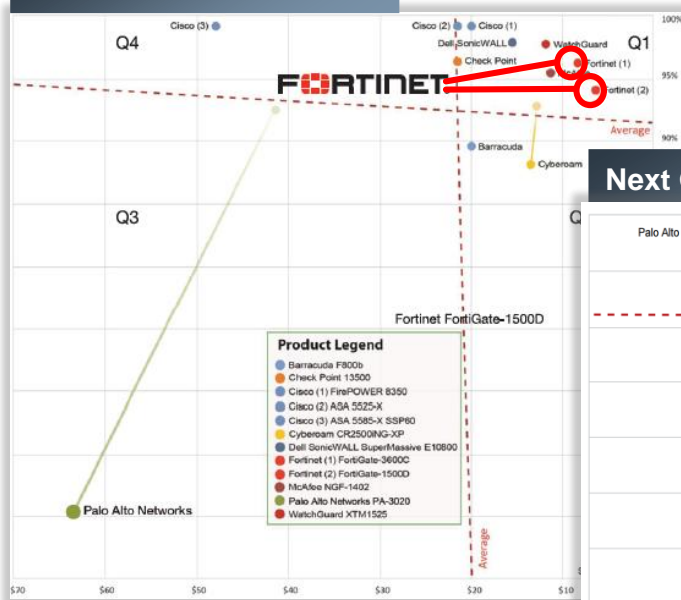
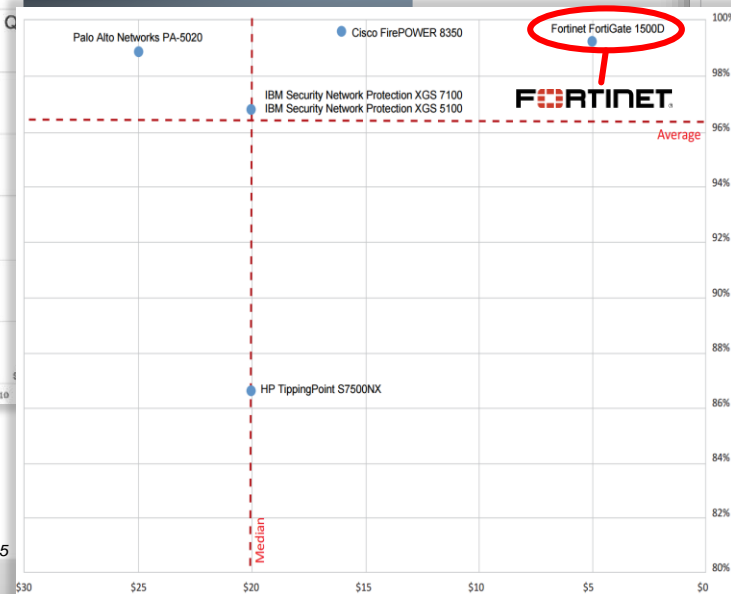**Breach Detection**

X-axis = TCO per protected Mbps, 'Value'   Y-axis = Security Effectiveness

Upper right quadrant = "Recommended"   Lower left quadrant = "Caution"   Other quadrants "Neutral"
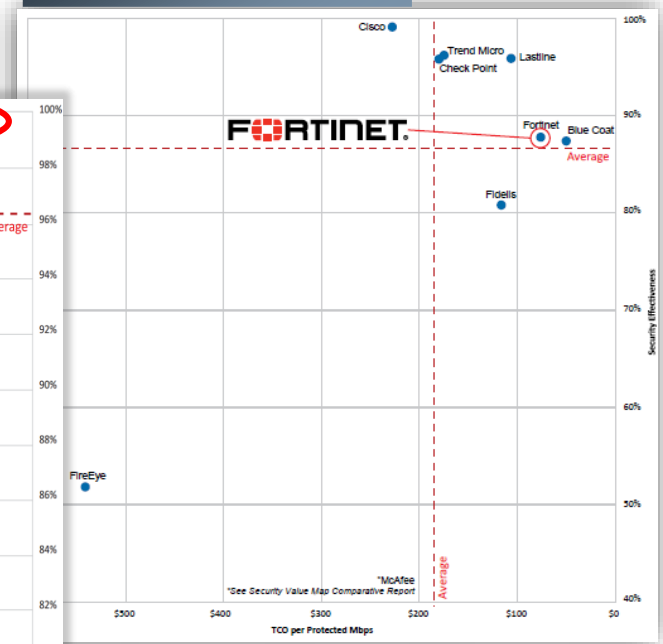
Sept. 2014

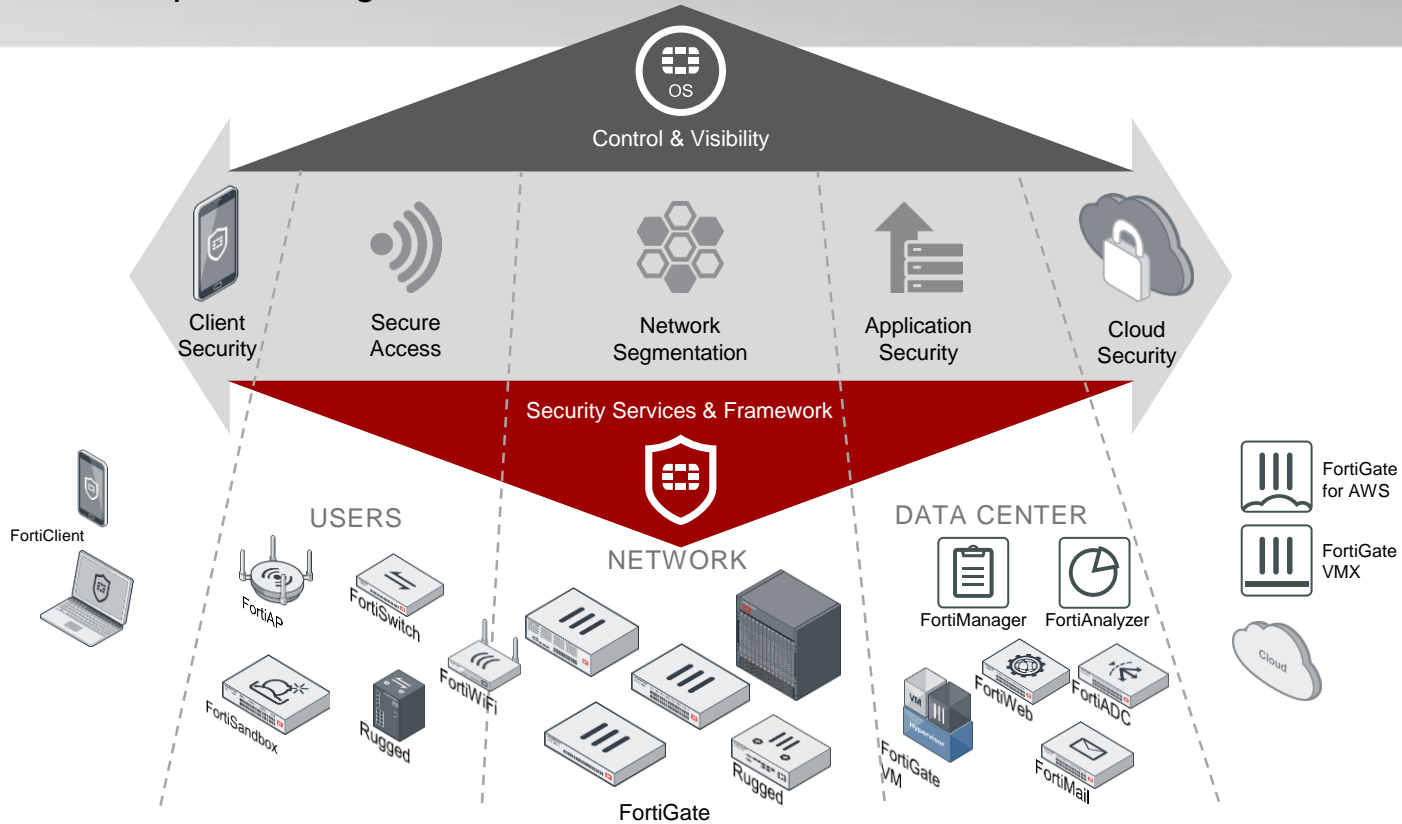Apr. 2015

Aug. 2015

FAST. SECURE. GLOBAL.

22

Requirement NO. 3 Global Cybersecurity Platform
Coverage from Endpoint to Edge to Core to Data Center to Cloud

Control & Visibility

Client Security

Secure Access

Network Segmentation

Application Security

Cloud Security

Security Services & Framework

FortiClient

USERS

FortiAP

FortiSwitch

FortiSandbox

Rugged

FortiWiFi

NETWORK

FortiGate

Rugged

DATA CENTER

FortiManager

FortiAnalyzer

FortiGate VM

Hypervisor

FortiWeb

FortiADC

FortiMail

FortiGate for AWS

FortiGate VMX

Cloud

Fortinet – Fast, Secure and Global

- Accelerate your business with

  Scalable, High-performance Security

- Protect your business with

  Proven, Certified Security

- Simplify your business with our

  Global Cybersecurity Platform

ASIC

OS

F⊟RTINET.   FAST. SECURE. GLOBAL.