FORTINET
FAST. SECURE. GLOBAL.

Data Center security trends

Tomislav Tucibat

Major accounts Manager, Adriatic

IT Security evolution

How did “threat market” change over the recent years?

Problem: Growing Attack Surface

Problem: Growing Attack Vectors

An Extensive, Poisoned, Dark, Deep Web

Trends Affecting the Network

BYOD, mobility and connected world

Internet of Things

Cloud consumption

Advanced Persistent Threats and Growing Attack Surface

Ever increasing bandwidth requirements

Extension of the Data Center into the Cloud

What We Used To Think

APT

ADVANCED PERSISTENT THREATS

How We Think Today

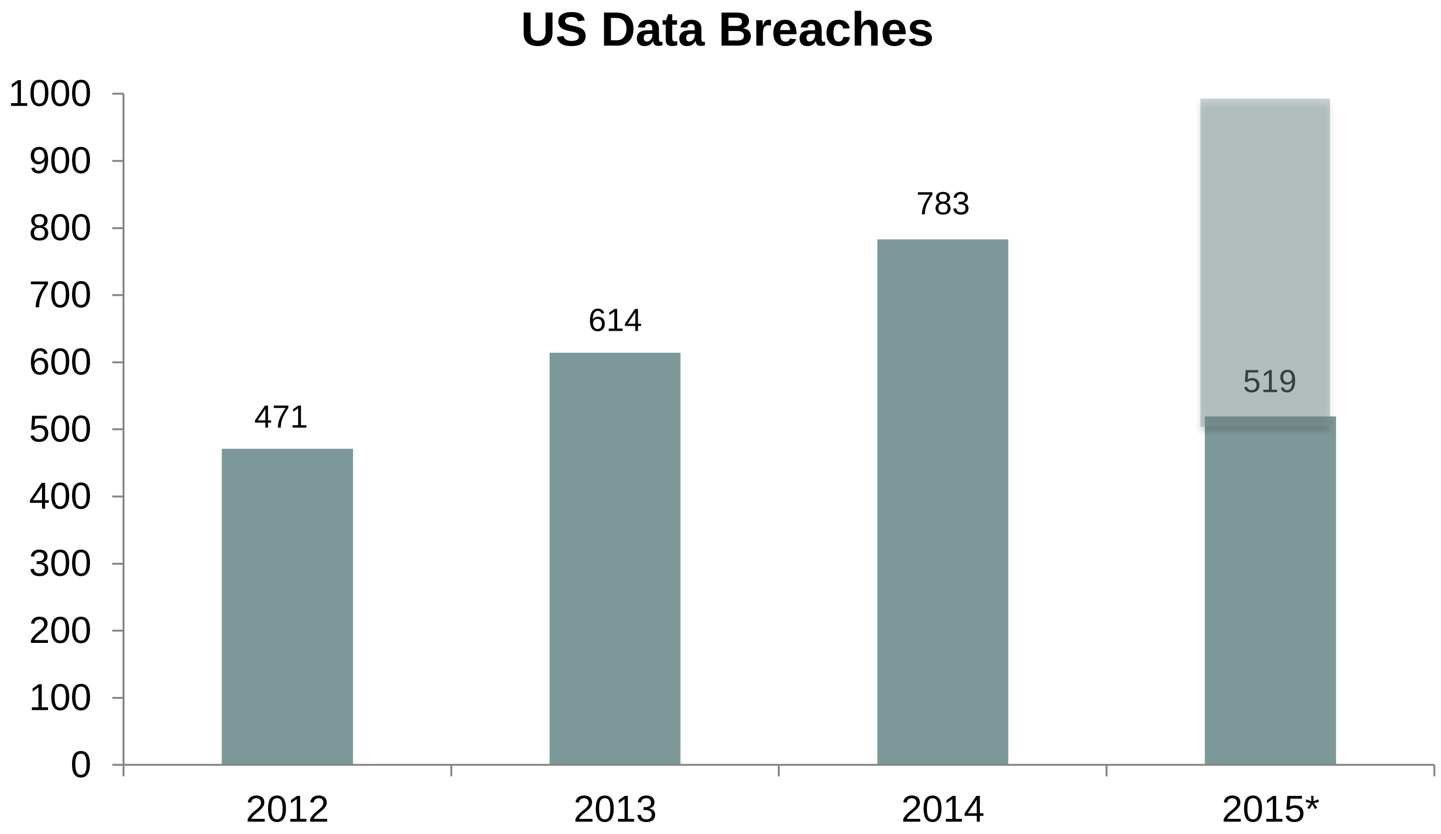
APT

ADVANCED PERSISTENT THREATS

ATA

ADVANCED TARGETED ATTACKS

Most Valuable Asset is at Risk



Source: Identity Theft Resource Center

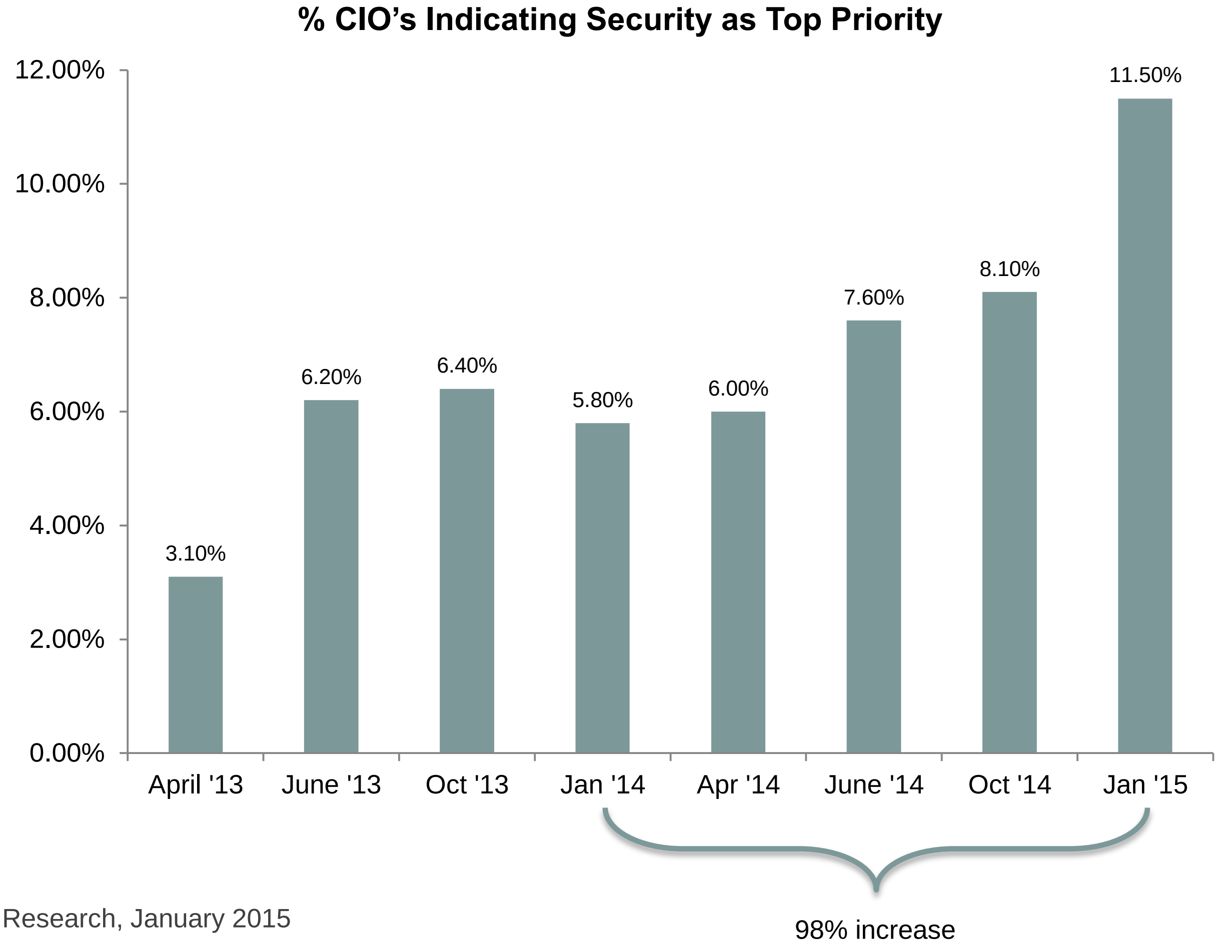
* Through 08/2015

Security Is Now A Board Room Discussion

“63% of Enterprise IT decision makers report a very high level of Board Level pressure regarding security”

Source: Lightspeed GMI Survey 2014

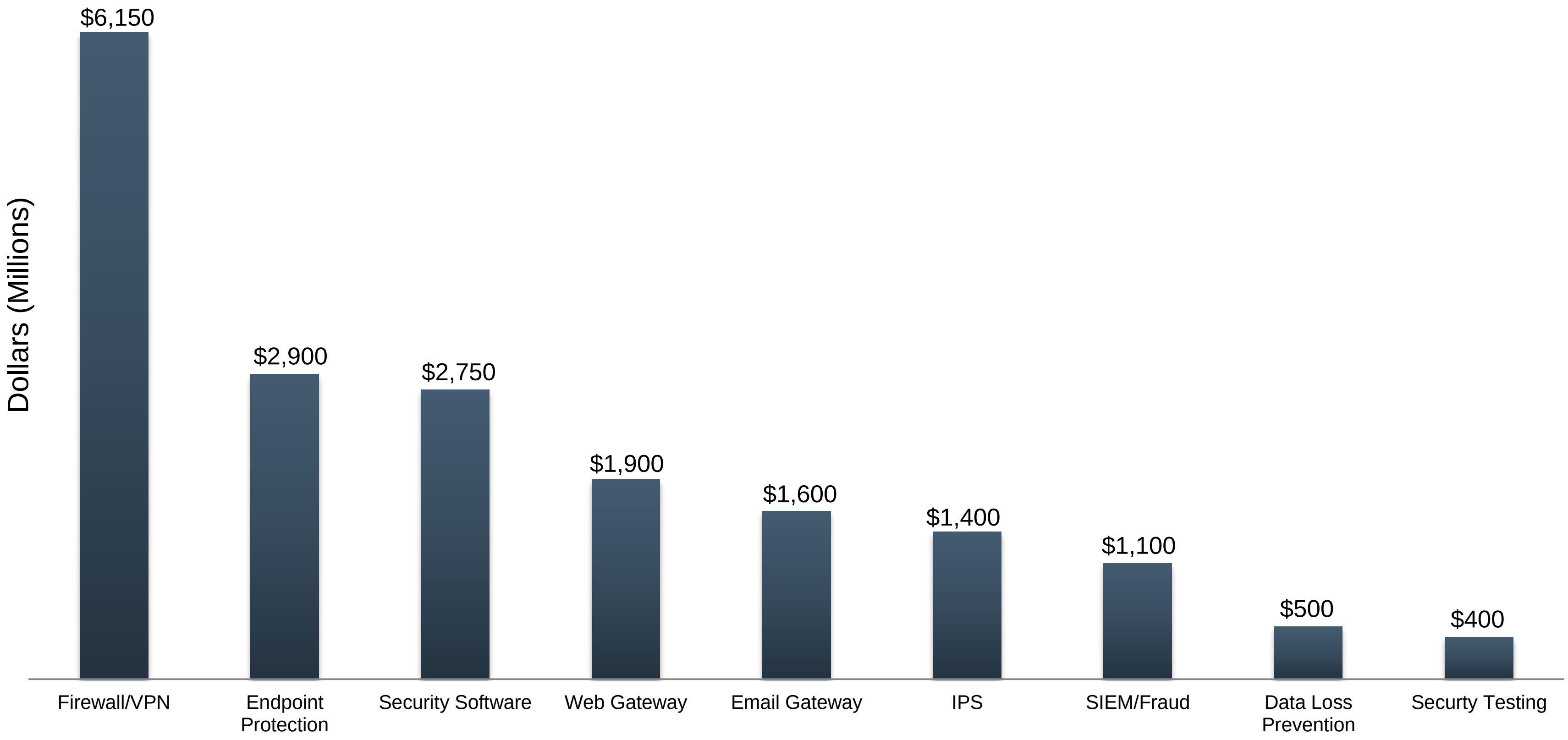
CIO’s Top Priority



Source: Morgan Stanley Research, January 2015

Firewall Spending is Top Priority

IT Security Spending by Technology

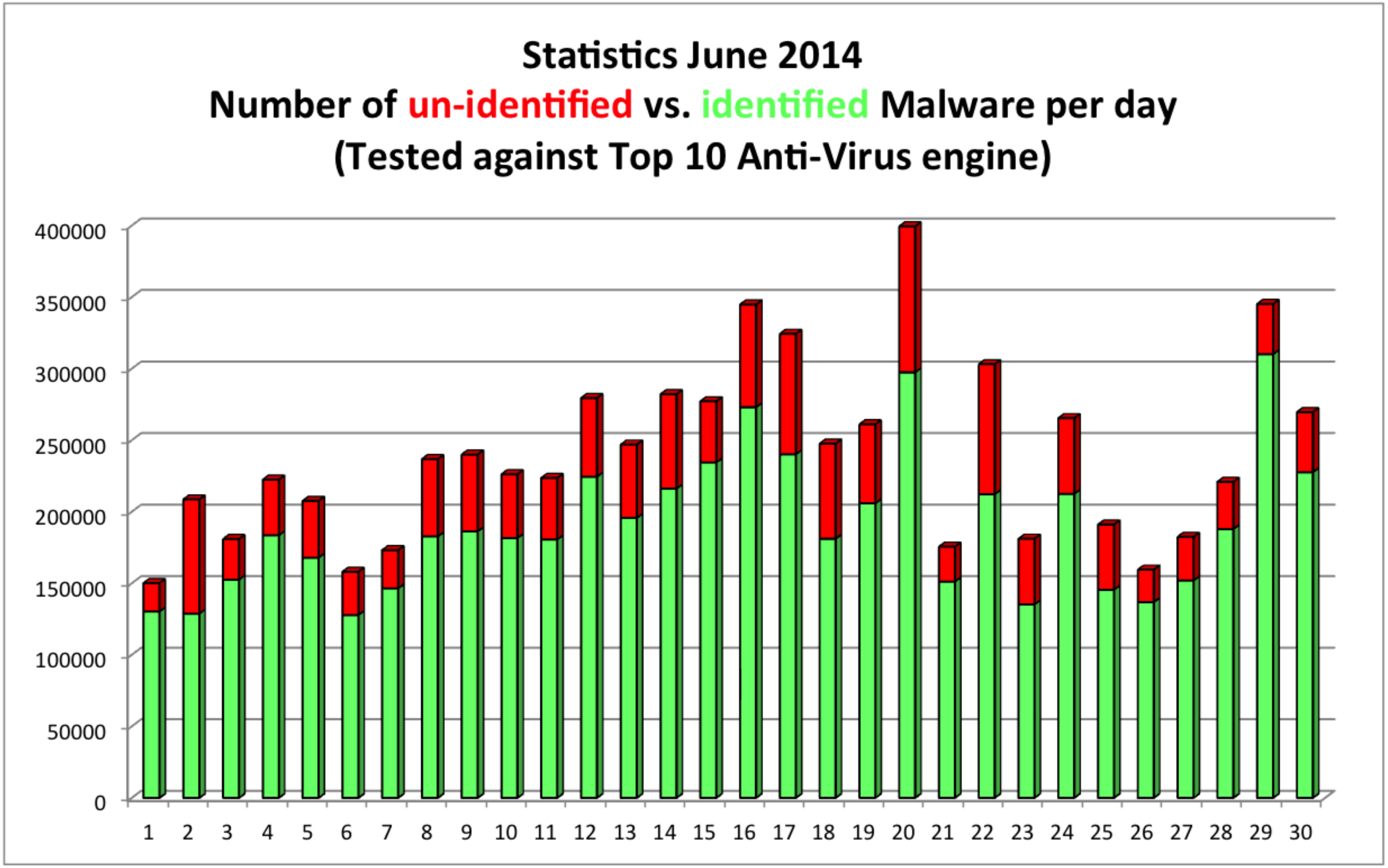


Source: Gartner 2014

Common theme with threats

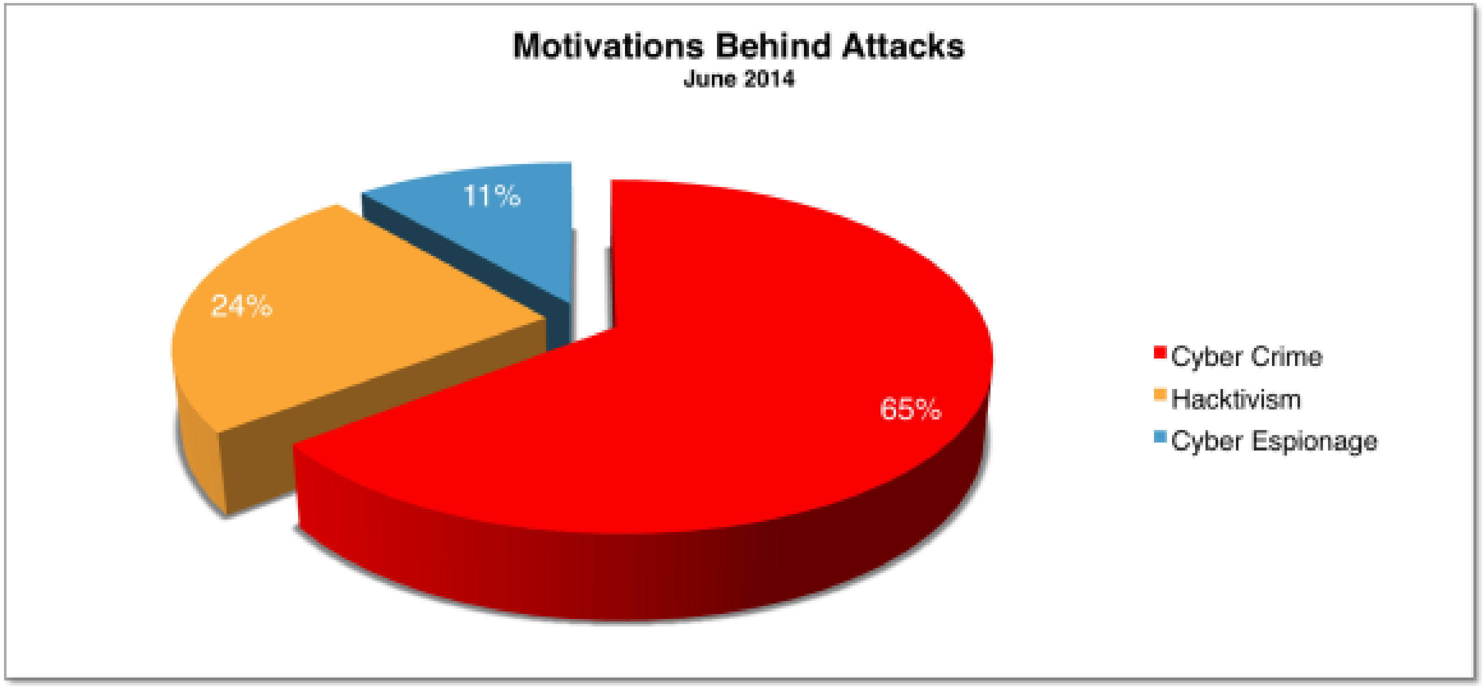
How do threats work in detail?

The Threat is Worse Than Ever



*Akylus July 2014

With A Consistent Motivation



***Hackmageddon July 2014**

Companies should be concerned

FACT:

- Prevention techniques sometimes **fail**, so detection and response tools, processes, & teams must be added

229 days

Average time attackers were on a network before detection

67%

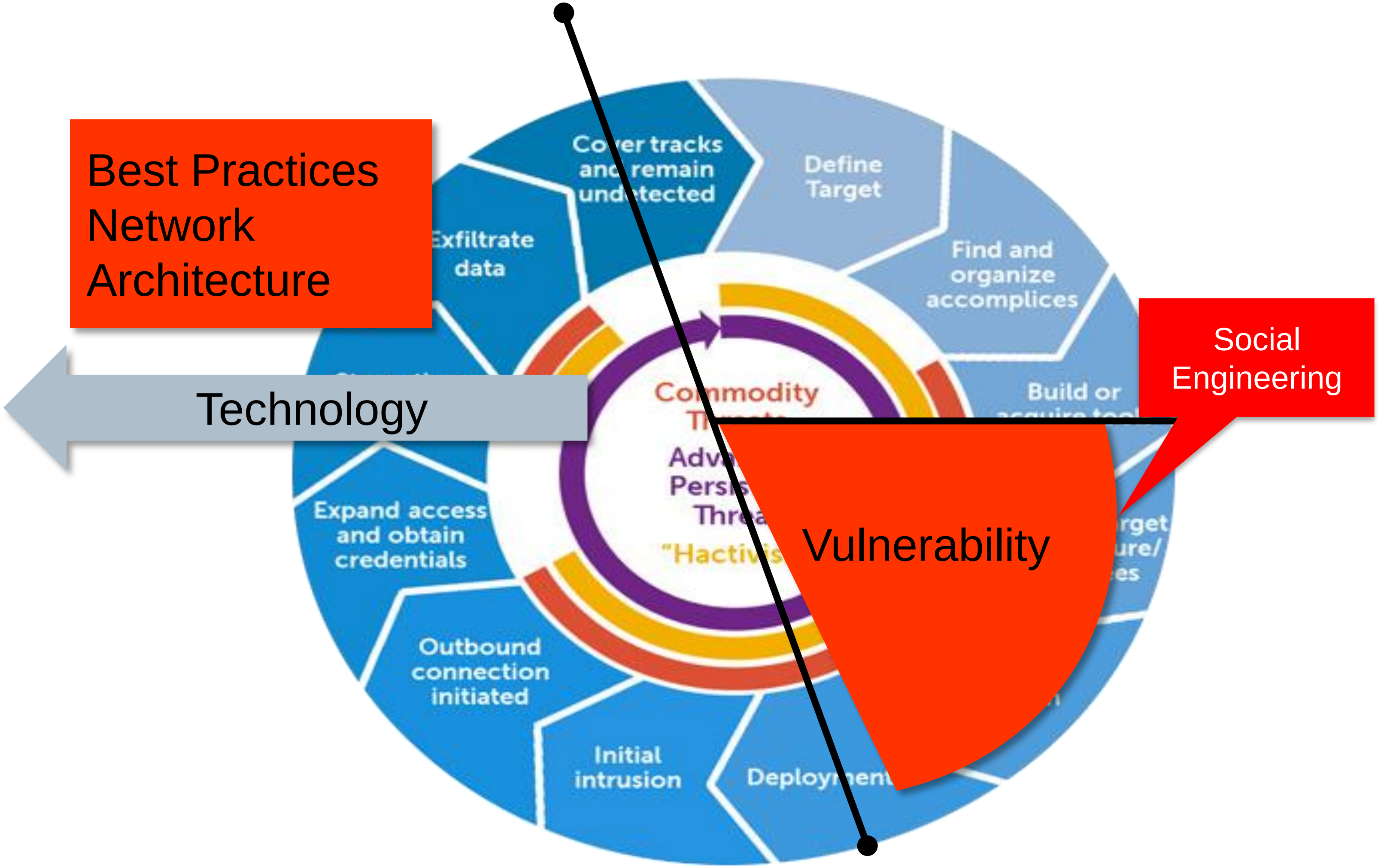
Victims were notified by an external entity

GOAL: Reduce time to **Find/Detect** incidents
Reduce time to **Investigate** incidents
Reduce time to **Remediate** incidents

How to loose 148M USD – a practical guide

1. Get infected by malware from a contractor’s computer. The malware stole a user’s credentials.
2. Hacker connects using stolen credentials and accesses Target’s application dedicated to contractors
3. Hacker exploits an internal web app. This exploit allows privileged code execution, so a set of tools installed on the server hosting the app.
4. Hackers perform LDAP searches until admin account is identified. Steal the cached admin token from the web server memory.
5. Hacker creates a new LDAP admin account ☺
6. Hackers copy readable information from reachable DBs (around 70M customer records, but no credit cards)
7. Install malware on POS system, steal 40M credit cards (Kaptoxa malware)

APT lifecycle



Best Practices Network Architecture

Technology

Social Engineering

Vulnerability

Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tool
Exfiltrate data
Commodity Threats
Advanced Persistent Threats
"Hactivis
Expand access and obtain credentials
Outbound connection initiated
Initial intrusion
Deployment

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.

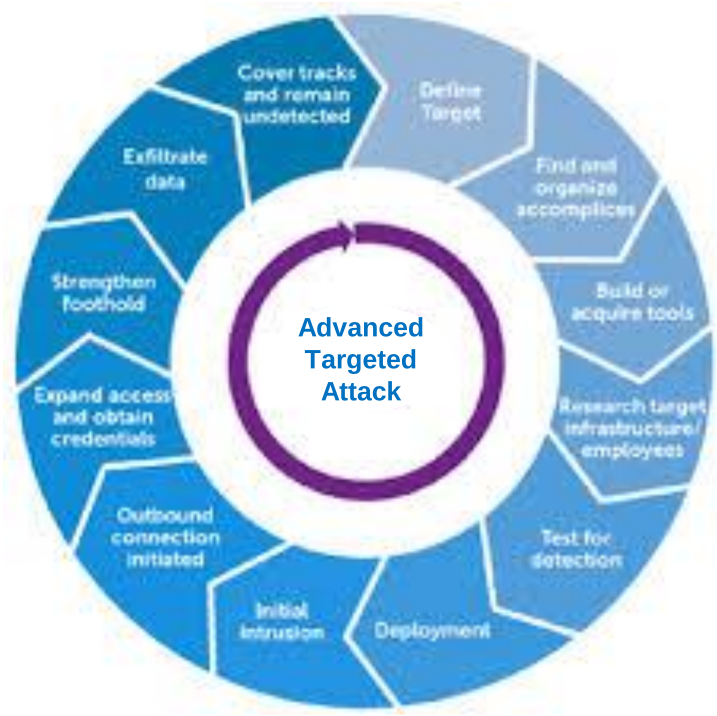
60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

Strategy to combat Threats

How can you protect yourself?

Is There A Silver Bullet For Defeating an ATA?

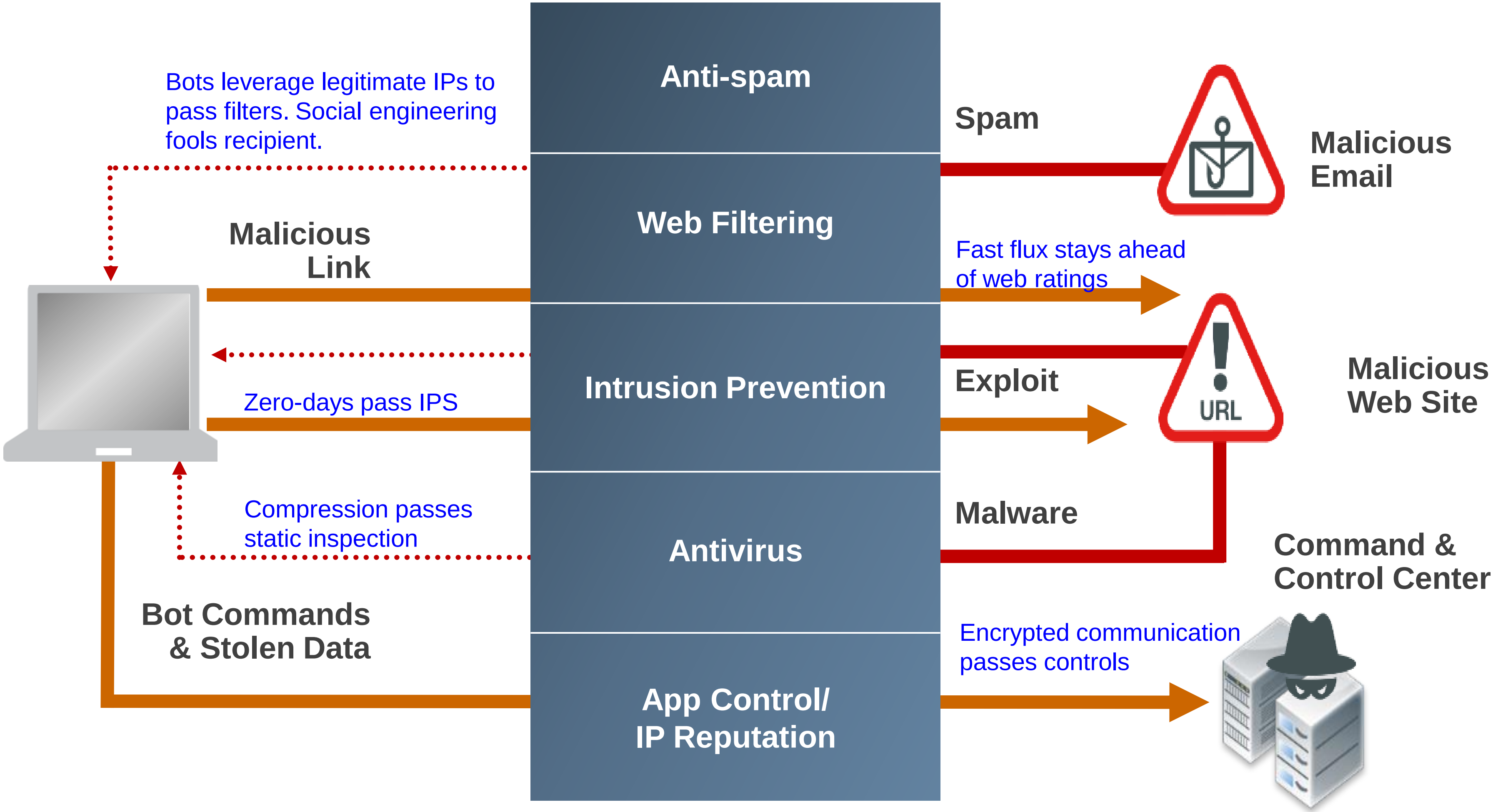

Advanced Targeted Attack
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

Training To Raise Awareness

http://krebsonsecurity.com/2012/01/phishing-your-employees-101/

- Policy
- Procedure
- Process

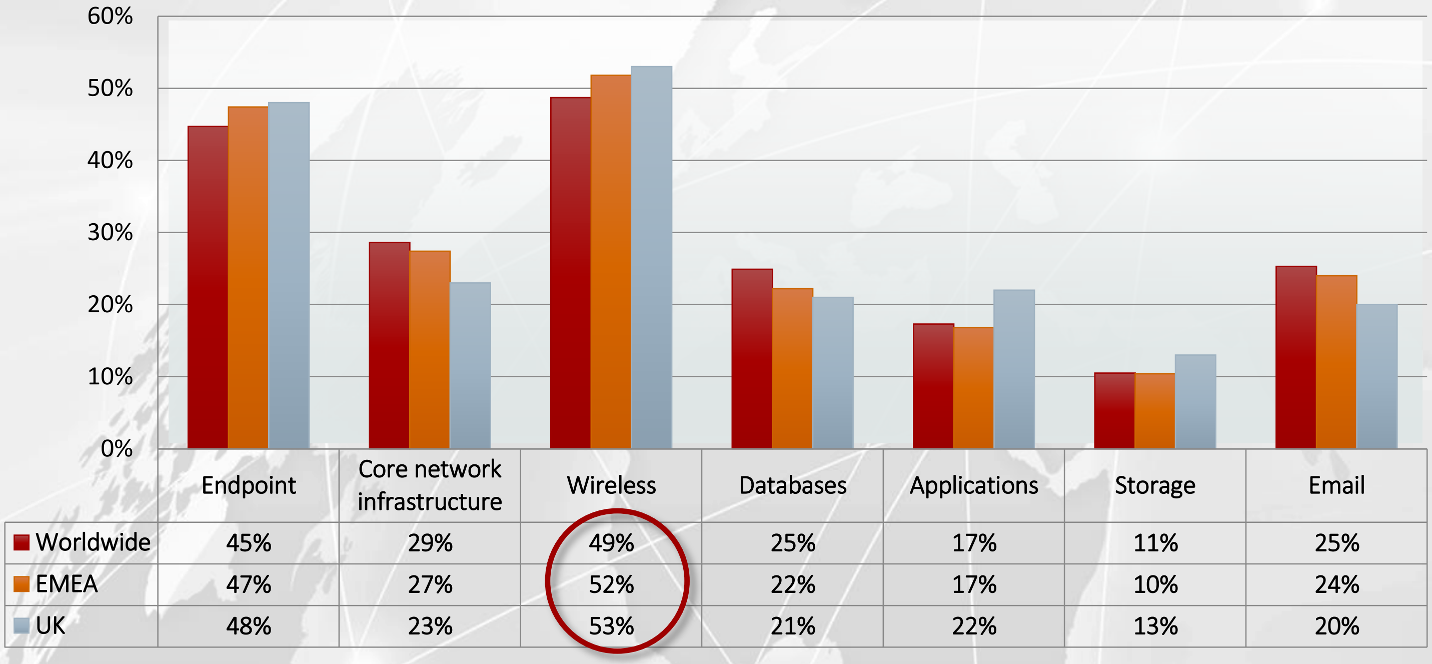
Kill Chain of an Advanced Attack



Anti-spam
Web Filtering
Intrusion Prevention
Antivirus
App Control/ IP Reputation
Bots leverage legitimate IPs to pass filters. Social engineering fools recipient.
Malicious Link
Zero-days pass IPS
Compression passes static inspection
Bot Commands & Stolen Data
Spam
Malicious Email
Fast flux stays ahead of web ratings
Exploit
URL
Malicious Web Site
Malware
Command & Control Center
Encrypted communication passes controls

Wireless Networks Ranked as the Most Vulnerable IT Infrastructure

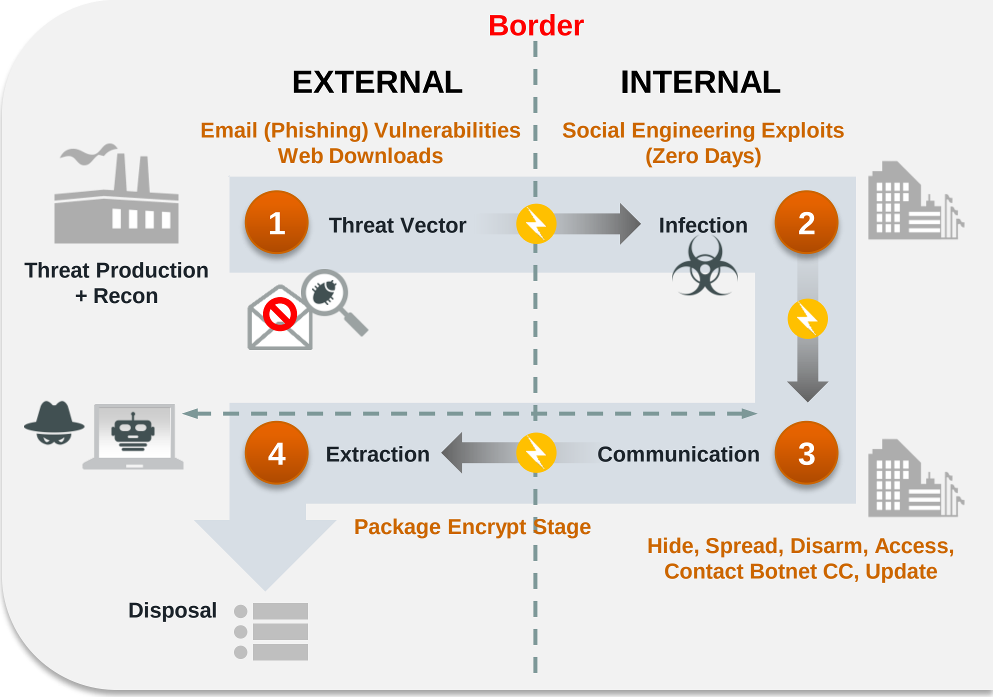
How vulnerable you believe each is from a security standpoint?



	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%

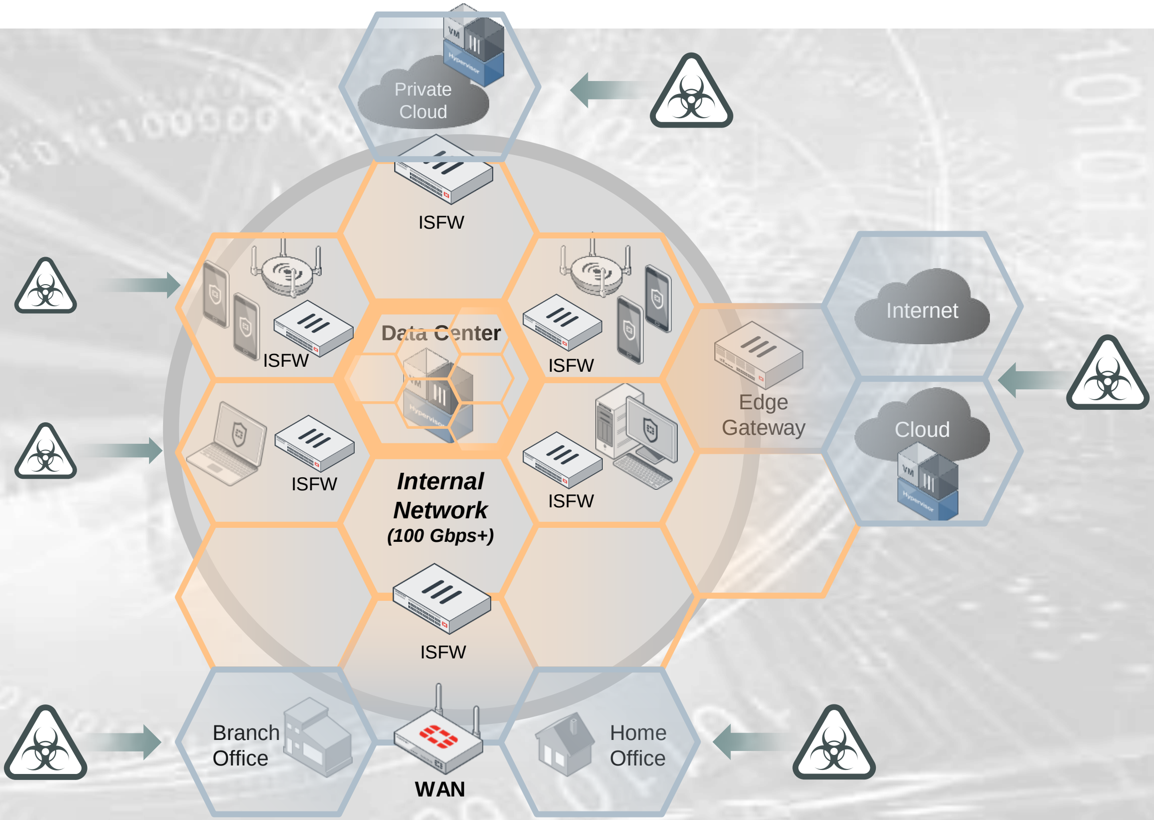
Advanced Threats Take Advantage of the "Flat Internal" Network

- Existing Firewalls focused on the **Border**
- Internal network no longer "trusted"
- Many ways into the network
- Once inside threats can spread quickly



Threat Landscape & Evolving IT Infrastructure

Internal Segmentation Firewall (ISFW)



External

Interna
l

ISFW Requirement NO. 1 - **PERFORMANCE**

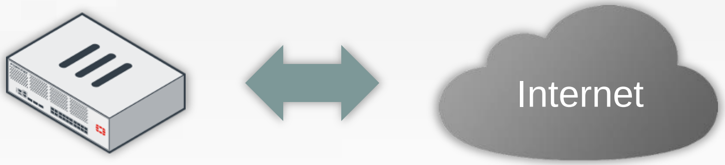
Internal Segmentation Firewall (ISFW)

Interfaces → 10G, 40G & 100G

No. of Ports → 8 to 48 Ge/10Ge

Throughput → 10Gps to 1Tbps

Border Firewall (NGFW)

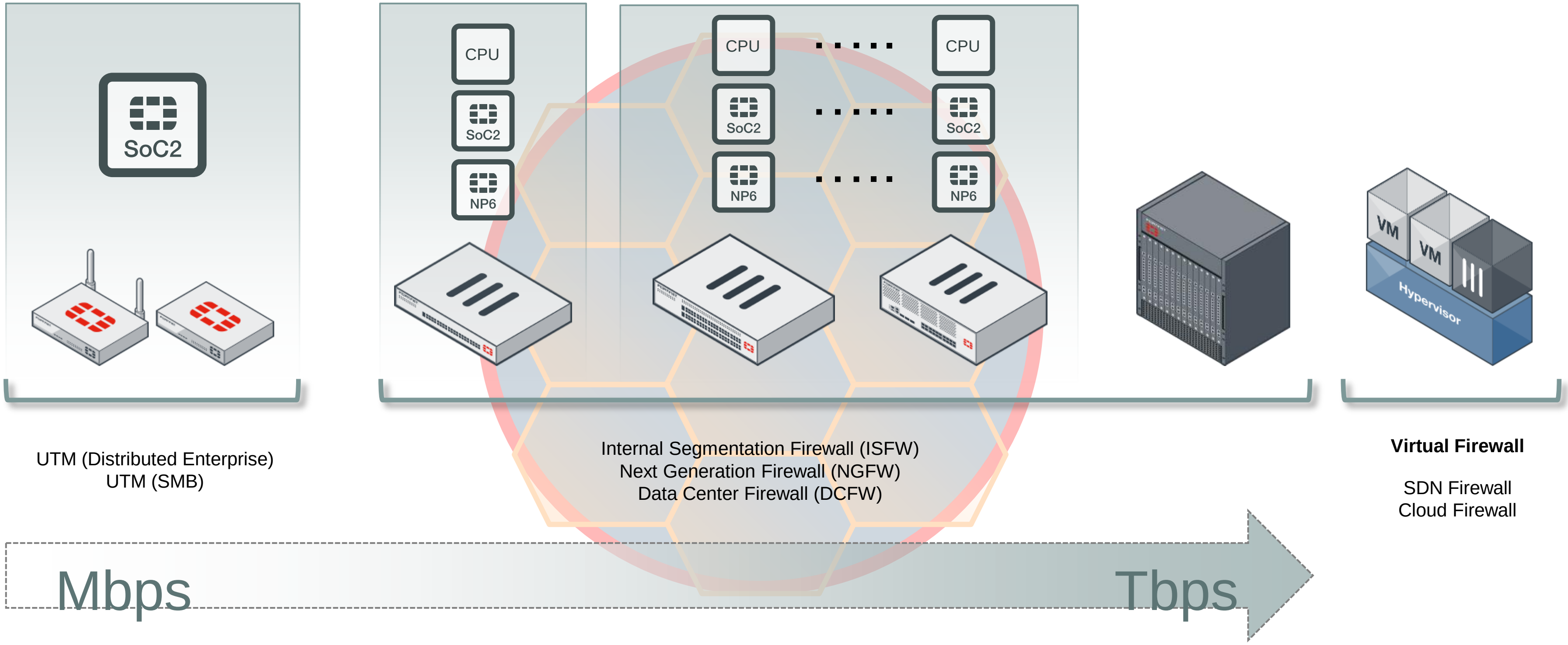


Ports Speeds → 1G, 10G

No. of Ports → 2 to 12

Throughput → Mbps to 1Gbps

High **Performance** Scalable Enterprise Firewall with **Optimum Path Processing (OPP)** Engine



UTM (Distributed Enterprise)
UTM (SMB)

Internal Segmentation Firewall (ISFW)
Next Generation Firewall (NGFW)
Data Center Firewall (DCFW)

Virtual Firewall

SDN Firewall
Cloud Firewall

- Low latency
- High speed

Conclusion in short

- ✓ Technology is important, but it is only a part of the solution
  - ✓ Always look to evaluate new solutions
- ✓ Single vendor solutions may provide an advantage
  - ✓ But only if elements actually work together
- ✓ Remember your network extends beyond you
  - ✓ Remote employees, third party suppliers and contractors
- ✓ Your employees are the first line of defense
  - ✓ Equip and use them
- ✓ Never assume
  - ✓ You’re fully protected and the network hasn’t already been breached

DON’T GO UNPROTECTED