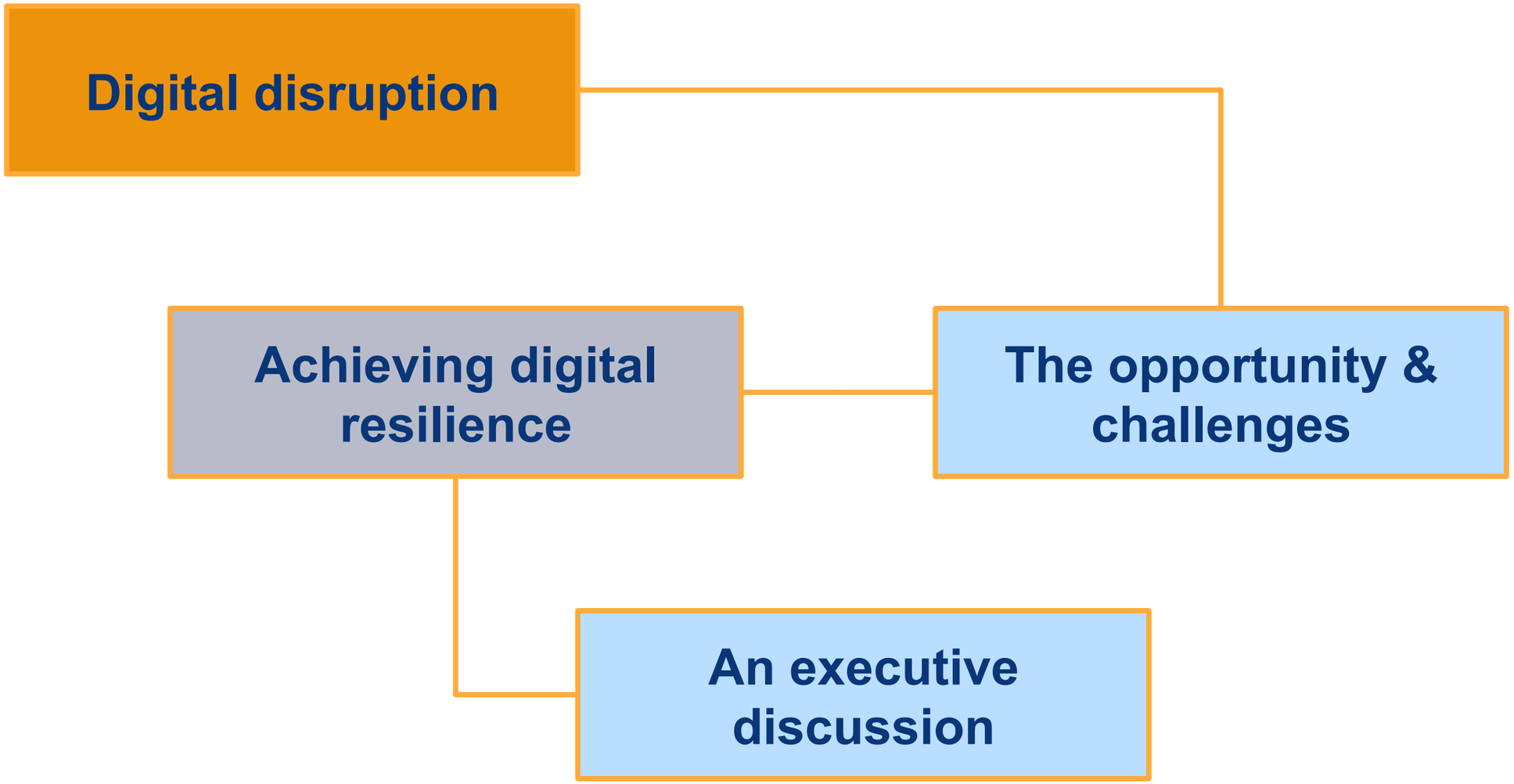
Digital Resilience in a hyper-connected world

John Ellis
Chief Strategist, Cyber Security (APJ)
Akamai Technologies

Today’s agenda



‘Resilience’

Our world is changing

Today's state of the art, is tomorrows obsolete

Rules are becoming much less certain

To remain competitive we must evolve

Be more flexible

Respond more quickly

…and provide a service that offers value

The revolution

World’s largest taxi company owns no taxis

UBER

The revolution

World’s most popular media owner creates no content

The most valuable retailer has no inventory

Alibaba.com™

The revolution

World’s largest accommodation provider owns no real estate

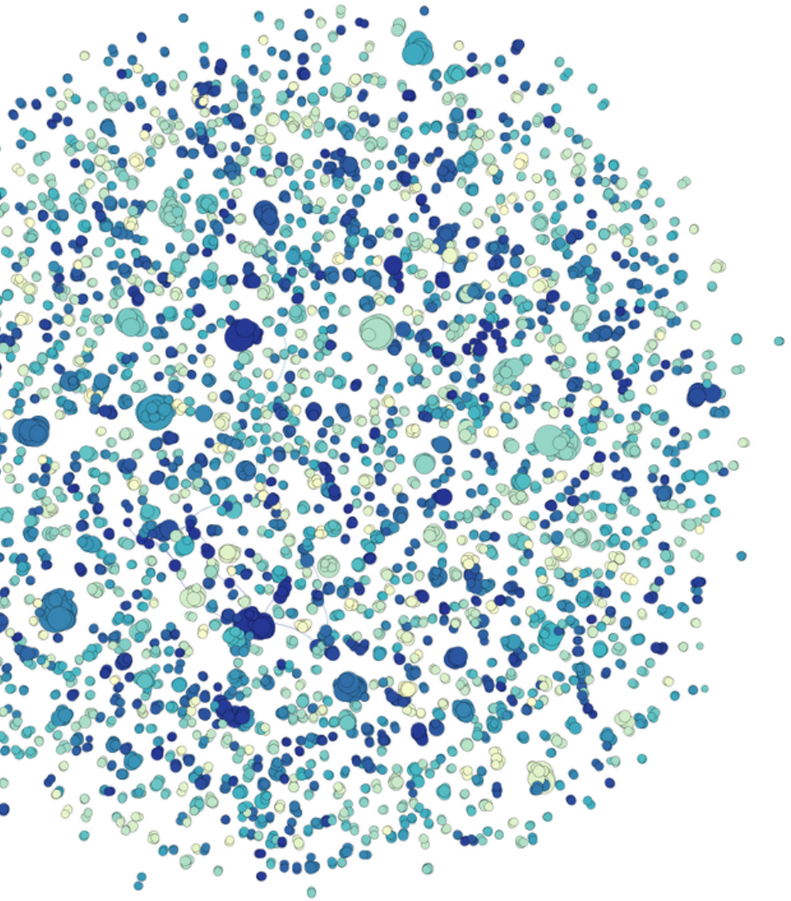
airbnb

Everyone and everything is getting connected.

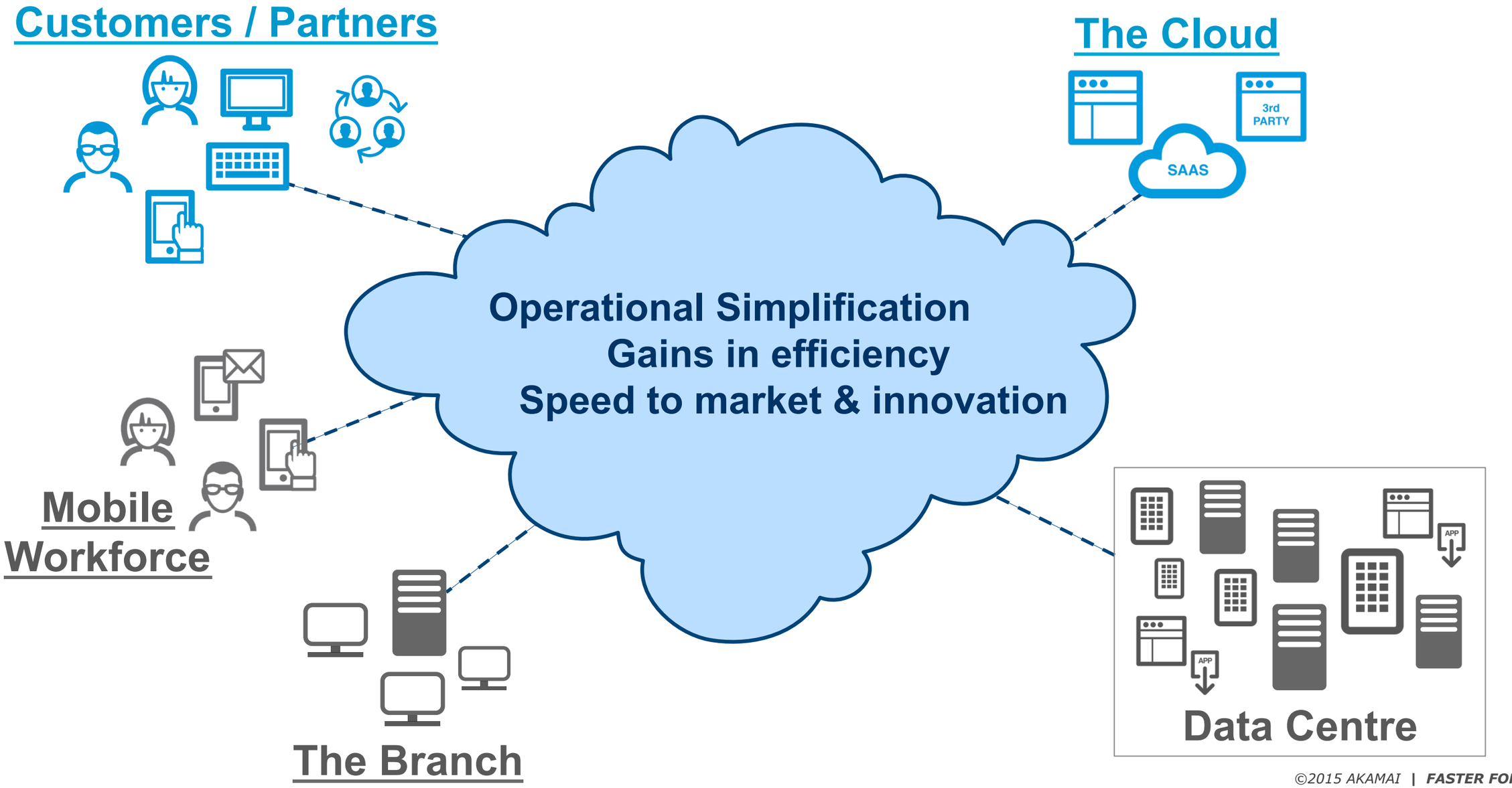
COUNTLESS PETABYTES OF DATA TENS OF BILLIONS OF DEVICES

BILLIONS OF PEOPLE

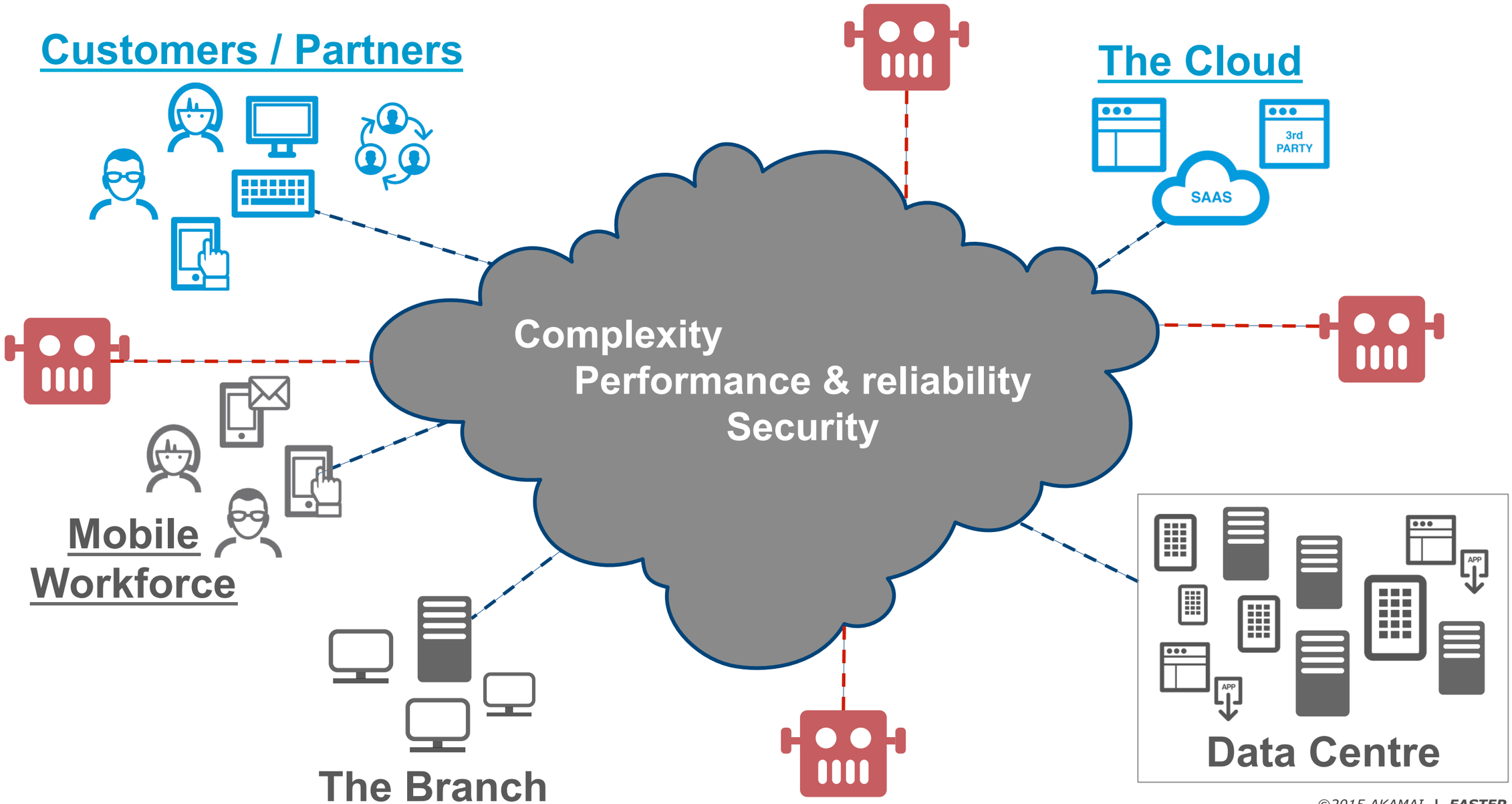
Technology trends that are enabling disruption and innovation



The Internet: The Opportunity



The Internet: The Challenges



It’s a complex yet very fragile eco-system

We’re still solving yesterday’s problems as well as today’s and trying to think about tomorrow’s. It’s complex but somehow works…..just

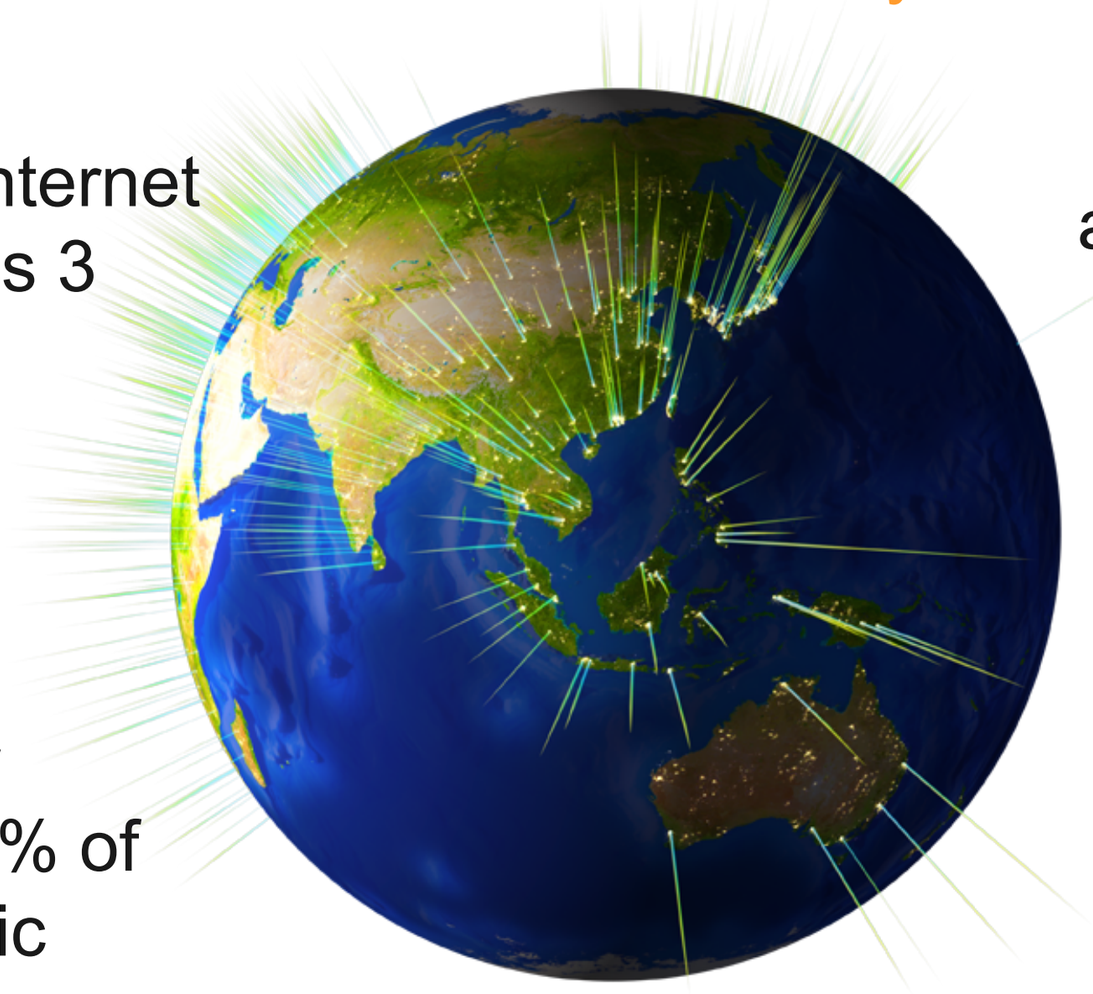
The perimeter as we knew it, is dead!

A.B.C has killed your perimeter!
Data is the new perimeter, but we can manage the risk

The nexus of innovation and connectivity

The number of Internet users will surpass 3 billion this year

Asia accounts for approximately 45% of internet users – 1.35 billon users



Asia accounts for approximately 70% of global attack traffic

What alternative is there to connect your customers?

The Internet

NOTHING IS SAFE


U.S. bank website hackers used advanced botnets, diverse tools
'Anonymous' hackers launch cyberattack on Israeli sites
There's nothing virtual about cyber attacks
By Bob Greene, CNN Contributor
updated 10:10 AM EDT, Sun October 7, 2012
A perfect storm' of cyber attack
India Under Cyber Attack From China
UK media websites hacked by Syrian Electronic Army
Among those targeted were
Bank-Busting Jihadi Botn
Life. But Who Is Controll
Bob Greene says as more of our everyday lives become bound to the digital world, we are vulnerable to hackers, cyb
Why the Bash bug will be a big headache
sh-3.2$ env x='()
rable' bash -c "ec
vulnerable
this is a test
Scams
Cybercrime now becoming a serious problem for many Britons
Russian Hackers Amass Over
Passwords
Russia gang hacks 1.2 billion usernames and passwords
European Central Bank website hacked
e group is alleged to have stolen credentials from hundreds of thousands of websites globally
REUTERS
Security Exp
Software Bug in Bash to Be Signific
Voluntary Sector Network
London-based charity hacked by pro-Isis group
continues to rise in India; 78 this year
govt sites shut down from apparent cyberattack
Summary: The country's presidential office and government policy coordination Web sites said
currently shut down for repair.
Nightly News | April 04, 2013
Bank cyber attack a 'major assa
industry
An ongoing series of attacks on the U.S. financial industry
before has resulted in a 15 of the largest U.S. banks being offline for a total of 249 h
Czech central bank, stock exchange, banks
hacked
NEWS
Anonymous Launches Operation Wall Street, Targets CEOs
Mathew J. Schwartz
See more from Mathew
Connect directly with Mathew:
Bio | Contact
Hacktivist collective cites mortgage crisis, Aaron Swartz and bank spying in call to arms to dox "any
and all personal information" on financial services firm executives.
GETS REGIONS BANK CUSTOMERS
42°
10:15
News Channel 5
KNOCKOUT GAME KILLER
DOG DRAGGED DOWN I-55
Hackers Assault Tel Aviv Stock Exchange, El Al Websites, Causing Slowdown

OperationAbabil @OccupyG20BNE

@Press_ECA OpIsrael OpGreenRights

Vietnamese Carders @AnonOpSaudiX

#LegionOps UGNazi OpFerguson

OccupyCentral @TN_cyberarmyRevizer

Traditional Hackers Political Hacktivism

Glory Hounds Testing Extortion

Business Competition Fear Factors

Protest State Sponsored Recon

Identity Theft Intellectual Challenge

Account Checkers Skipfish Shellshock

WebHive Pagination Proxy Pivoting

Slowloris UDP Flood Slow HTTP Post

Spoofed Origin Accunetix Darkness

LOIC Fraggle RUDY Pyloris Spike

WHO

WHY

HOW

OpPetrol OpHackingCup Tweet4Taiji

OpSaveGaza al-Qassam Cyber Fighters

@AnonHackNews @official_sea16

NaoVaiTerCopa OpMundial2014

FreeAnonsSG OpKillingBay Sochi2014

Defacing Content Disruption Revenge

Excitement Intellectual Property Theft

Credit Card Theft Personal Gratification

Mischief Research Fun Publicity

Profit Prestige Chaos Thrill

Dirt Jumper Cross-Site Scripting (XSS)

ICMP Flood HashDoS SYN Flood

Blackshades RAT SNMP Amplification

DNS Amplification HOIC Brobot

NTP Amplification Havij ApacheKiller

$400 Billion

annual cost of cyber attacks

and it's growing at least 25% every year!

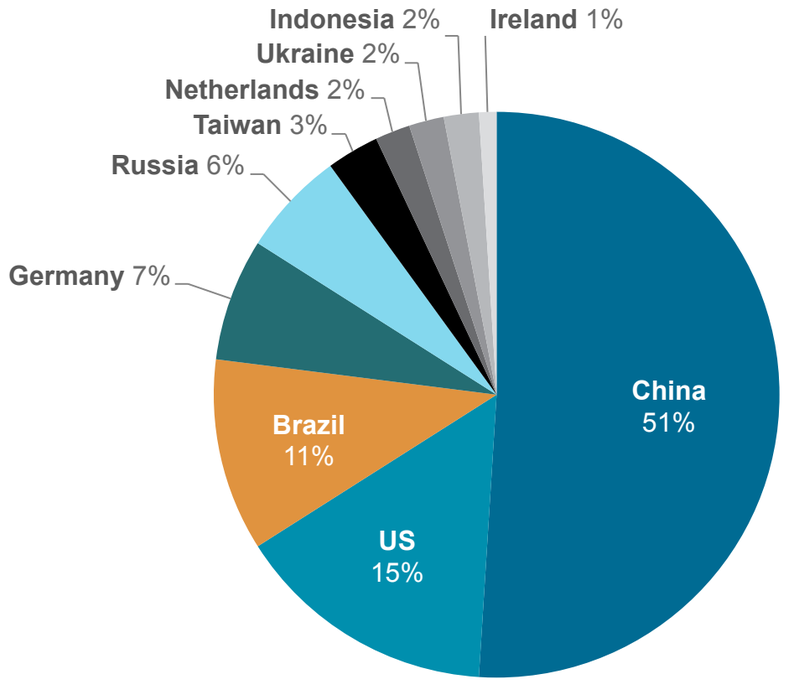
Web Attack Activity

Q2 2015

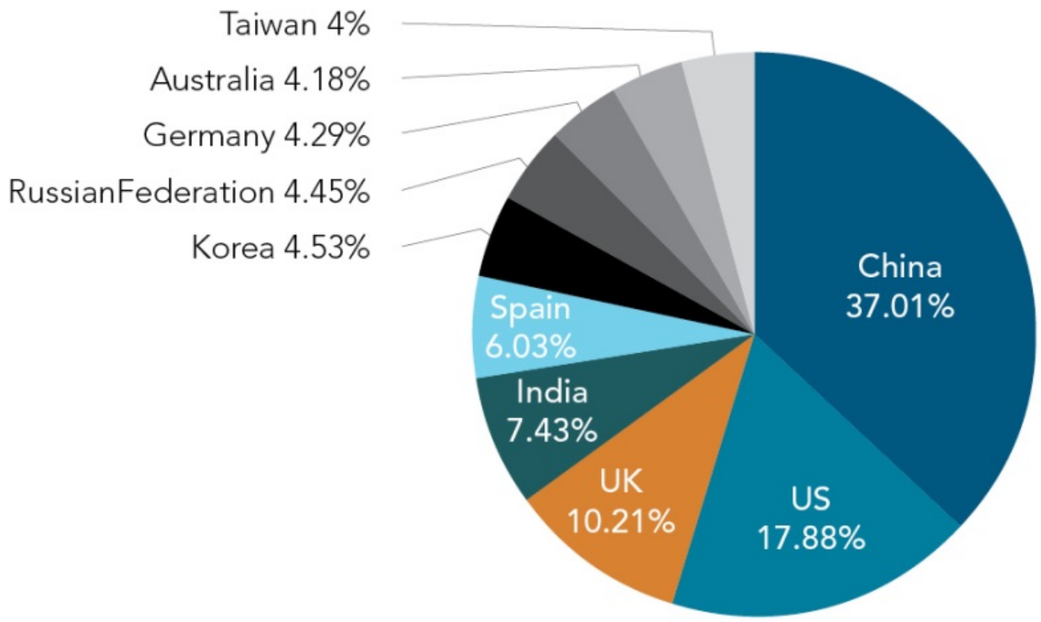
Web & DDoS

ATTACKS BY COUNTRY

Top 10 Source Countries (Web Attacks)

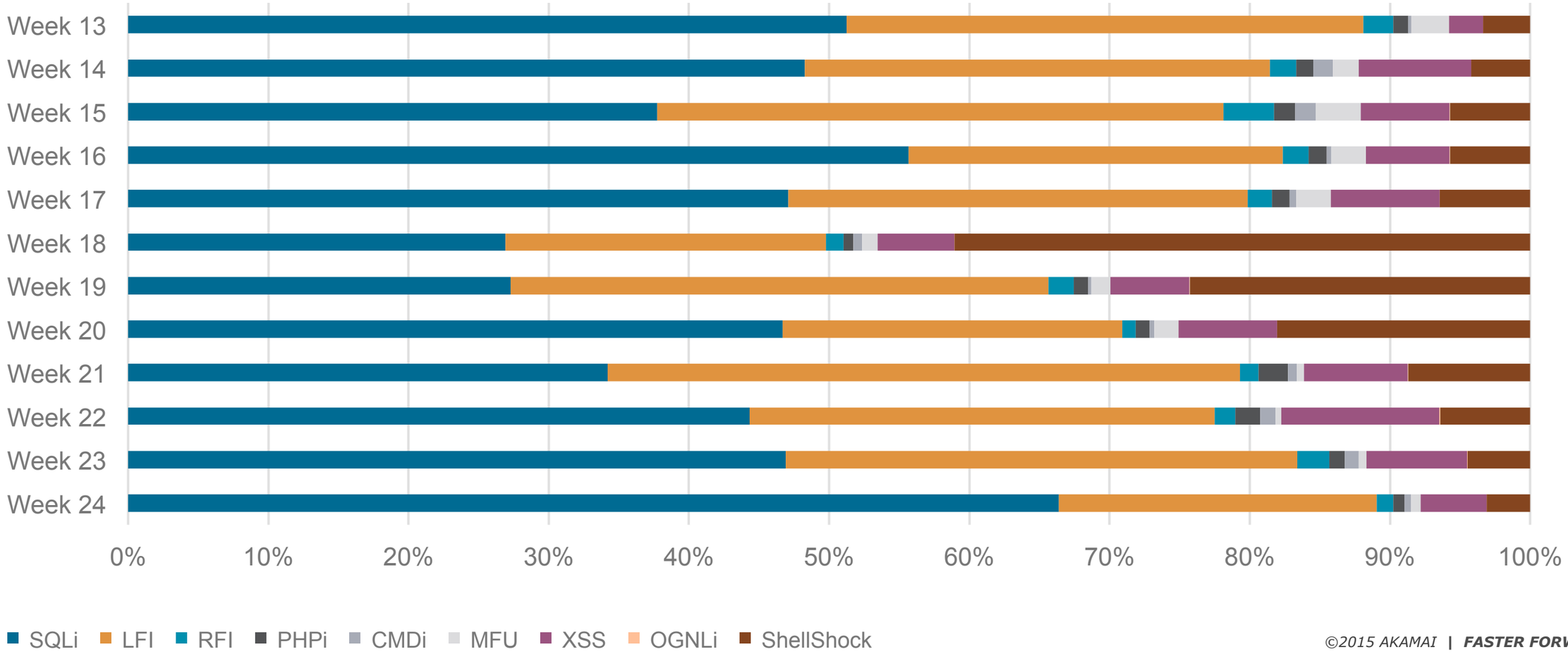


Top 10 Source Countries (DDoS attacks)



Web attack vectors

BREAKDOWN BY WEEK



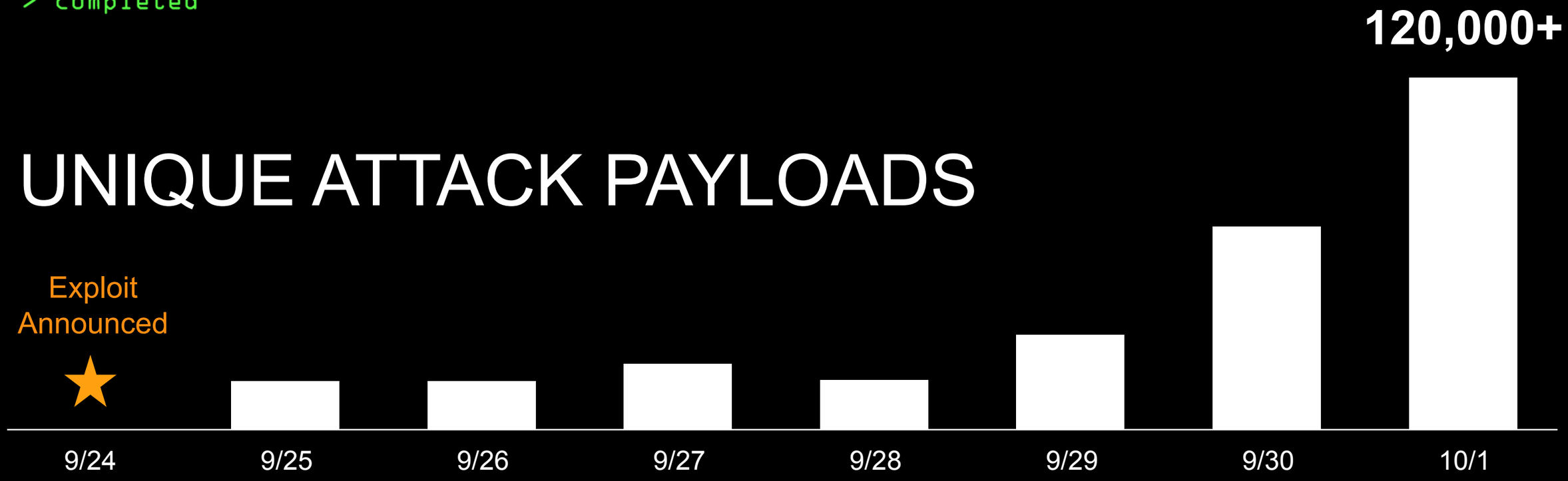

HEARTBLEED

#!/bin/bash_

```
~root: env X="() { :;} ; echo shellshock" /bin/sh -c "echo completed"

> shellshock
> completed
```

UNIQUE ATTACK PAYLOADS

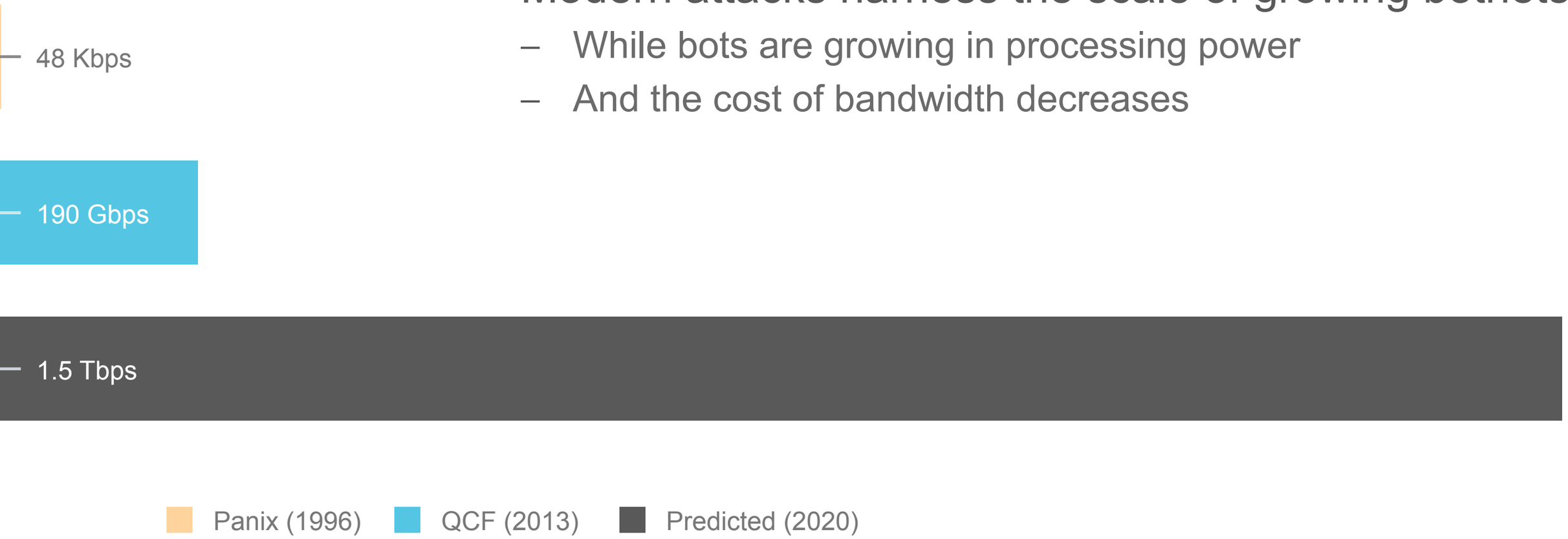


DDoS Attack Activity

Q2 2015

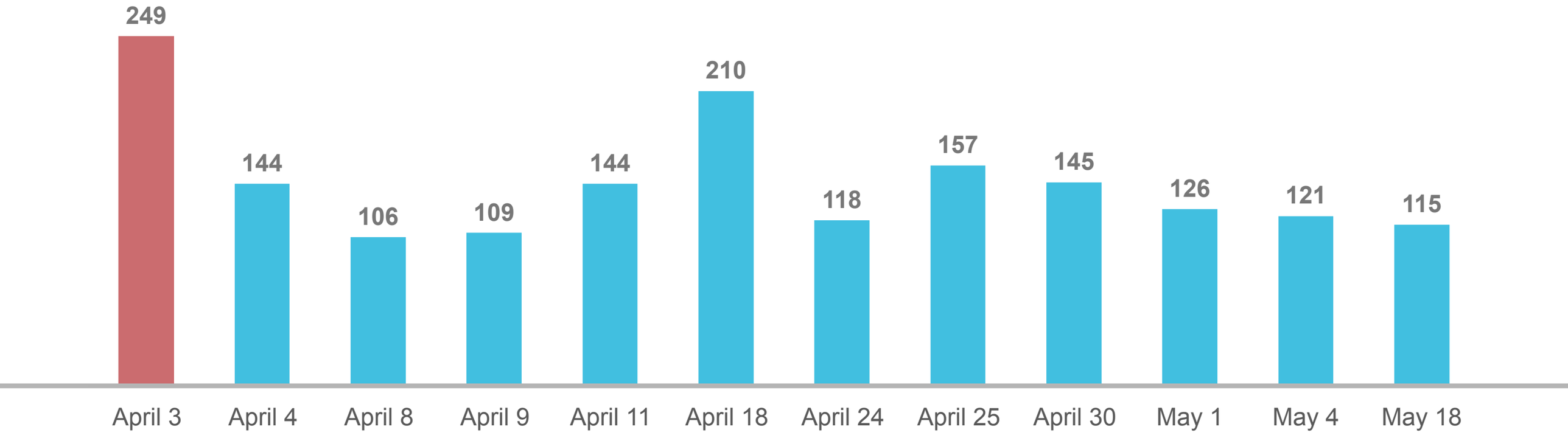
Denial-of-Service Attacks Growing in Size

- Modern attacks harness the scale of growing botnets
  - While bots are growing in processing power
  - And the cost of bandwidth decreases



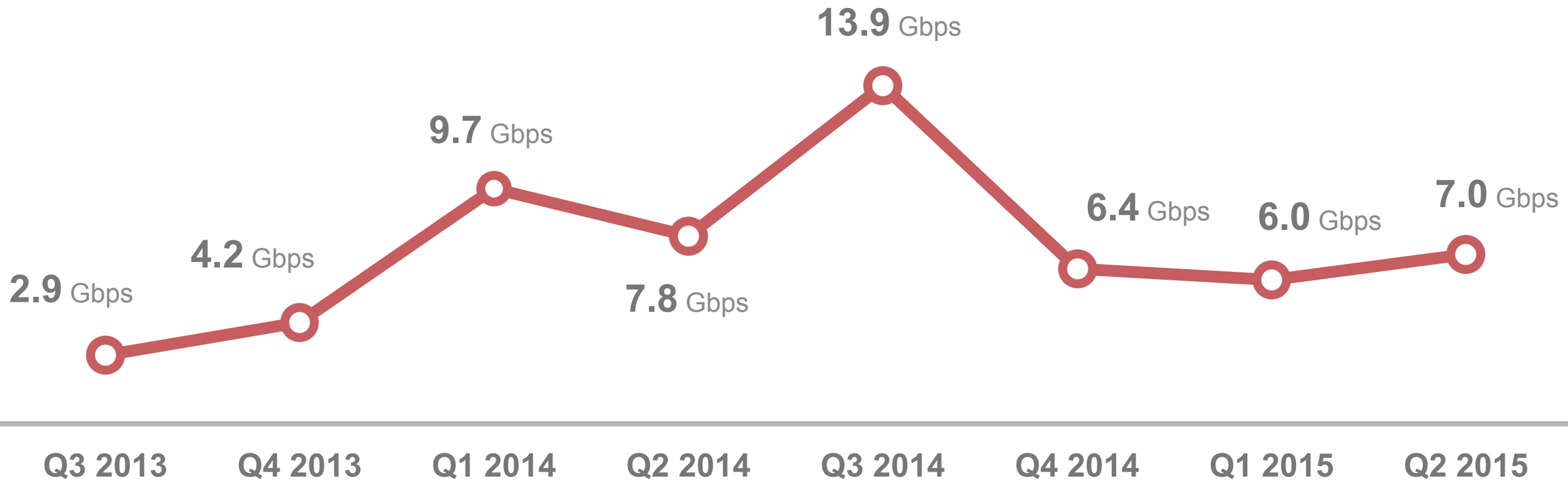
Attacks > 100 Gbps

MEGA ATTACKS



Average attacks require cloud

AVERAGE SIZE



DDoS Extortion

Growing trend in Q2 2015

DDoS for Bitcoin

THREAT COMPONENTS

1. **Motivation** – DDoS attacks for ransom
2. **Objective** – obtain bitcoins as payment
3. **Members** – unknown
4. **Resources** – booter / stresser toolkits, DDoS-for-hire botnets
5. **Knowledge source** – publicly available tools
6. **Victimology** – bitcoin Ex / gaming sites to reputable business operations
7. **Typology** – publicly available DDoS toolkits plus rented botnets

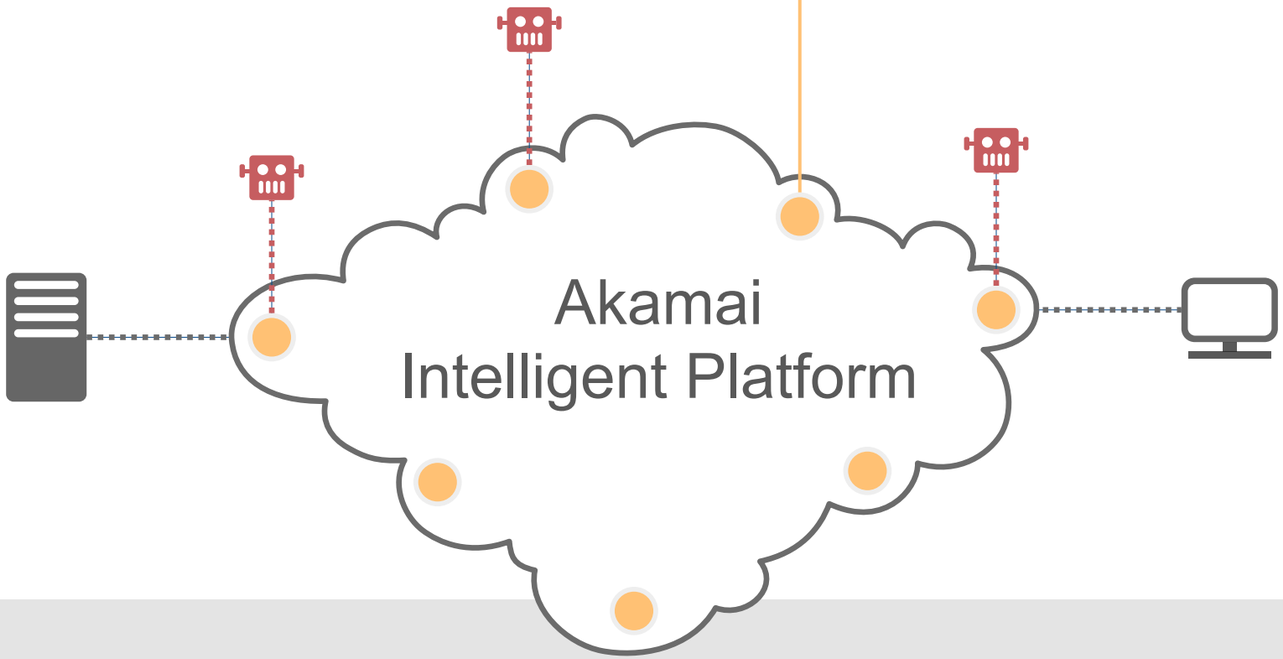
Globally distributed cloud platform

Scale | over 200,000 servers | six scrubbing centers | more than 2,000 name servers

Distribution | 117 countries | over 2,700 locations | more than 1,300 networks

Resiliency | automatic failover within network | multiple networks for independent services

Integrated web security

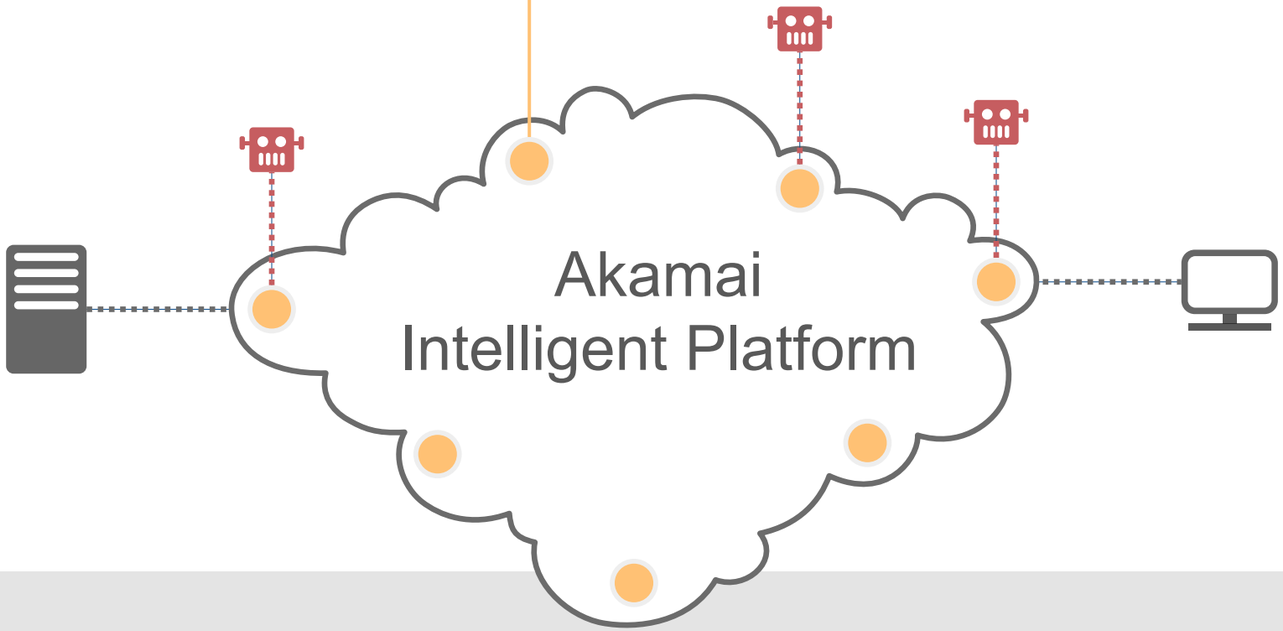


DDoS | always-on protection | automated response within seconds

WAF | proprietary rules engine | highly accurate | no performance impact

IP reputation | hundreds of millions of IPs monthly | customize policies based on risk of attack

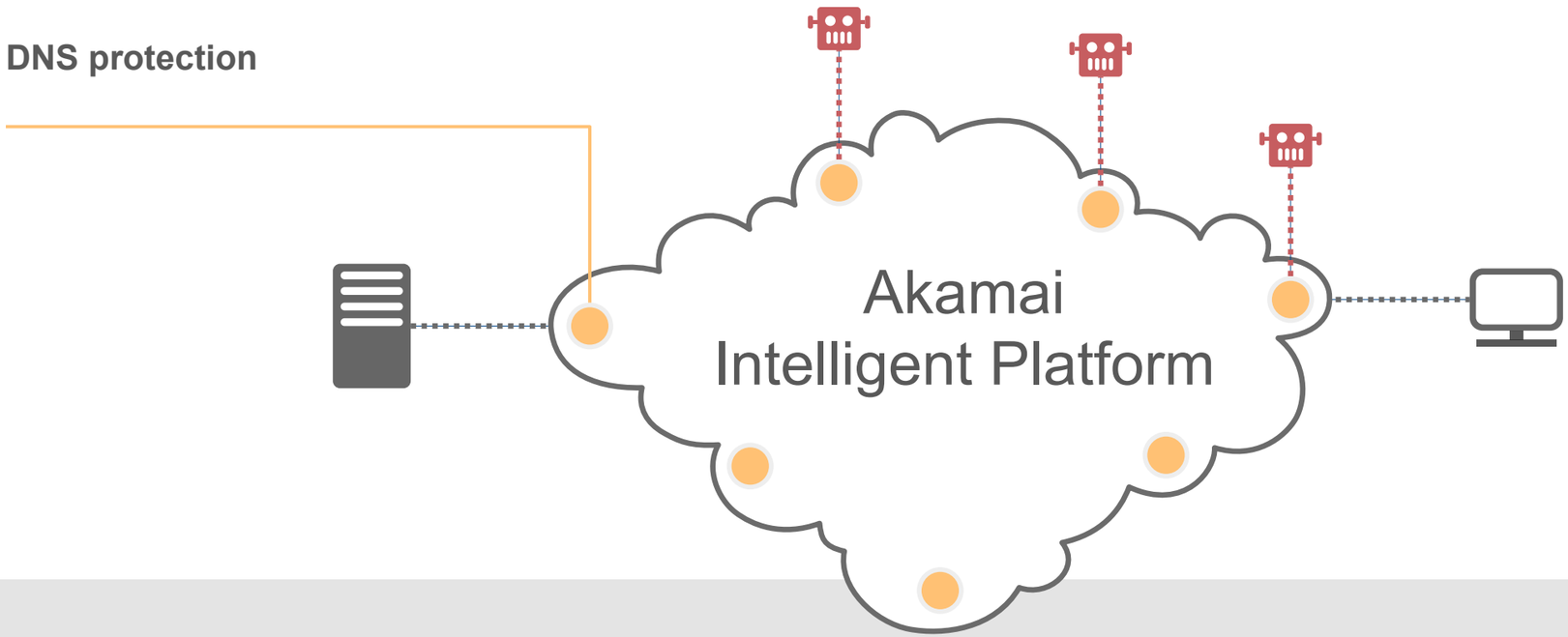
Infrastructure protection



DDoS | people-driven response | customized mitigation | time-to-mitigate SLAs

Data center | hundreds of applications | network infrastructure | Internet bandwidth

Flexible deployment | always-on or on-demand | 24x7 traffic monitoring

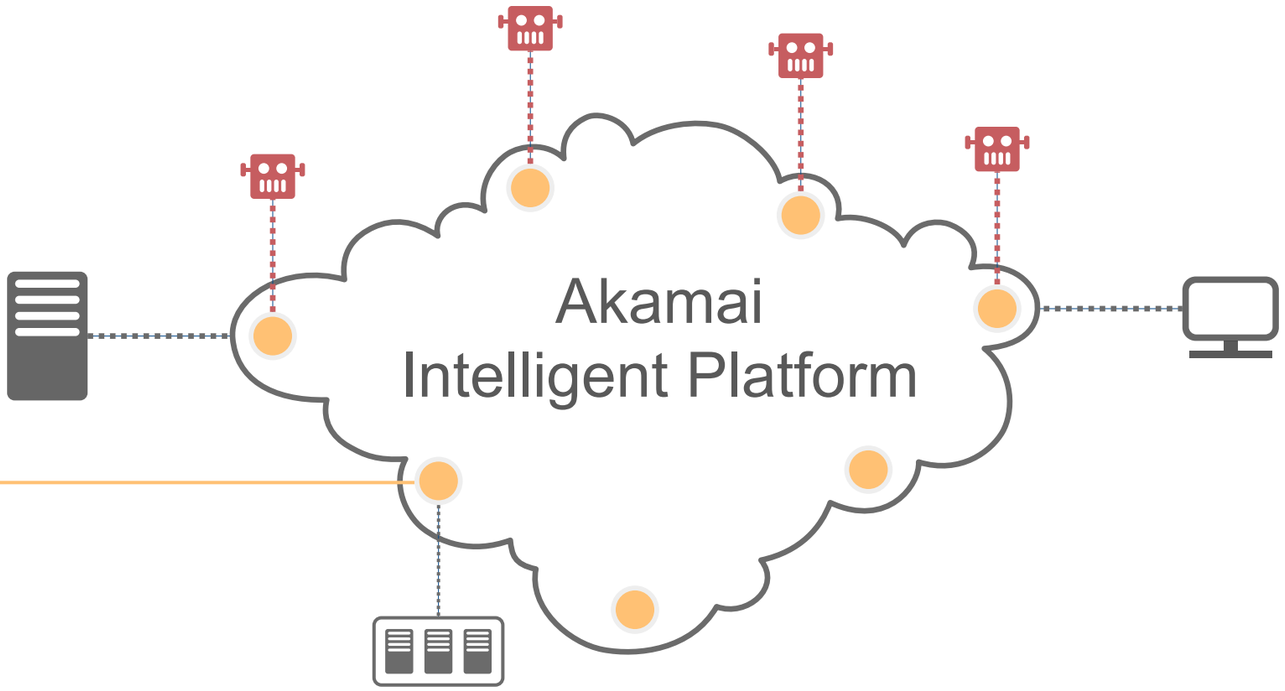


DDoS | adaptive rate limiting | white listing | multiple redundant DNS clouds

DNSSEC | optional protection against DNS forgery | Serve or Sign-and-Serve

DNS experience | high-performance DNS cloud | zone apex mapping

Cloud Security Intelligence



Visibility | 15-30% of global web traffic | every Akamai customer

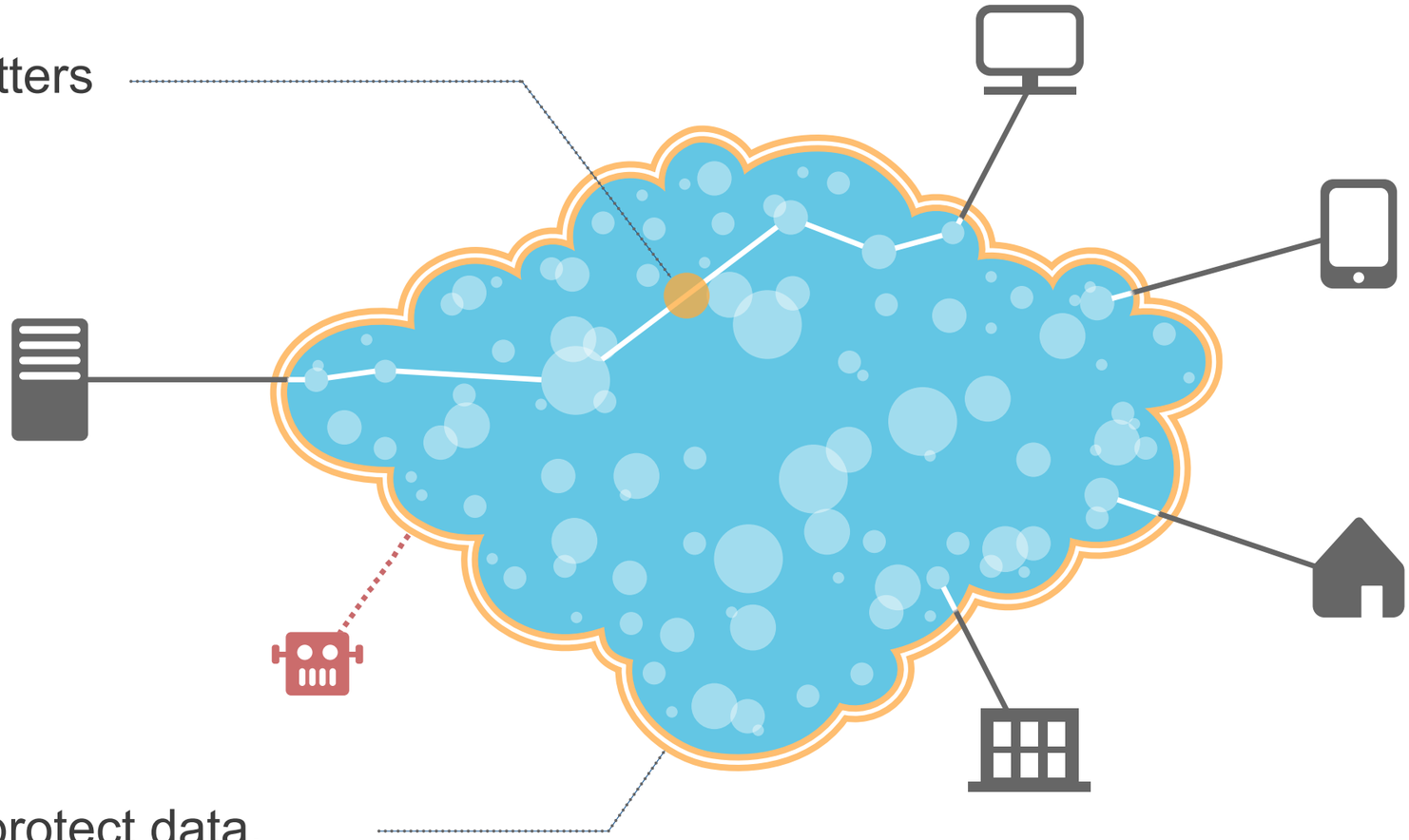
Data | 80 million WAF triggers per hour | 600,000 log lines a second | 20 TB new attack data daily

Analysis | dedicated threat research team | 8,000 queries a day

Building a Better Digital Bank Web Experience

Performance

Every millisecond matters



Security

Maintain availability, protect data,
and protect transaction integrity

EXECUTIVE DISCUSSION ON SECURITY

Security is a business issue with a technology element

Are we prioritizing our security investments correctly?

How do we know our security investments are improving our security posture?

Are we focusing enough on protecting what matters the most?

How ready are we to respond to cyber attacks?

How do we know we have or haven’t been hacked, breached, or compromised?

Security needs to be tailored

Organizational constructs

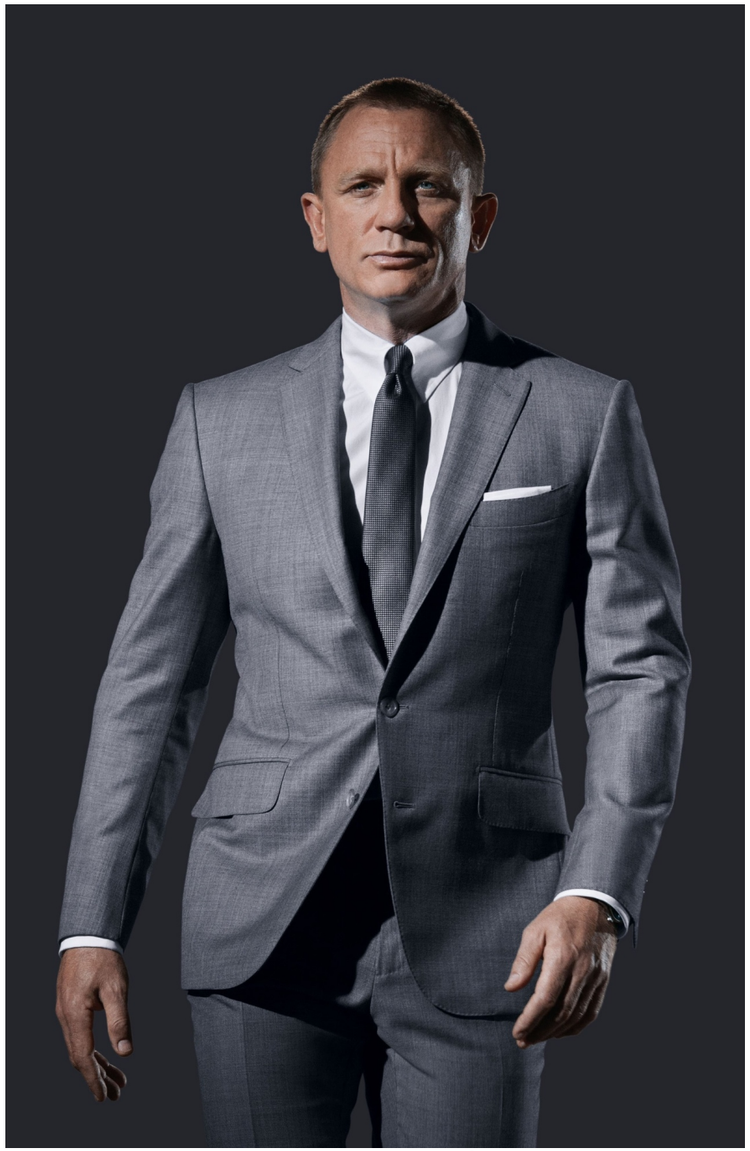
Geography & culture

Industry

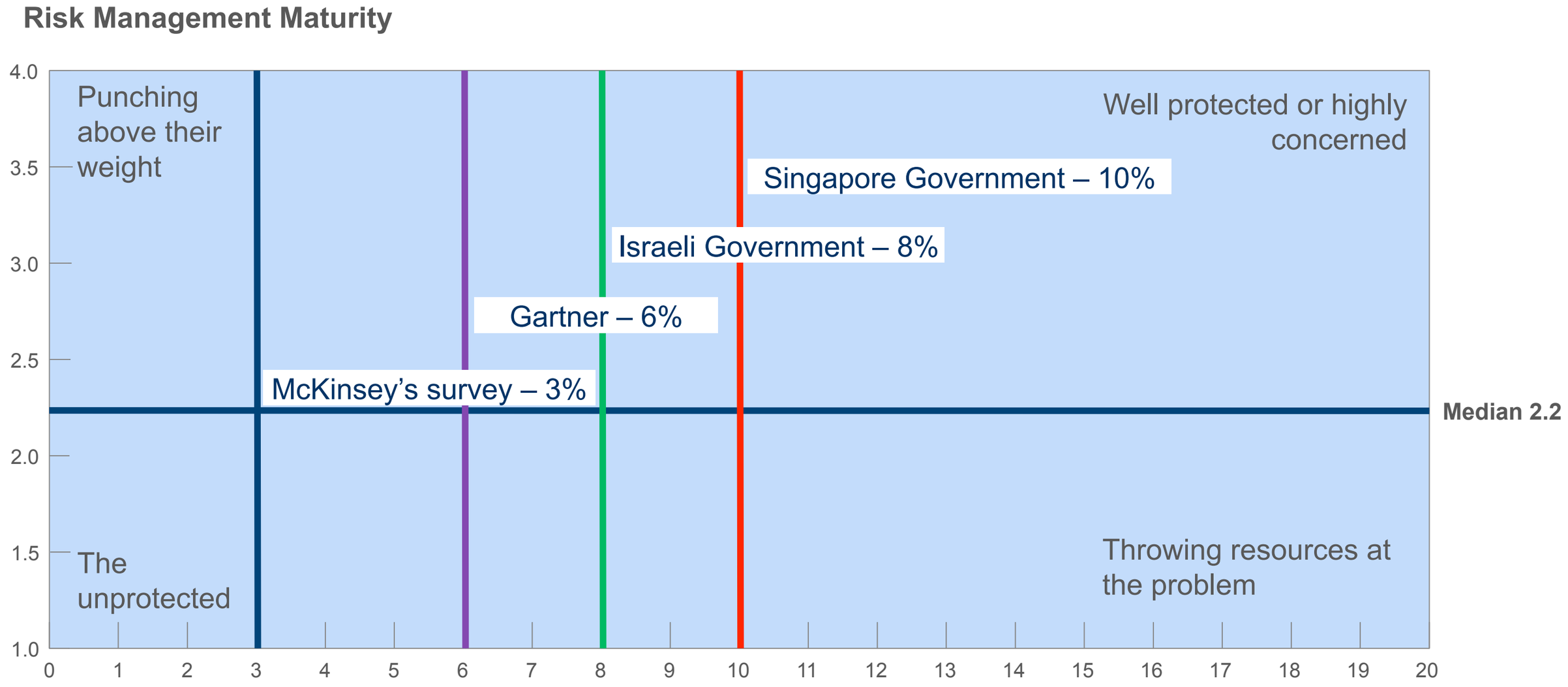
Resources & capabilities

Technology adoption & maturity

Process & how data is used

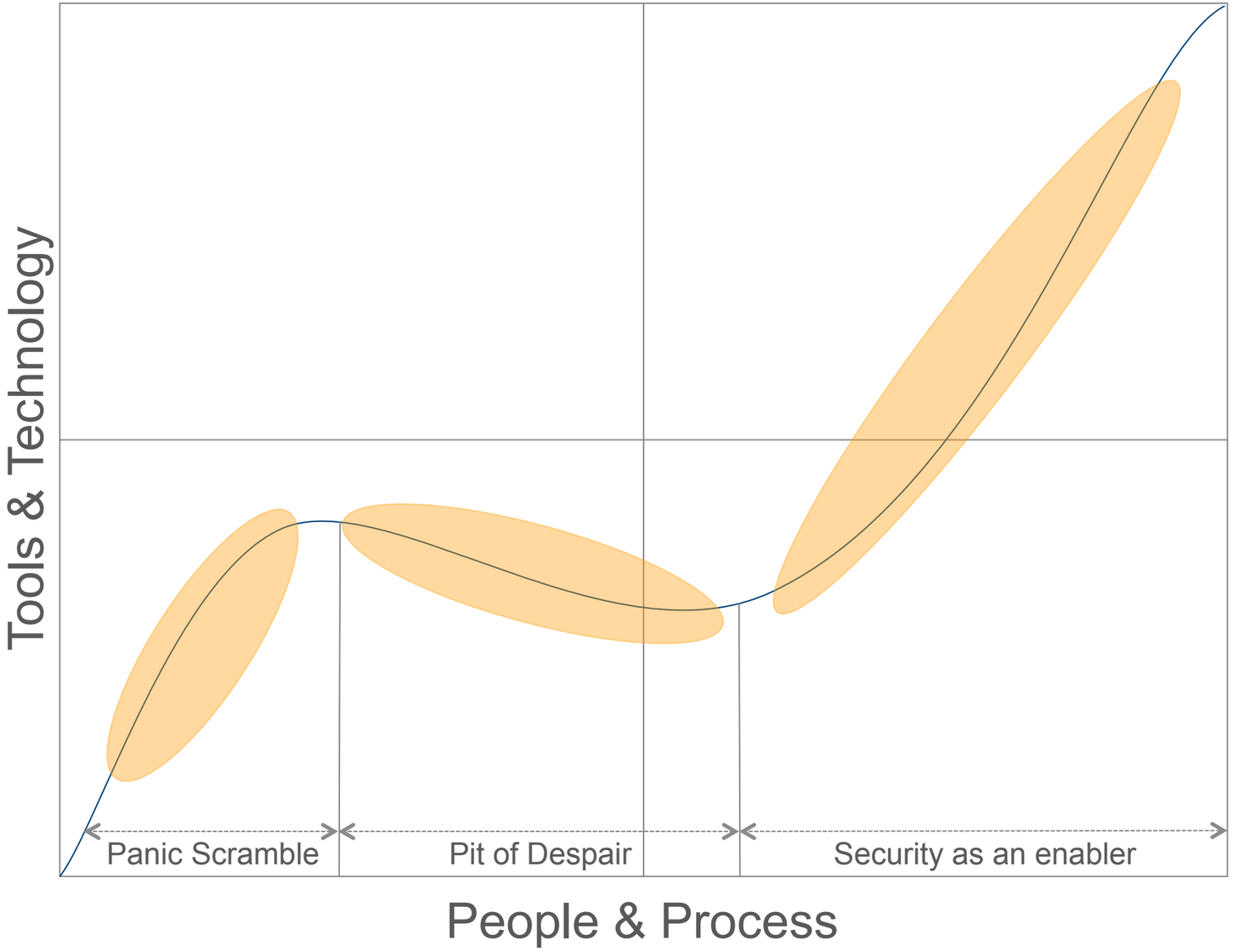


How much to spend to achieve resilience?



Source: Beyond Cybersecurity: Protecting your digital business
ISBN: 978-1-119-02684-6

Security Buyers Maturity Curve



Panic Scramble

- Typically responding to a security incident
- Need to make immediate security investments
- Over reliance on technology with little understanding of complexities

Pit of despair

- Realization that security tools fail to reduce risk
- Security is not as pervasive as originally thought
- Re-think on how to leverage investment, tools, people, and process to achieve desired state

Security as a core process

- Realize that security needs to be engrained in business processes
- Dedicate more budget to security investment
- Security processes are repeatable and consistent

Digital Resilience – build a robust, strong and safe business

Prepare – Absorb – Recover – Adapt

THANK YOU.