Security matters

Financial crime prevention: 'the human factor'

Terry Greer-King
Director, Cyber security, UK & Africa

February 2017

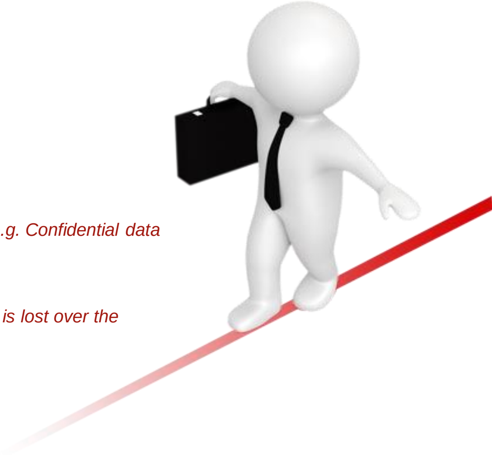
‘There are only two types of organisations in the world……’

Actually Cyber Security is actually all about risk, risk to people and business..

- Risk: ***Likelihood*** *that a* ***threat*** *will exploit a* ***vulnerability*** *and cause harm*
- Vulnerability: *A flaw or* ***weakness*** *that allows* ***threat*** *to succeed in causing harm*
- Threat: *A possible* ***danger*** *that might* ***exploit*** *a* ***vulnerability*** *to breach security and therefore cause possible harm*
- Likelihood: *A rough* ***measure*** *of how likely a particular* ***vulnerability*** *is to be uncovered and* ***exploited***
- Exploit: *Something that takes advantage of a* ***vulnerability*** *to cause harm*
- Impact: ***Extent*** *of the resulting harm*
- Options for Treating Risk:
  - ***Transfer***
  - ***Avoid***
  - ***Reduce***
  - ***Accept***

Risk is the probability of a **threat agent** exploiting a **vulnerability** and the resulting business **impact**. For example, an open port could be a vulnerability and the corresponding threat agent could be a hacker who gets through that port and causes damage or loss, such as accessing customer credit card information in a backend database.

Understanding risk



- What's the "Hazard" we are talking about – *Hazard is something that has potential to cause damage e.g. Confidential data stored in live computing environments, PCI related maybe*
- What are the "Top events" that can emerge from the "Hazard" – *Moment when control is lost over the Hazard e.g. unauthorized access to the confidential data*
- What leads to this Top event – *In other words "Threats" that will cause top event e.g. A Malware*
- What are the potential consequences of this – *Results from the Top Event e.g. Exposure to sensitive data, Reputational damage, Legal or Regulatory Action*
- Are there any controls/"barriers" in place already – *Barriers interrupt the scenario so that the threats do not result in a Loss of Control (the Top Event) or do not escalate into an actual impact (the consequences)*
- Are there any potential vulnerabilities/ weaknesses from the controls themselves – *If the barrier fails e.g. For instance, a door that opens and closes automatically using an electrical mechanism might fail if there's a power failure; A solution for this might be a Backup Generator!*
- Explore and complete the Risk state – *can the risks can be quantified ?*
- Close the Loop before moving to the next phase – *Have we covered everything?*
- Move to the next phase – *We should have covered both Why and What by now. The potential next step is defining the "how"*

So where are we ?

Security as an after thought

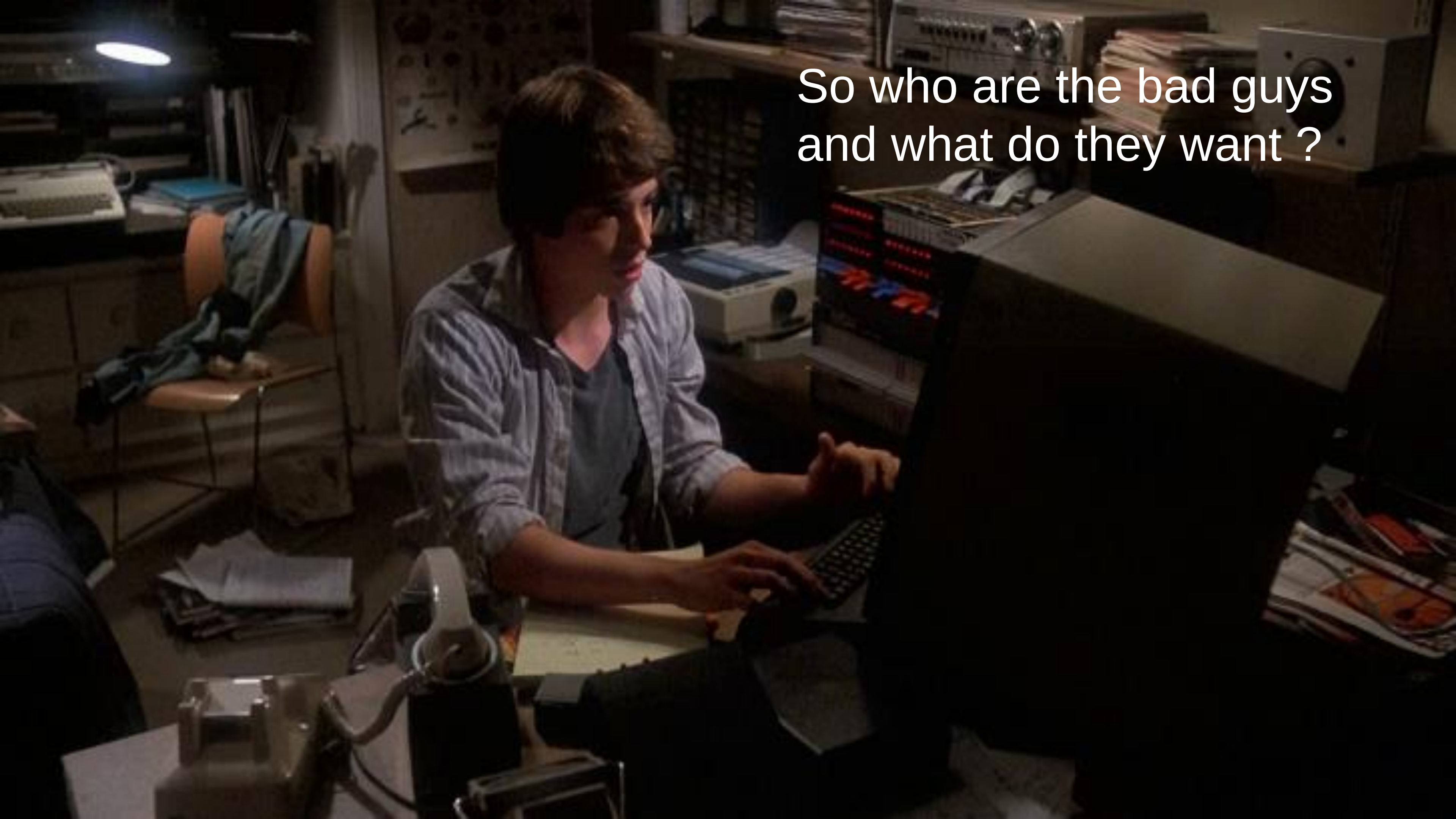
Security whack-a-mole

Not Operationalised

Technology Lead

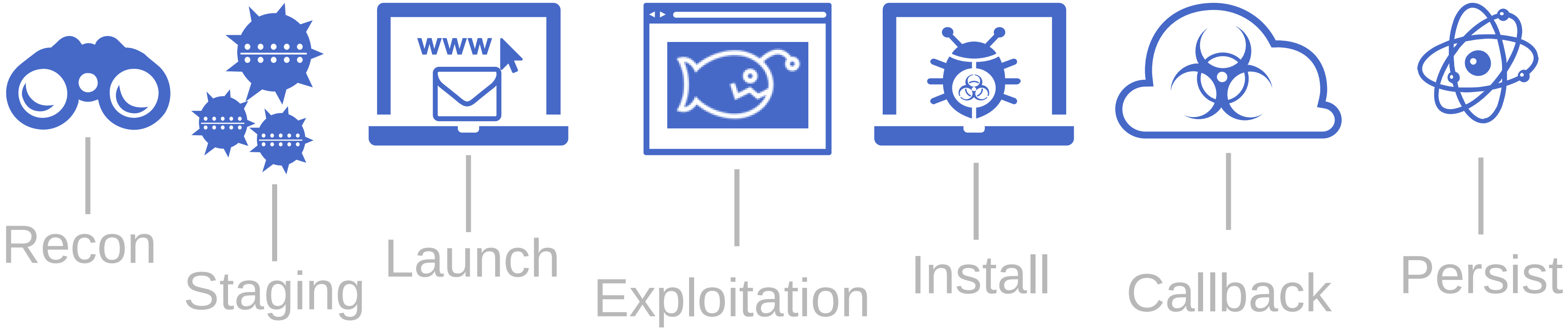
Security vs. Compliance

Fragmented and siloed



So who are the bad guys
and what do they want ?

Different stages of an attack



Recon

Staging

Launch

Exploitation

Install

Callback

Persist

Watching and Waiting

Adversaries Take Time Inspecting and Looking for Opportunities

12K Browser Redirection

15K Phishing attempts

35K Facebook Scam Links

18K Browser Redirection-Downloads

87K Suspicious Binaries

27K Trojan Downloaders

50K Trojan Droppers (VBS)

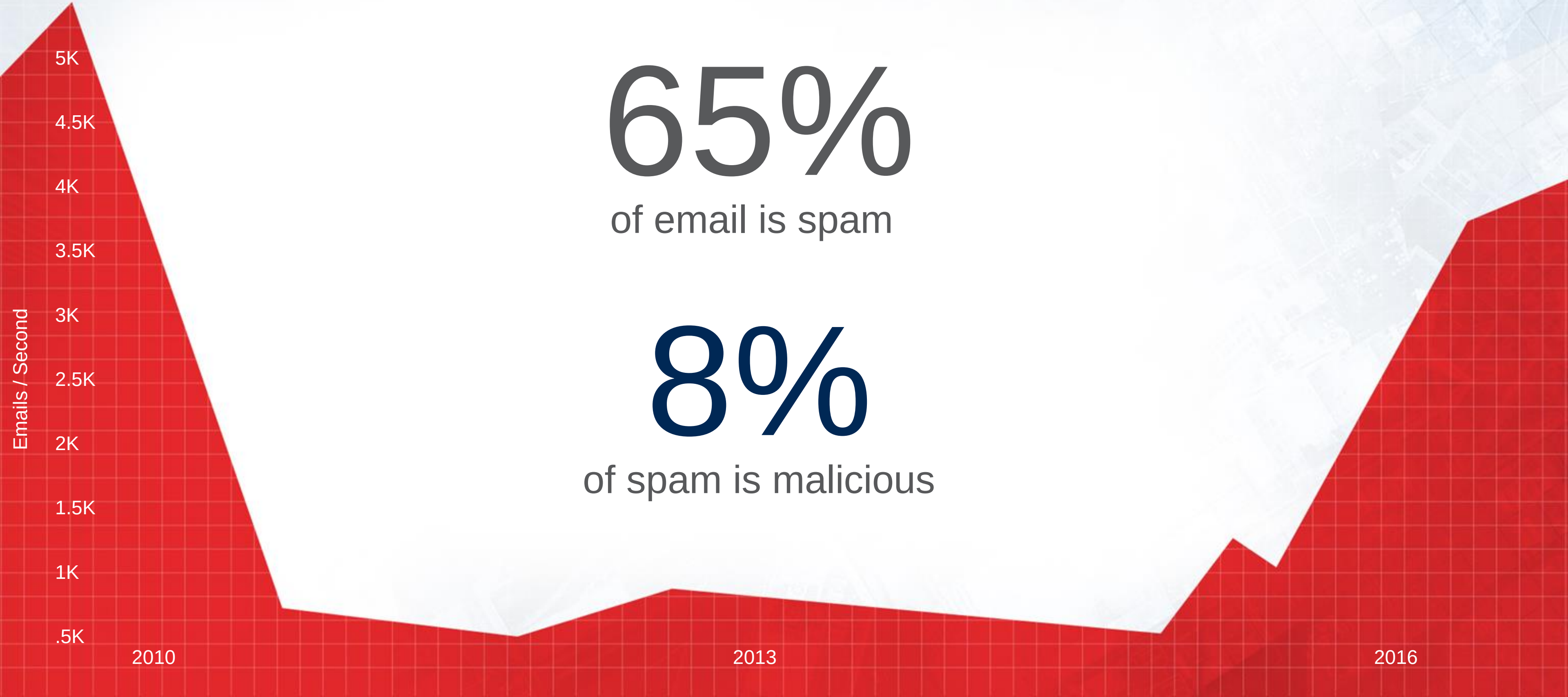
24K Browser Redirection

11K Facebook Hijacking

14K Android Trojans

Spam Comes Roaring Back

Email is Back in Vogue



65%

of email is spam

8%

of spam is malicious

Adware and Malvertising Shift Into High Gear

Malvertising

Using brokers (gates) to increase speed and agility

Switching quickly between servers without changing redirection

ShadowGate: a cost-effective campaign

Adware

75%

of organizations investigated had adware infections

Vulnerabilities on the Rise

Adversaries Find Space and Time on the Server Side.

Server
(from 2332 to 3142)
▲ 34%

Client
(from 2300 to 2106)
▼ 8%

Network
(from 501 to 396)
▼ 20%

Middleware Vulnerabilities

PDF
20
PDF

12
Image

10
Office

9
Compression

11
Other

Losses After an Attack Are Real for Organizations

Opportunity

- Productivity loss through downtime
- Political
- Reduced pace of innovation

Money

- Ransomware, $24M 2015 - $1bn 2016
- Average cost of breach $4m *(IBM/Ponemon)*
- Theft, each sensitive record $158 *(IBM/Ponemon)*
- Reduced price M & A
- Market manipulation
- Fine, ICO, GDPR

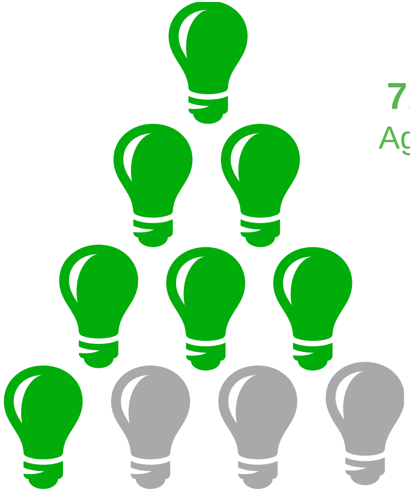
Customers

- Customer can move their business
- TalkTalk, 101,000

Lack of Cybersecurity Hinders Innovation in the Digital Era

Survey

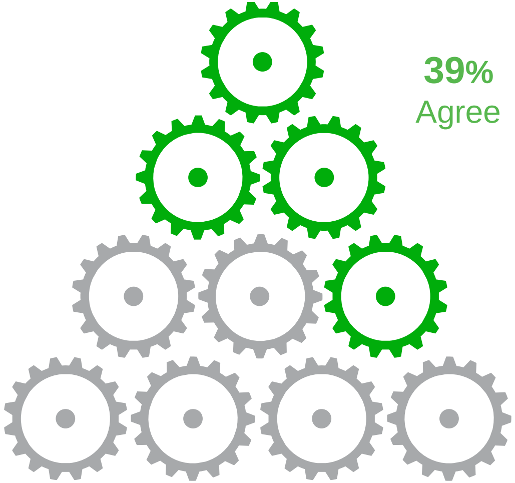
“Cybersecurity **risks and threats hinder innovation** in my organisation.”



71% Agree

Survey

“My organisation **halted a mission-critical initiative** due to cybersecurity fears.”



39% Agree

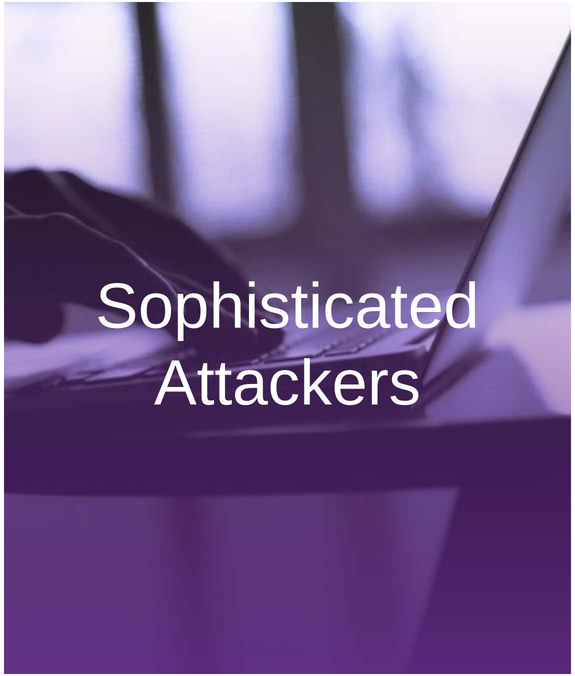
> “Innovations are moving forward, but probably at 70%-80% of what they otherwise could if there were better tools to deal with the dark cloud of cybersecurity threats.”
>
> Robert Simmons
> CFO

1014 respondents

Problem

Complexity: Are We Secure Yet?

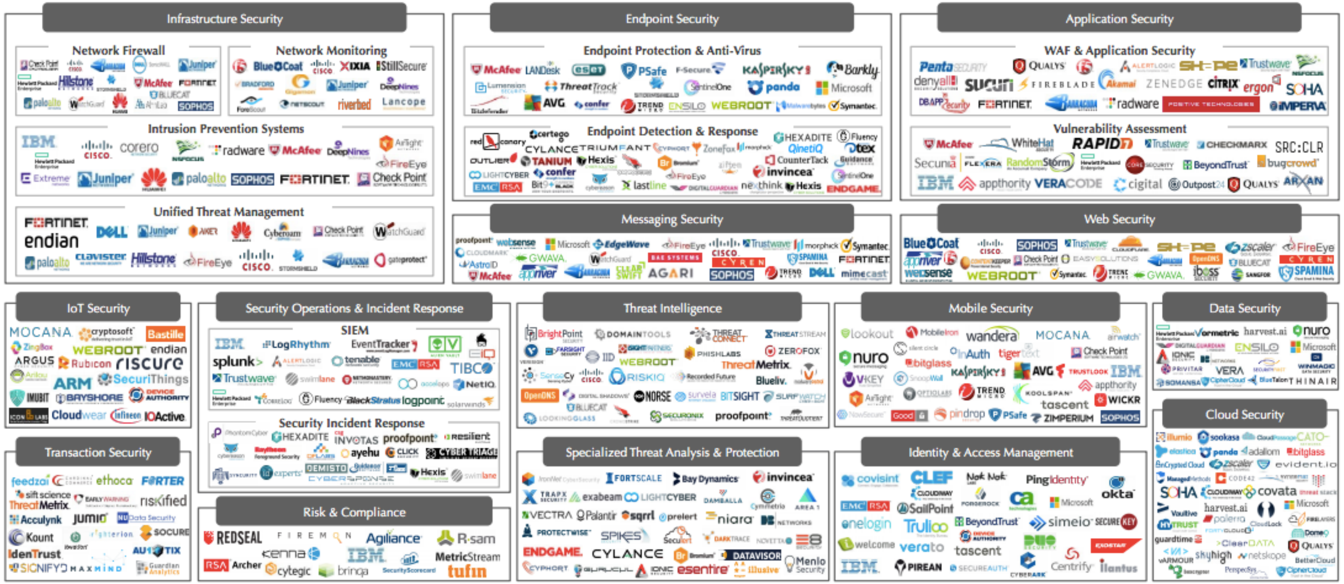
Frankenstructures



Sophisticated Attackers

Proliferating Point Products

The product centric approach


Infrastructure Security
Network Firewall
Network Monitoring
Intrusion Prevention Systems
Unified Threat Management
Endpoint Security
Endpoint Protection & Anti-Virus
Endpoint Detection & Response
Application Security
WAF & Application Security
Vulnerability Assessment
Messaging Security
Web Security
IoT Security
Security Operations & Incident Response
SIEM
Security Incident Response
Threat Intelligence
Mobile Security
Data Security
Cloud Security
Transaction Security
Risk & Compliance
Specialized Threat Analysis & Protection
Identity & Access Management

Source: Momentum Partners.

Biggest Obstacles to Advancing Security

Business Constraints

35%
Budget
(-4%)

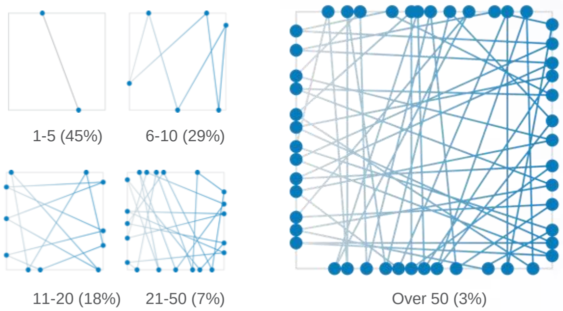
28%
Compatibility Issues
(-4%)

25%
Lack of Trained Personnel
(+3%)

25%
Certification Requirements
(+/-0%)

(Change from 2015)

Complexity

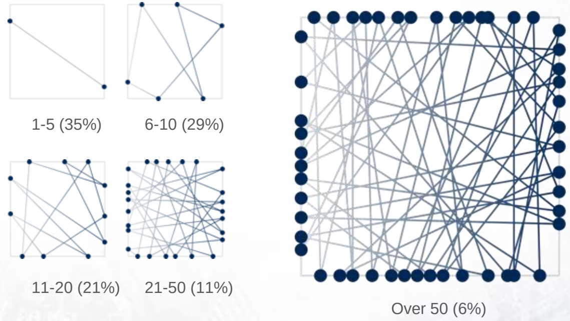


Vendor

55%

of organizations use **6 to >50 security vendors**

2016 (n=2,850)



Products

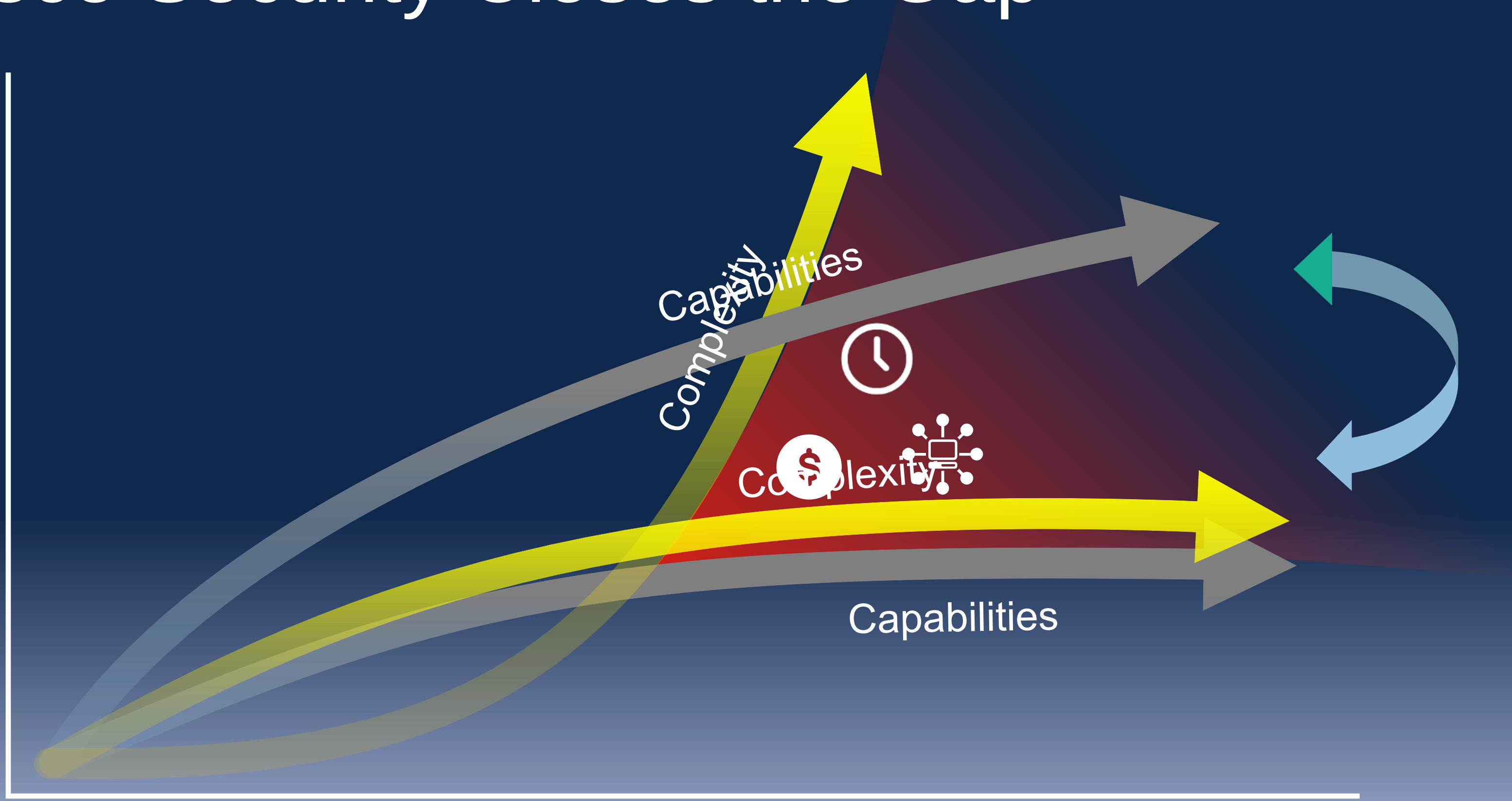
65%

of organizations use **6 to >50 security products**

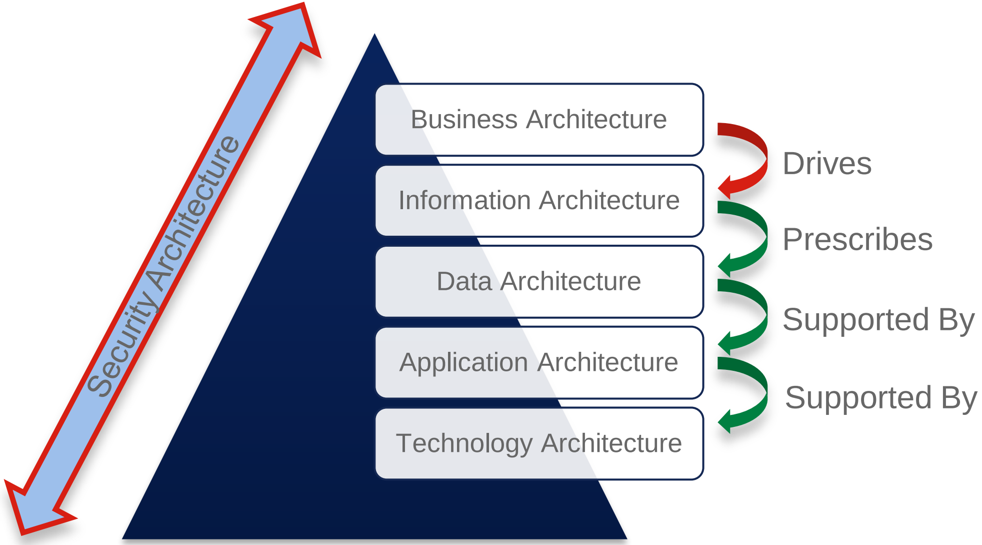
2016 (n=2,860)

The Security Effectiveness Gap

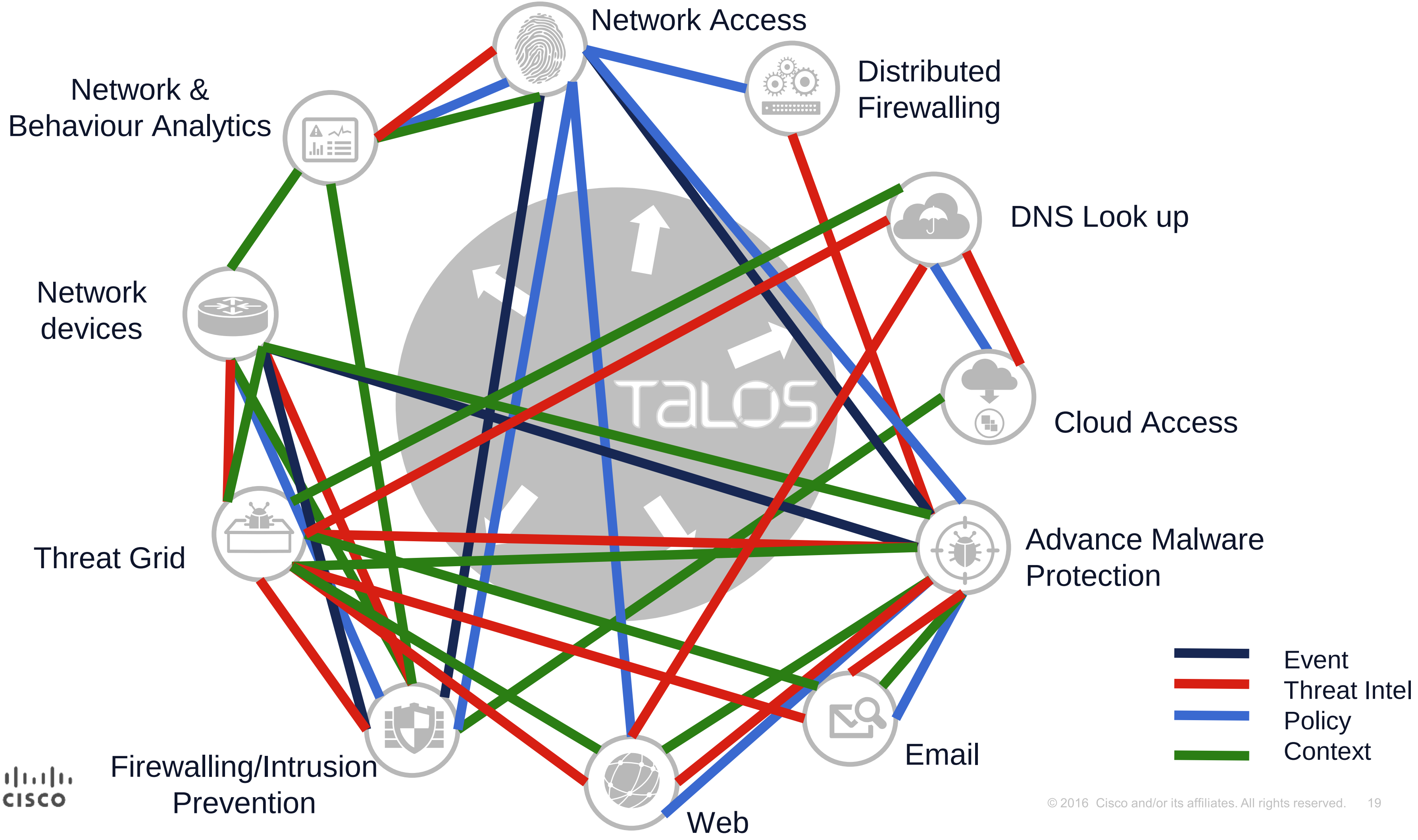
Cisco Security Closes the Gap



The Architectural Approach



- Integral Part of Enterprise Architecture
- Vital Element of IT Strategy that aligns to Business Goals
- Always Top Down
- Cuts Across horizontally
- An enabler for Business to meet its vision



Network Access

Distributed Firewalling

Network & Behaviour Analytics

DNS Look up

Network devices

Cloud Access

Threat Grid

Advance Malware Protection

Firewalling/Intrusion Prevention

Web

Email

Event

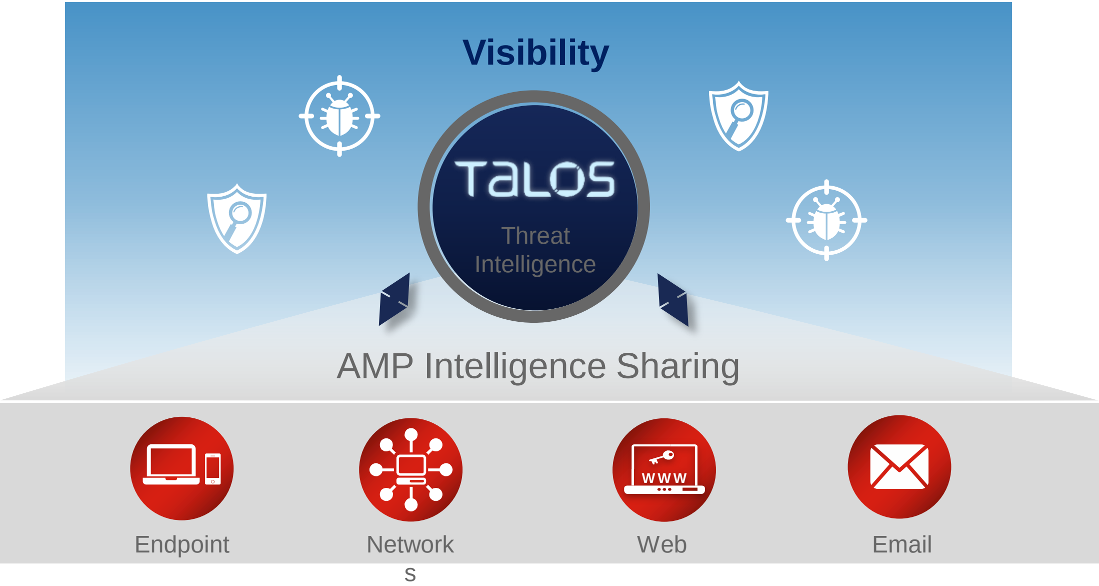
Threat Intel

Policy

Context

Advanced Malware Protection

AMP Everywhere: See Once, Protect Everywhere



Visibility

Talos

Threat Intelligence

AMP Intelligence Sharing

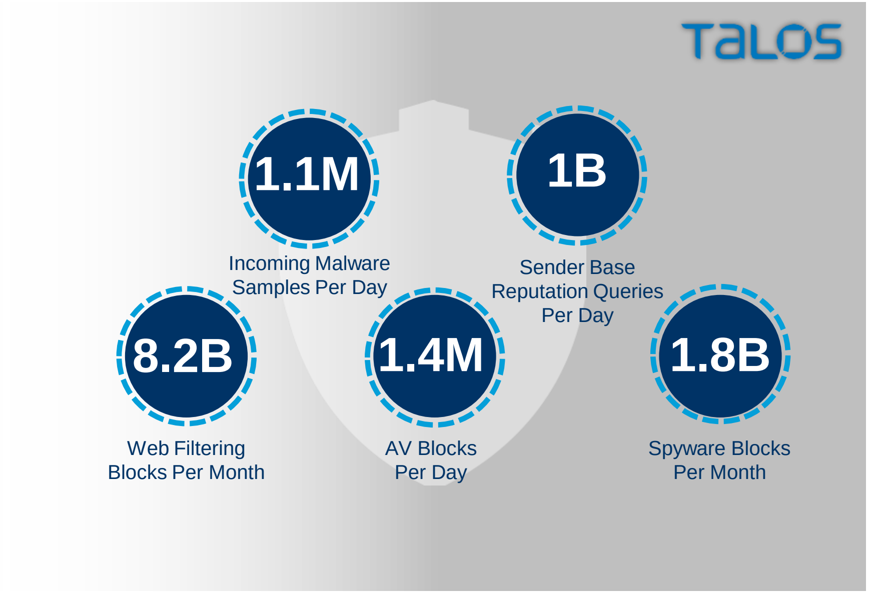
Talos provides the best threat intelligence capabilities

World-Class Threat Research

250
Threat Researchers

100TB
Threat Intelligence

19.7B
Threats Per Day



TALOS

1.1M
Incoming Malware Samples Per Day

1B
Sender Base Reputation Queries Per Day

8.2B
Web Filtering Blocks Per Month

1.4M
AV Blocks Per Day

1.8B
Spyware Blocks Per Month

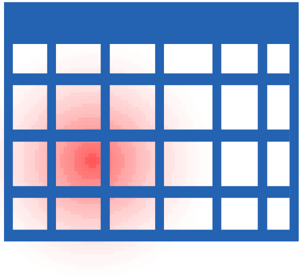
More Effective Against Sophisticated Attacks

Much Faster Than Most Organisations Discover Breaches

Industry

100

DAYS



vs.

Cisco

Less than

~~13~~ 6

hours

Source: Cisco Annual Security Report, 2016

For further information please contact:

Amy Lawrence: 020 88241309 - amlawren@cisco.com

or

Hanna Alderman: 020 88240669 - hasalter@cisco.com