
Security matters
‘There are only two types of organisations in the world……’
Terry Greer-King
Director, Cyber security, UK & Africa
March 2017

‘You could just wait……’

Problem

Complexity: Are We Secure Yet?

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

Not Operationalised

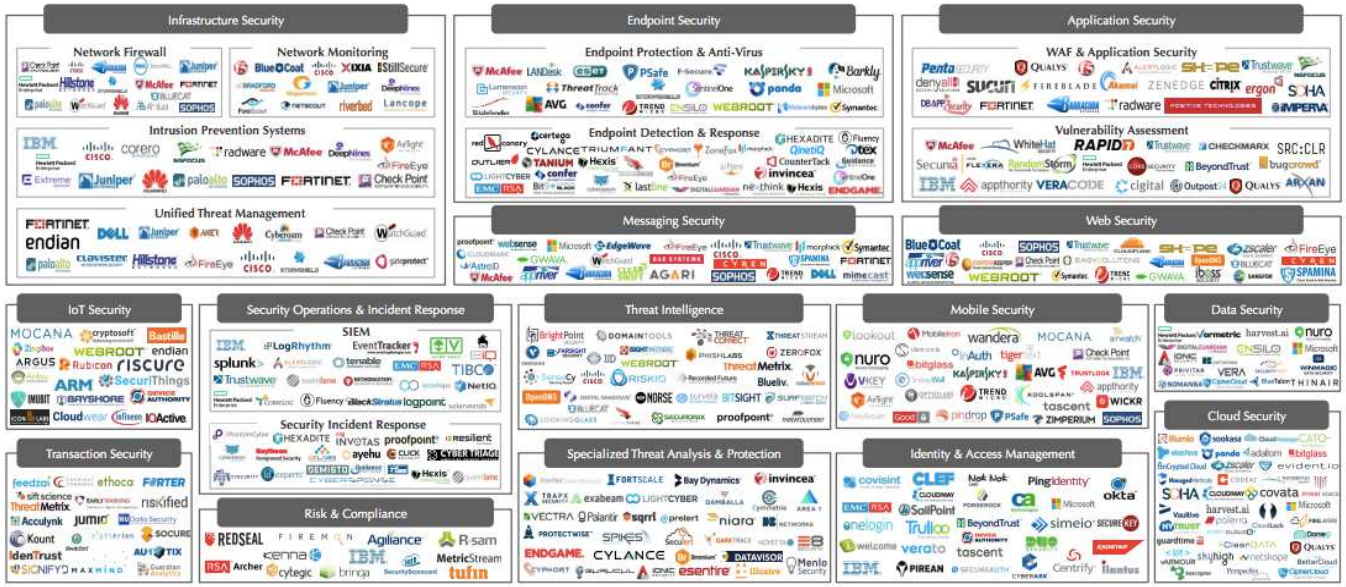
Security vs. Compliance

Security whack-a-mole

Technology Lead

Fragmented and siloed

The product centric approach



Source: Momentum Partners.

Biggest Obstacles to Advancing Security

Business Constraints

35%
Budget
(-4%)

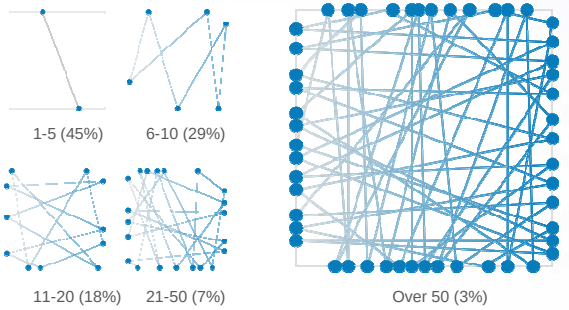
28%
Compatibility Issues
(-4%)

25%
Lack of Trained Personnel
(+3%)

25%
Certification Requirements
(+/-0%)

(Change from 2015)

Complexity

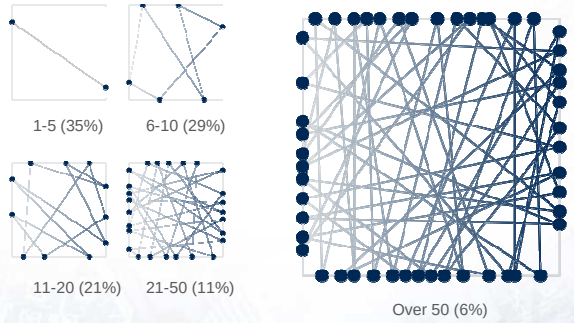


Vendor

55%

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

2016 (n=2,850)



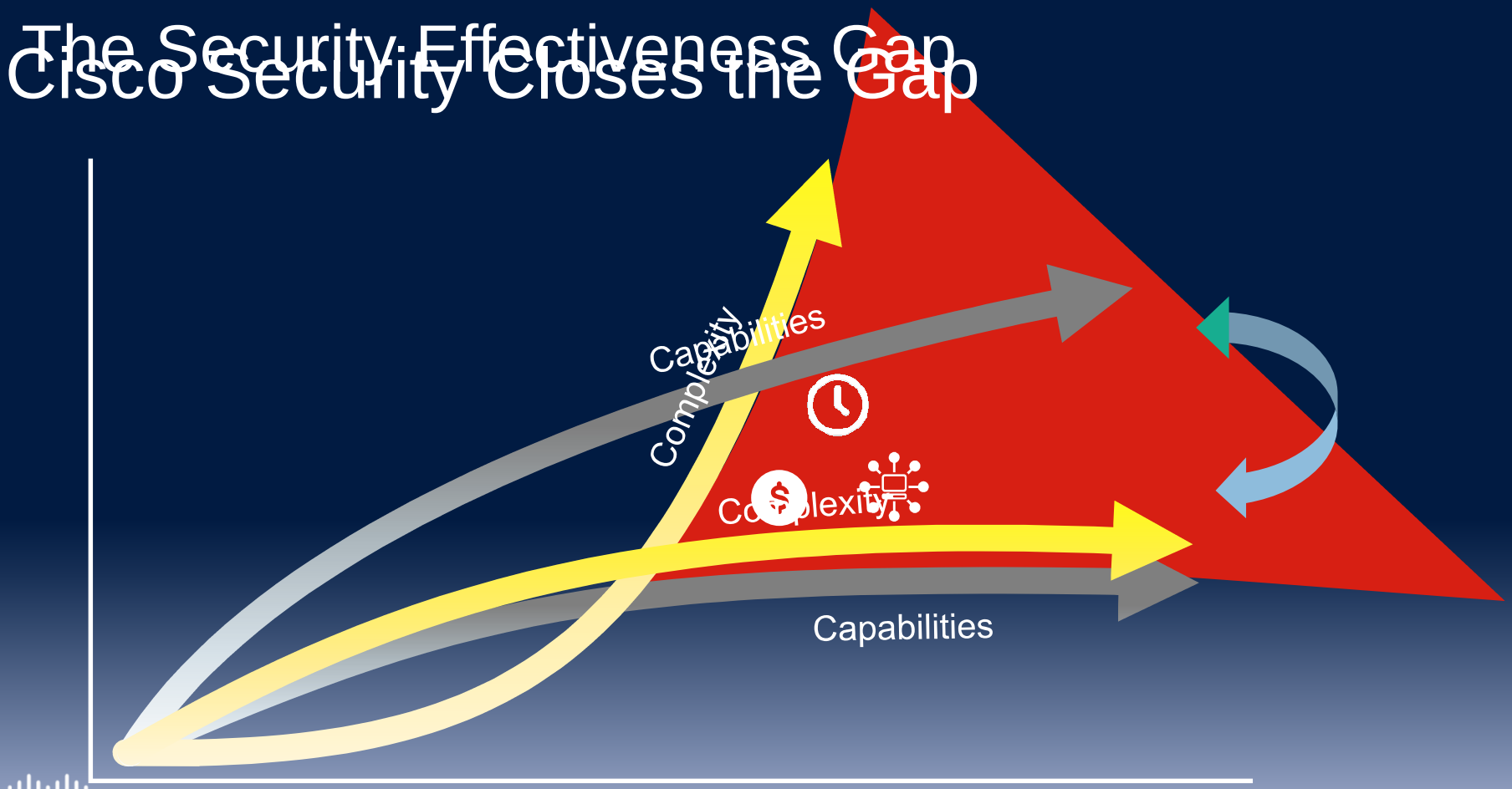
Products

65%

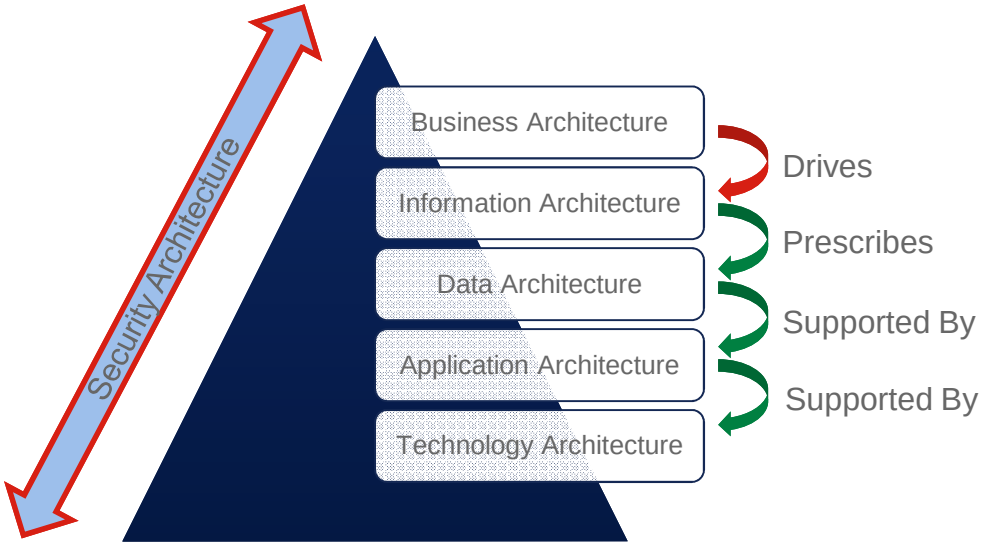
of organizations use **6 to >50 security products**

2016 (n=2,860)

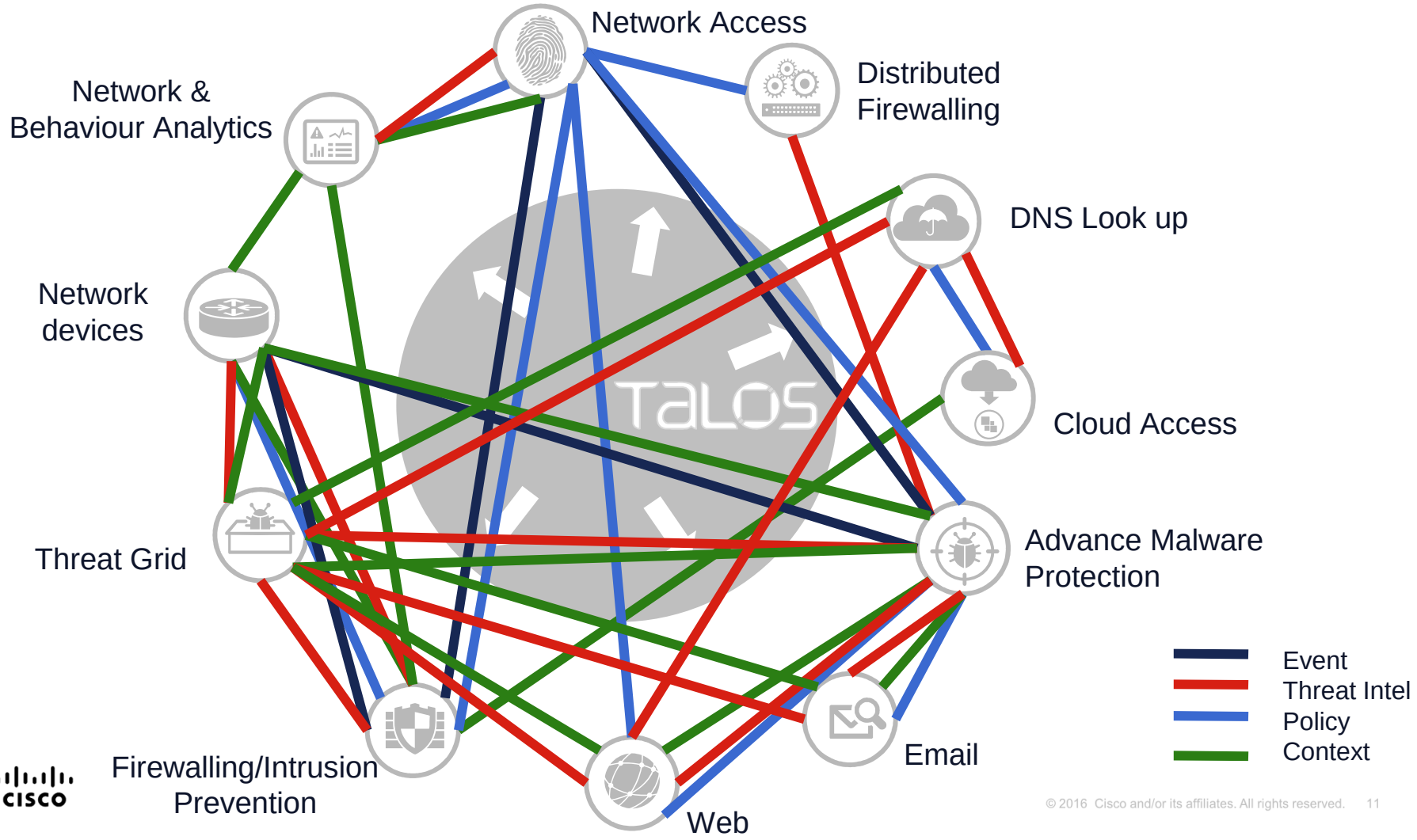
The Security Effectiveness Gap
Cisco Security Closes the Gap



The Architectural Approach

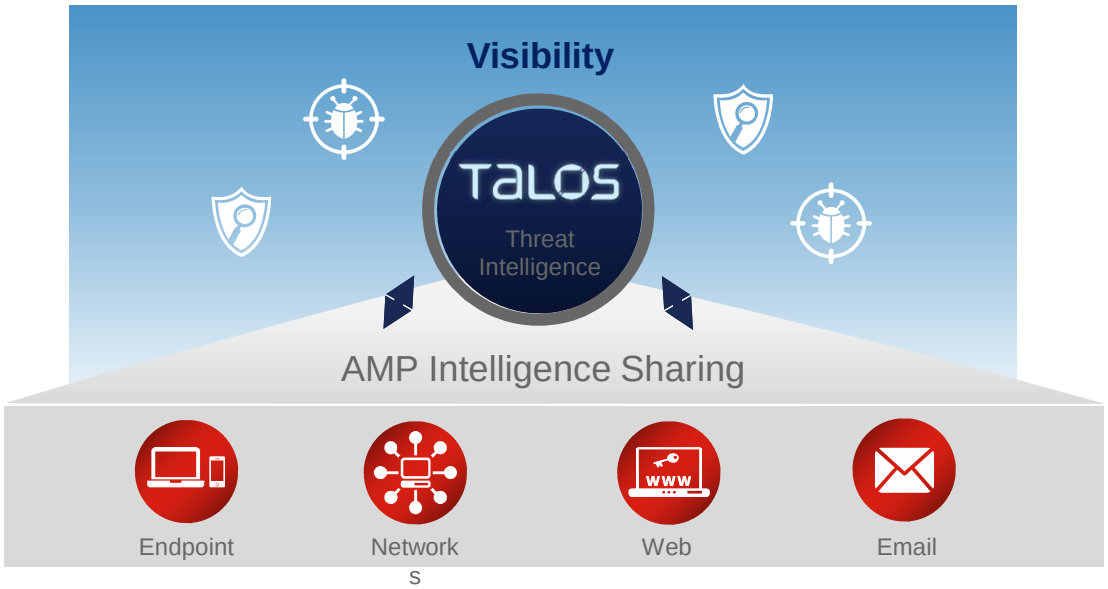


- Integral Part of Enterprise Architecture
- Vital Element of IT Strategy that aligns to Business Goals
- Always Top Down
- Cuts Across horizontally
- An enabler for Business to meet its vision



Advanced Malware Protection

AMP Everywhere: See Once, Protect Everywhere



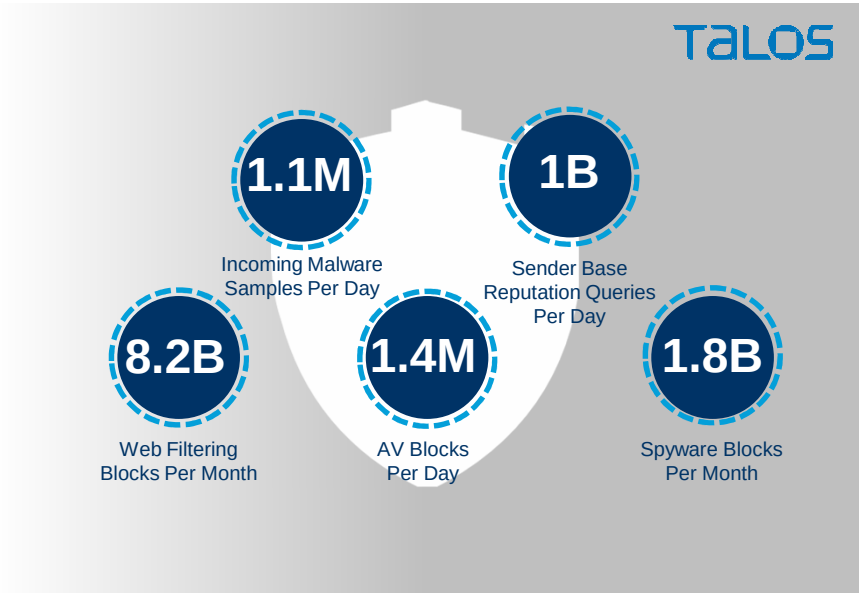
Talos provides the best threat intelligence capabilities

World-Class Threat Research

250
Threat Researchers

100TB
Threat Intelligence

19.7B
Threats Per Day



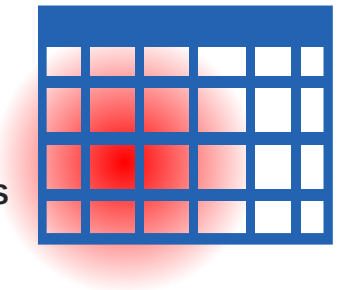
More Effective Against Sophisticated Attacks

Much Faster Than Most Organisations Discover Breaches

Industry

100

DAYS



VS.

Cisco

Less than

~~13~~ **6**

hours

Source: Cisco Annual Security Report, 2016


CISCO
TOMORROW starts here.