McAfee™
Together is power.

Measuring effectiveness in Information Security Controls

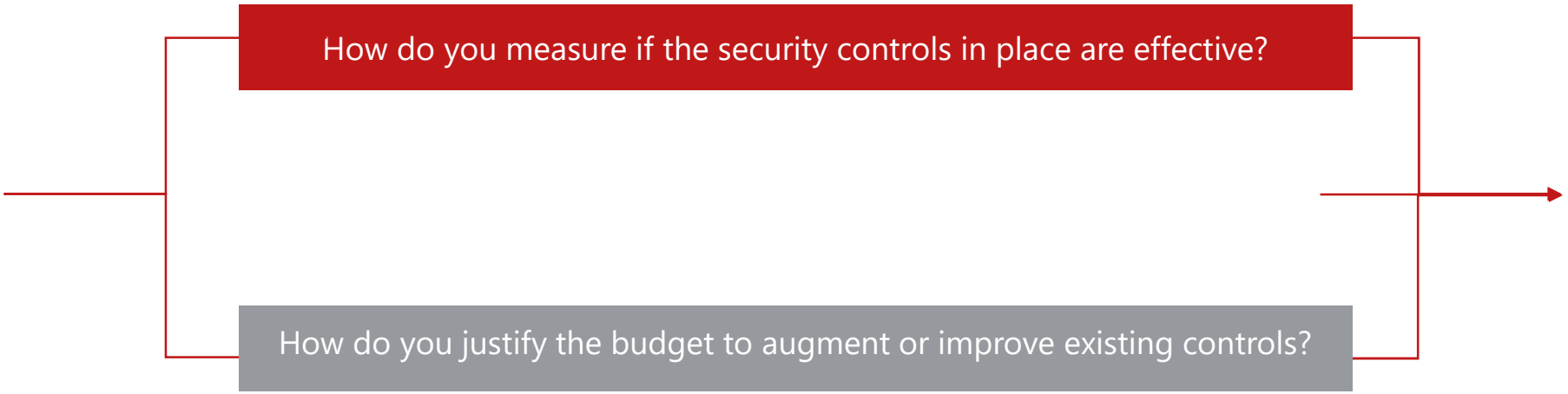
Which horse to back?...Architectural blueprint versus best in breed point solutions

Scott Manson | Managing Director

Our Challenge

As part of our Cyber security pledge we all seek to control the exposure to information security risks…

How to address this challenge?



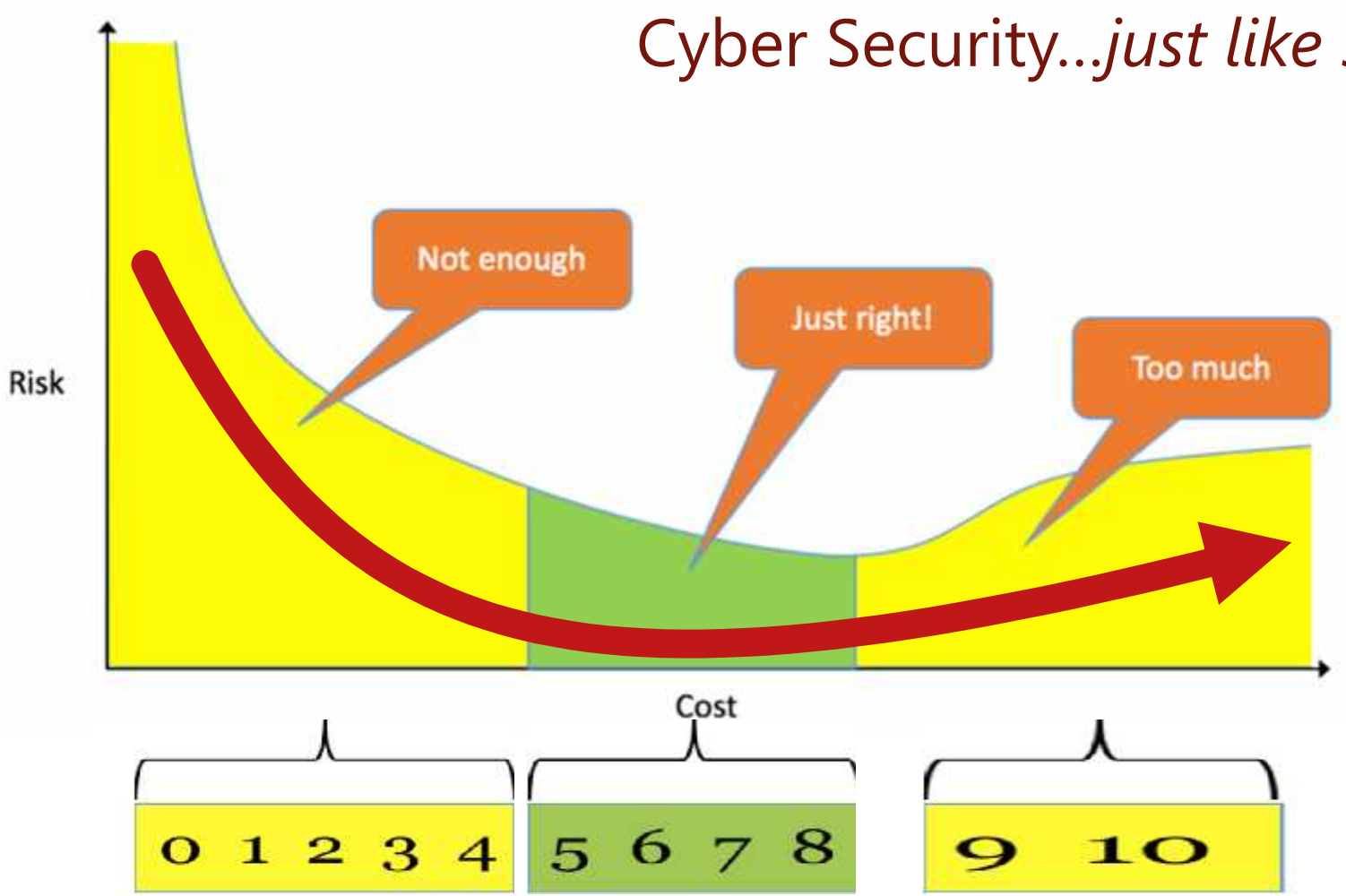
Challenge	How
How do I know my controls are effective?	Prioritization and Metrics
If they aren't working well enough, how far off are they?	Defining 'Good' and common metric
If my controls are too restrictive, how much should I dial them back?	Setting thresholds and tolerance levels
If I want to make improvements, how much budget will I need?	Benchmarking reality

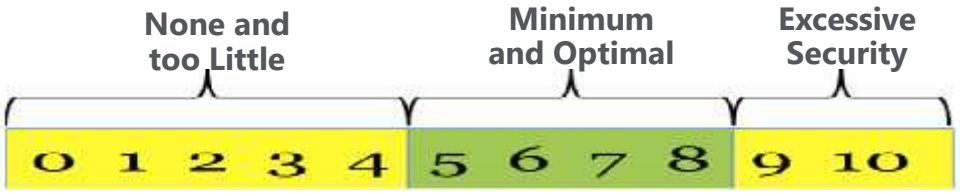
Effectiveness index $= \Sigma((ei \bullet ri))$

Information Security controls – a continuous loop…

Assessing Information Security Risks

Cyber Security…*just like salt*





Score Card - Defining 'good'

The desired deliverable rarely or does not happen at the right time

0

The desired deliverable happens when needed, but unreliably, no predictability

3

The desired deliverable happens consistently with some minor flaws occasionally.

5

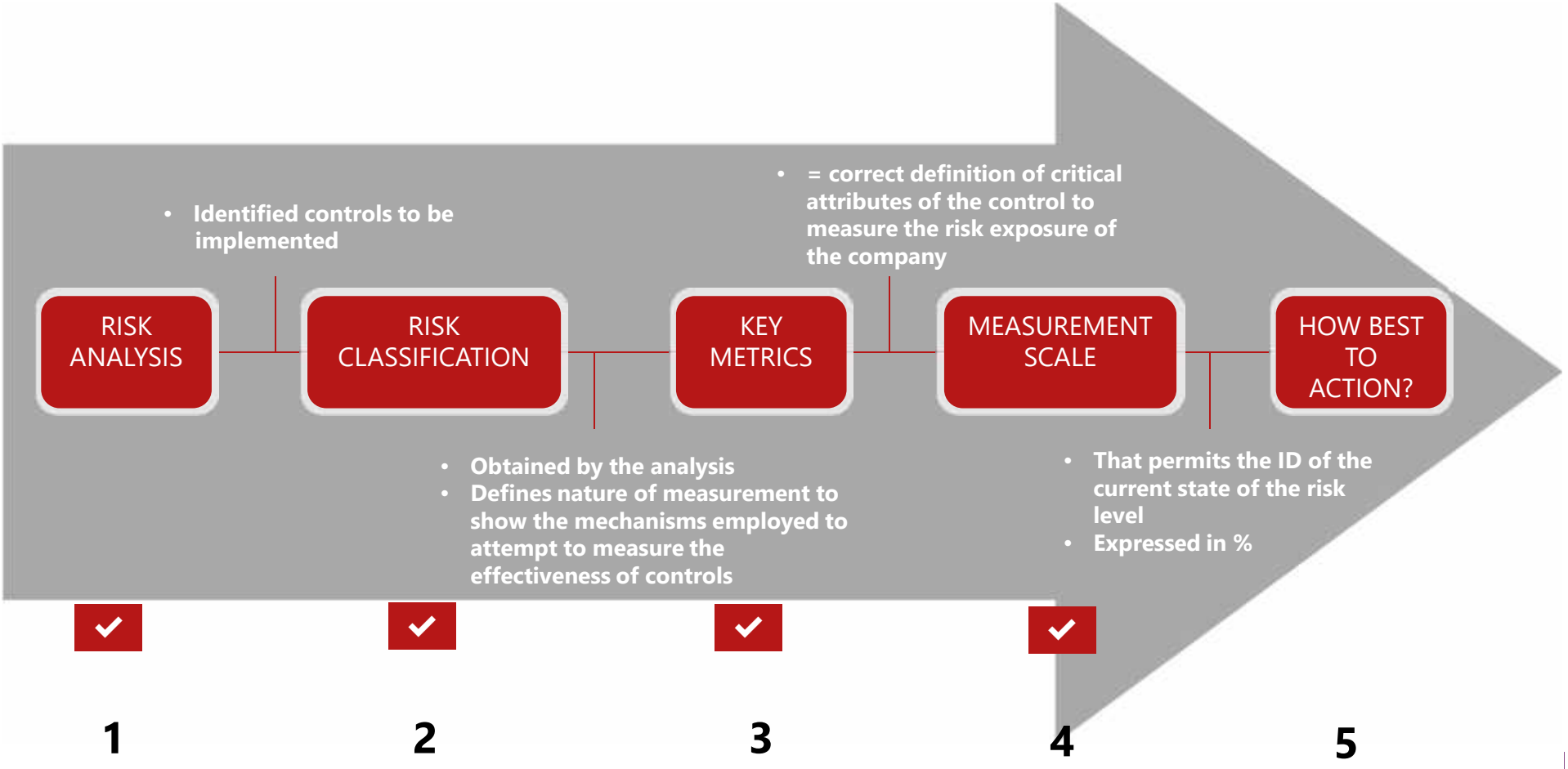
The desired deliverable happens consistently with great effectiveness and with high quality

8

The desired deliverable happens at excessive cost to the business and exceeds the requirements delivering no tangible benefit to the business

10

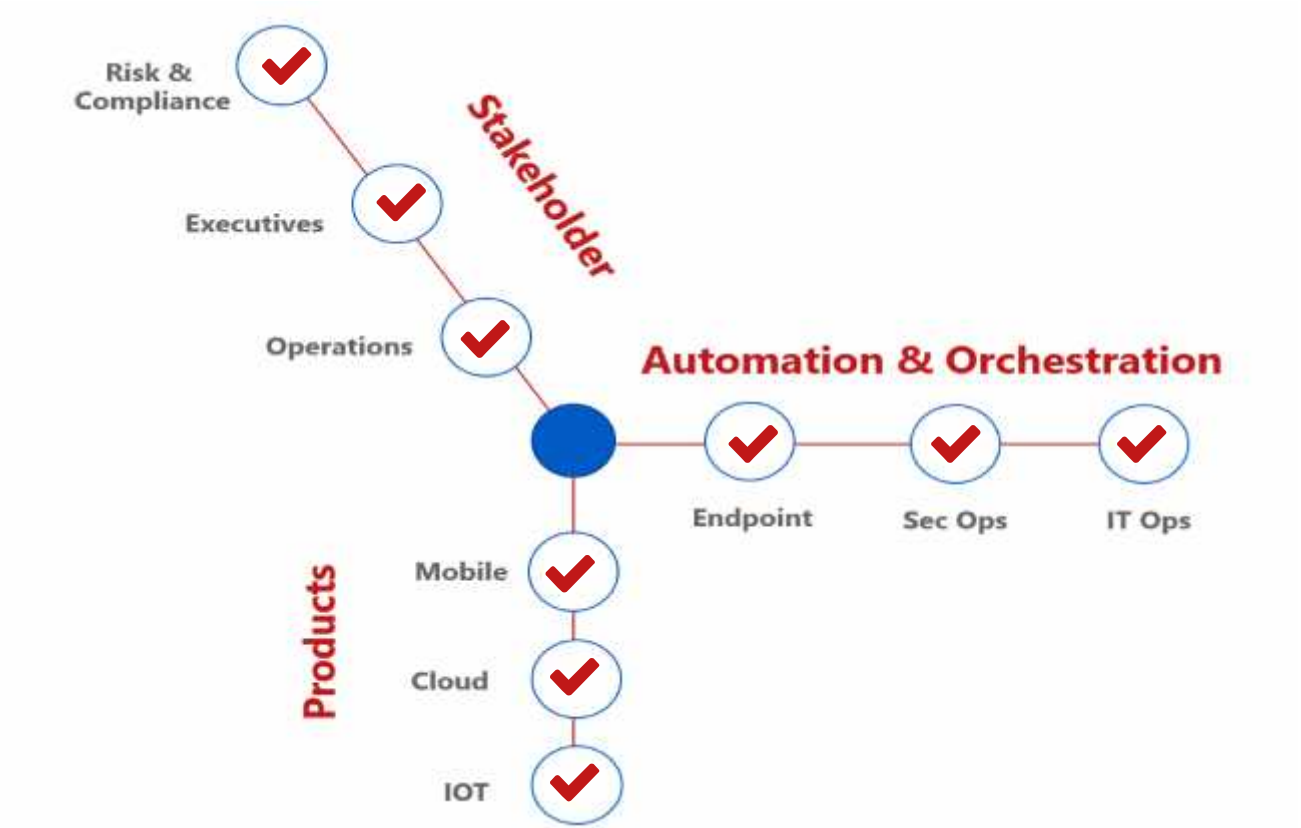
Step by step

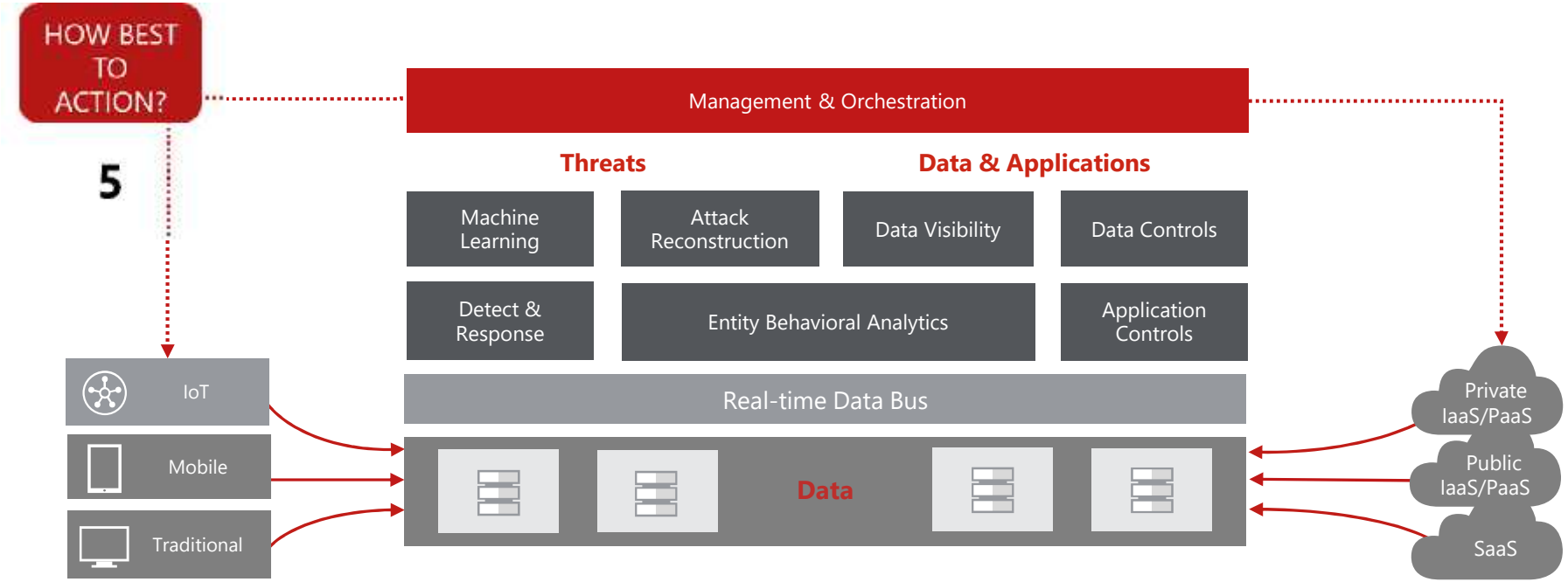

RISK ANALYSIS
RISK CLASSIFICATION
KEY METRICS
MEASUREMENT SCALE
HOW BEST TO ACTION?
• Identified controls to be implemented
• Obtained by the analysis
• Defines nature of measurement to show the mechanisms employed to attempt to measure the effectiveness of controls
• = correct definition of critical attributes of the control to measure the risk exposure of the company
• That permits the ID of the current state of the risk level
• Expressed in %
1
2
3
4
5

HOW BEST TO ACTION?

5

Which horse to back?...Architectural blueprint versus best in breed point solutions





Device

- Visibility and contextual control
- Data Protection
- Threat Detection and Response

Security Operations

- System level Data Protection
- System level Threat Detection and Response
- Automation & Orchestration (Proactive / Reactive)

Cloud

- Visibility and contextual control in hybrid and multi-cloud environment
- Data and Workload Protection
- Threat Detection and Response

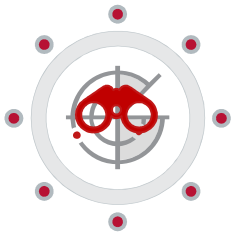
So in summary – Architectural blueprint is the answer, but one vendor does not fit all sizes…

Discover, inventory and classify personal data

- McAfee DLP (Network and Endpoint)
- McAfee Vulnerability Manager for Databases
- McAfee Skyhigh Security Cloud

Protect data wherever it resides

- McAfee DLP, McAfee Complete Data Protection Suites
- McAfee Skyhigh Security Cloud, McAfee Database Activity Monitoring
- McAfee Enterprise Security Manager, McAfee Behavioral Analytics



Increase speed of breach detection and response

- McAfee Enterprise Security Manager/ McAfee Behavior Analytics
- McAfee Vulnerability Manager for Databases
- McAfee Active Response