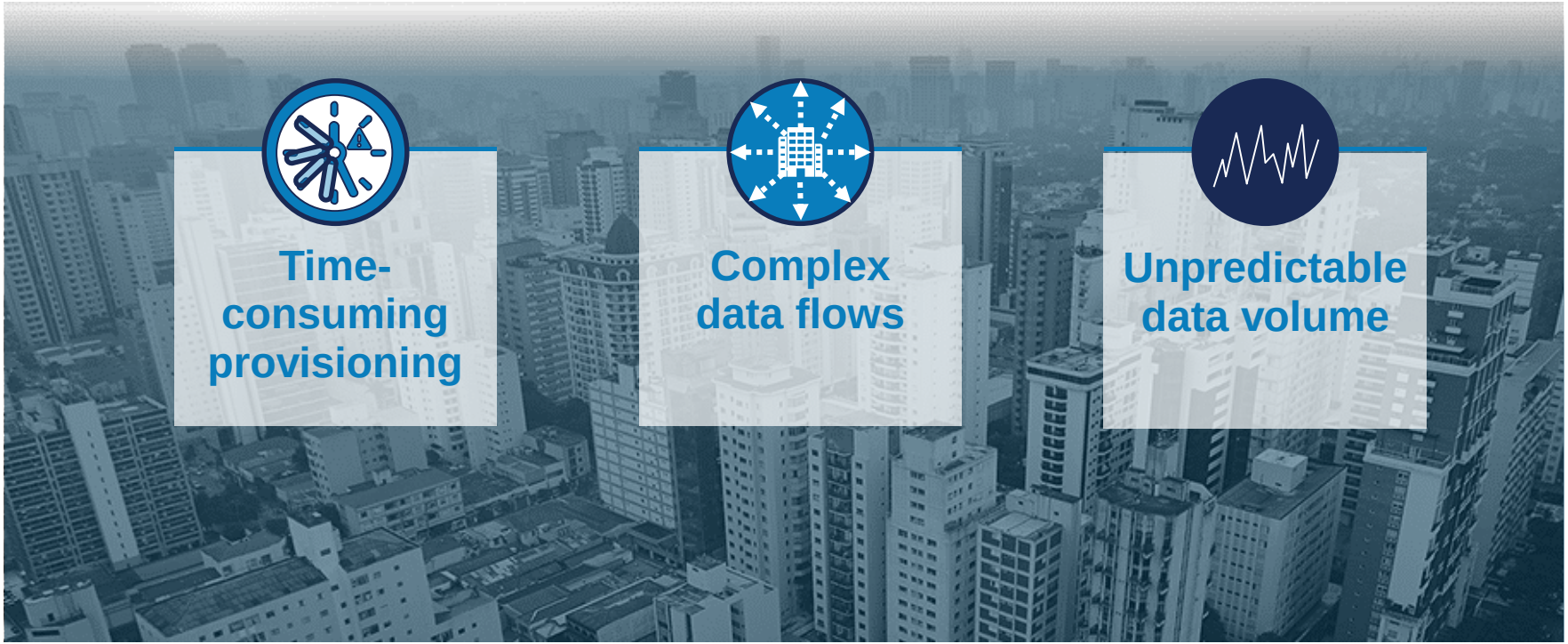
Securing the Data Center

- Intelligent Security Solutions

Demetris Booth
Head of Security Products And Solutions Marketing
29 March 2016

Data Center is a Challenging Environment



Sacrifice Security to Gain Performance

Malware Threats To Data Centers Are Growing in…

Sophistication

- Organizations often have 40 to 60+ disparate security solutions
- But they don't – and often can't – work together

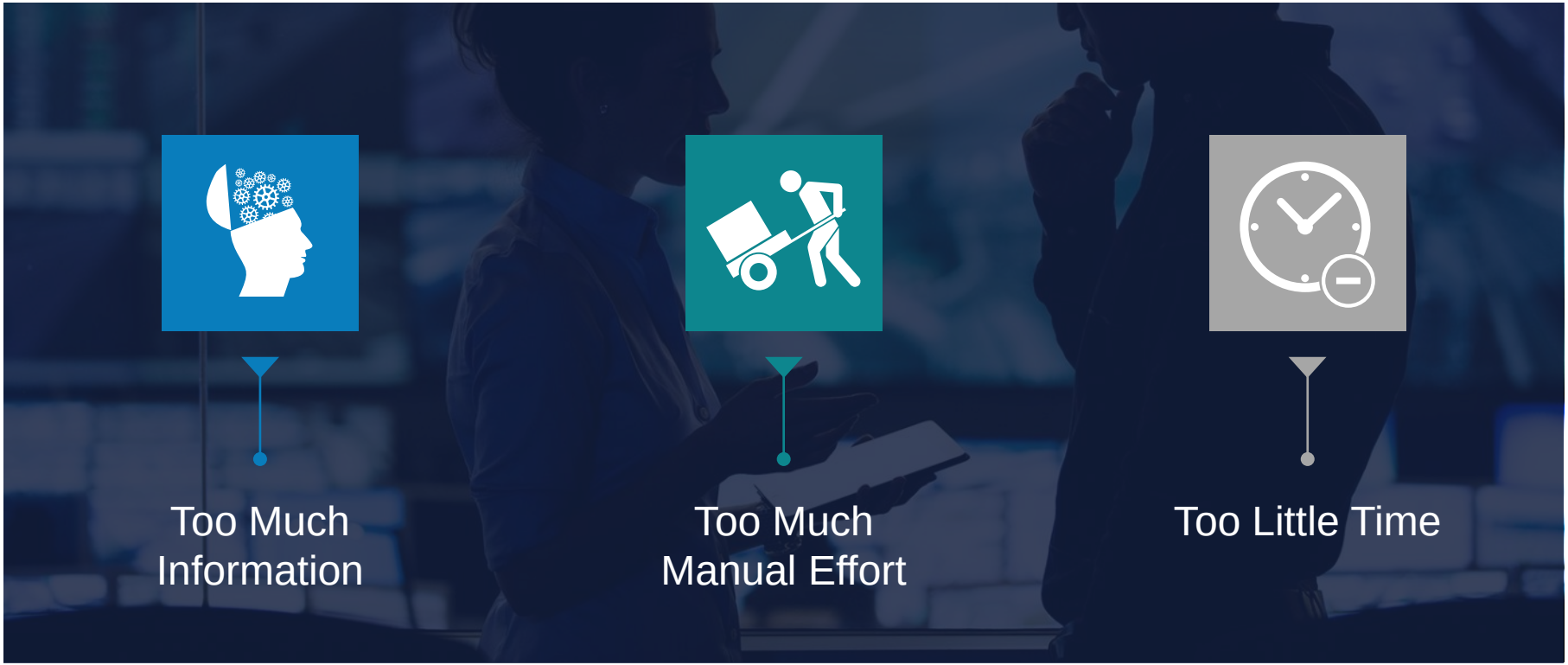
Stealth

- 17,000 alerts received on average per week
- 19% prove reliable
- Security teams have time to investigate just 4% of warnings[1]

Speed

- The longer threats stay undetected, the greater for damage
- But current industry average detection time: 200 days
- Average cost per data breach: $3.8 million[2]

Malware Preys on Dis-Integrated Security Infrastructure



Advanced Malware Requires Advanced Threat Detection and Response

Malware defense should be:

- Automated
- Advanced
- Scalable
- Accelerated

Data Centers Require Specialized Security

Standard edge security		Data center security
Sees symmetric traffic only		Requires asymmetric traffic management
Scales statically for predictable data volume, limited by edge data connection		Must scale dynamically to secure high volume data bursts
Monitors ingress and egress traffic		Needs to secure intra-data-center traffic
Deployed typically as a physical appliance		Requires both a physical and virtual solution
Deploys in days or weeks		Must deploy in hours or minutes

What If You Could…?

- Improve Threat Visibility and Detection Across the Network
- Speed Time to Containment
- Lower Operational Overhead and Costs

….And Automate Protection Across The Full Attack Continuum

Continuous Analysis and Retrospective Security

Advanced Detection and Remediation Capabilities

Monitor

- Understand your network and data center normal
- Gain real-time situational awareness of all traffic

Detect

- Leverage Network Behavior Anomaly detection & analytics
- Detect behaviors linked to APTs, insider threats, DDoS, and malware

Analyze

- Collect & Analyze holistic network audit trails
- Achieve faster root cause analysis to conduct thorough forensic investigations

Respond

- Accelerate network troubleshooting & threat mitigation
- Respond quickly to threats by taking action to quarantine through Cisco ISE

Protect Automatically with Rapid Threat Containment

Cisco FirePOWER Management Center (FMC) and Cisco Identity Service Engine (ISE)

Benefits

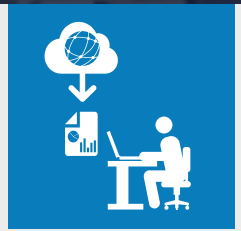
Detect Threats Early
FMC scans activity and publishes events to ISE

Automate Endpoint Containment
ISE alerts the network of suspicious activity according to policy

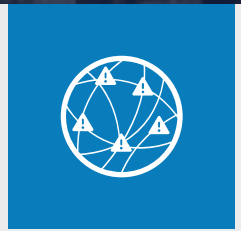
Integrate Best-of-Breed Security
Growing ecosystem of threat defense partners integrate with ISE

Rapid Threat Containment in Action

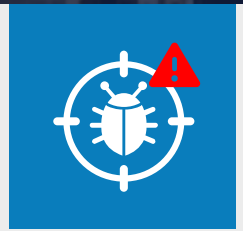
Automatically Defend Against Threats with FMC and ISE



Corporate user downloads file, not knowing it's actually malicious

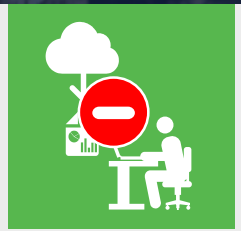


Cisco security sensors scan the user activity and downloaded file. FMC aggregates and correlates sensor data



FMC detects flagrantly suspicious file and alerts ISE. ISE then changes the user's/device's access policy to **suspicious**

Based on the new policy, network enforcers automatically restrict access



Device is quarantined for remediation or mitigation—access is denied per security policy

Taking A Deeper Look….

Cisco Rapid Threat Containment Solution

Advanced Threat Sensors

- Cisco ASA with Firepower Services
- FirePOWER NGIPS Appliances
- Cisco AMP for Networks
- Firepower on Cisco ISR
- Stealthwatch Network Analysis

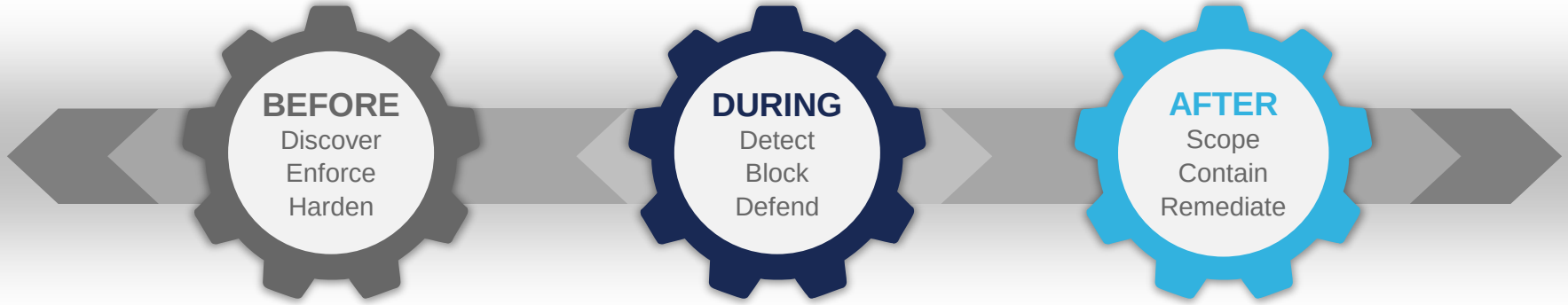
Threat Visibility

- Cisco FirePOWER Management Center
- Automated Contextual Analysis and Threat Qualification
- Continuous Threat Intelligence Updates to Threat Sensors

Automated Enforcement

- Cisco POWER and Cisco ISE Automate Containment
- Policy Enforcement from Cisco TrustSec, Downloadable ACL, or VLAN

Cisco RTC protects across the full attack continuum



NGFW

ISE & TrustSec

AnyConnect

NGISR

NGIPS

Cloud Access Security

Advanced Malware Protection

ISE & TrustSec

Talos

Differentiated Threat Defense

Advanced, Automated Malware Detection

Contextual Visibility to Understand and Contain Threats Faster

Continually Updated Threat Intelligence

Pervasive Network Enforcement

Your Cisco Network as Security Sensor and Enforcer

Rapid Threat Containment Protects The Data Centre With….

Learn More

- Cisco Rapid Threat Containment Product Page: http://www.cisco.com/go/rtc
- Cisco Rapid Threat Containment At-A-Glance: http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-735770.pdf
- Datasheet: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/rapid-threat-containment/datasheet-c78-736242.html
- Solution Overview: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/rapid-threat-containment/solution-overview-c22-736229.html

Thank You For Your Time


CISCO