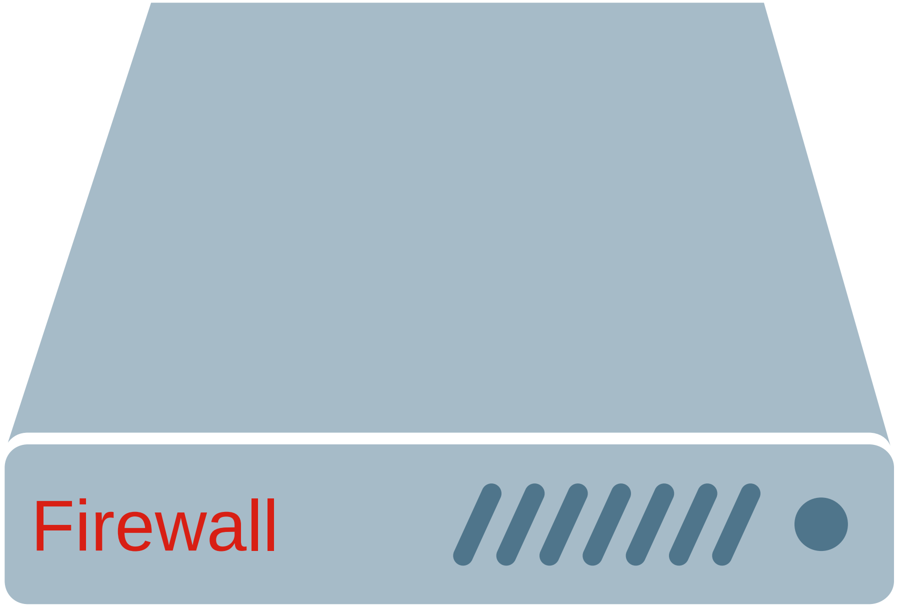
Why Cisco? Security Product Integration

Story Tweedie-Yates
Head of Security Product Marketing, EMEAR

March 2017

Would you rather. . .

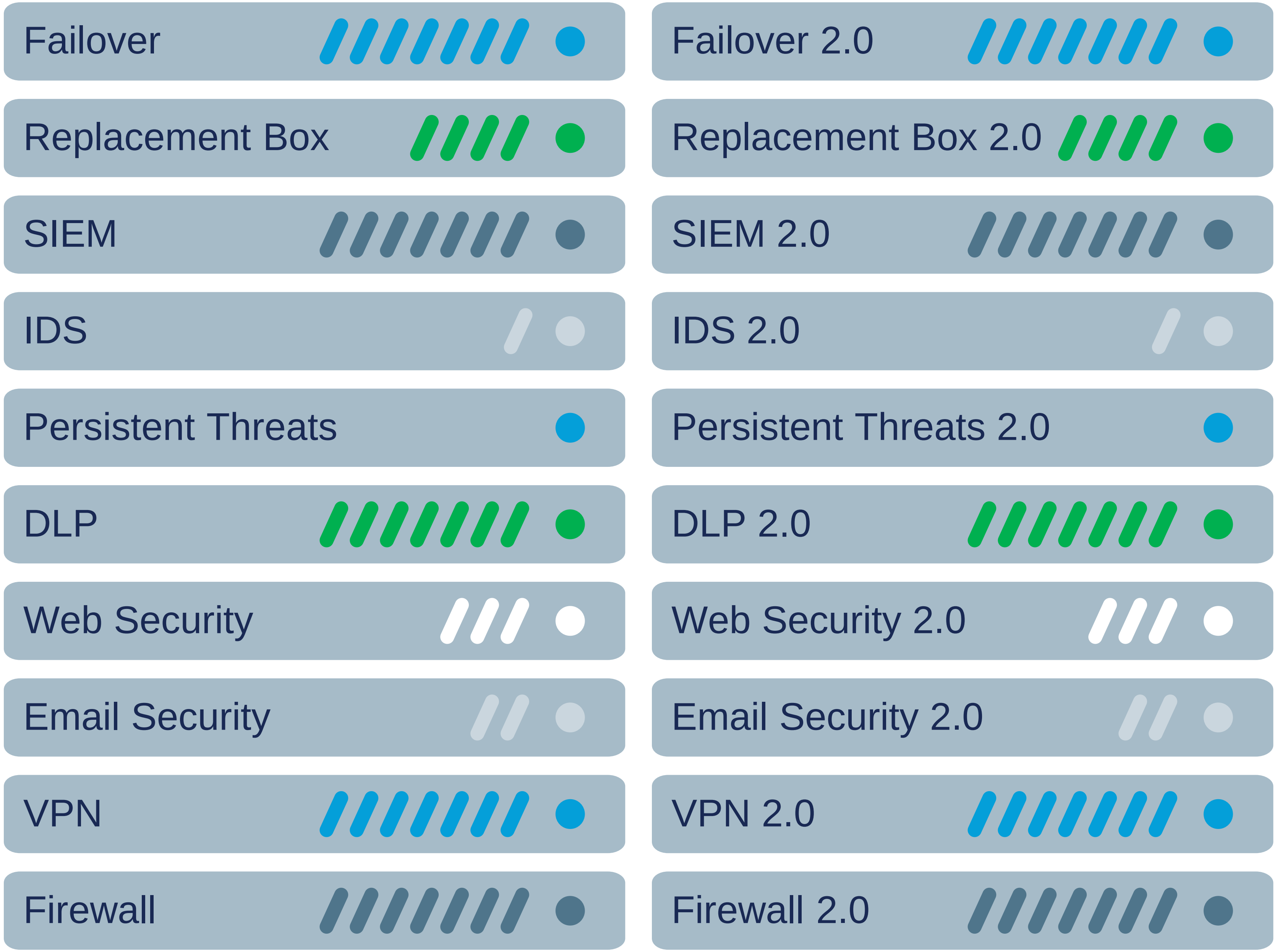


Last 20 years of security:

Got a problem?

Buy a Box

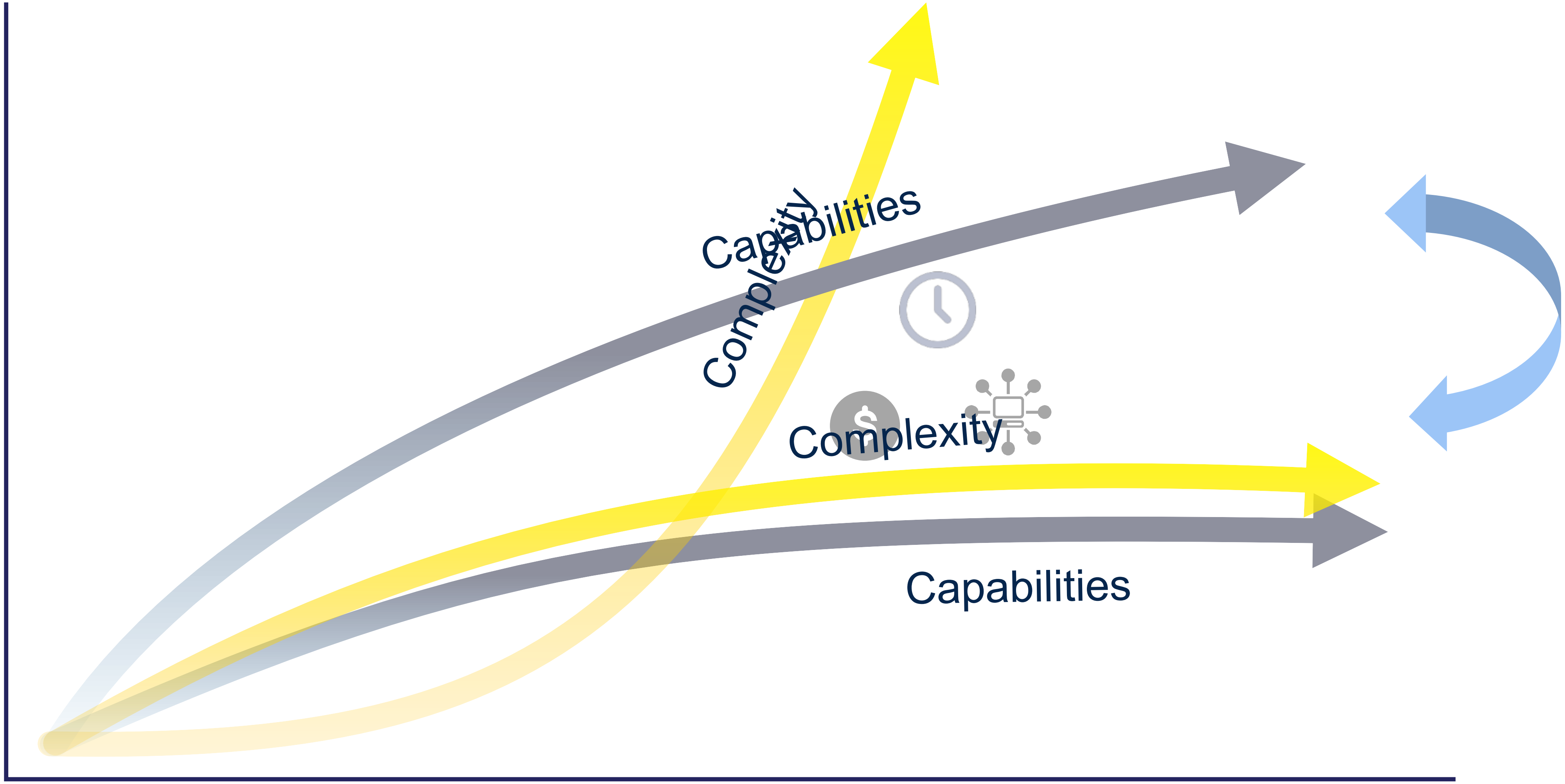
The Existing security stack…



Failover	Failover 2.0
Replacement Box	Replacement Box 2.0
SIEM	SIEM 2.0
IDS	IDS 2.0
Persistent Threats	Persistent Threats 2.0
DLP	DLP 2.0
Web Security	Web Security 2.0
Email Security	Email Security 2.0
VPN	VPN 2.0
Firewall	Firewall 2.0

The Security Effectiveness Gap

Cisco Security Closes the Gap



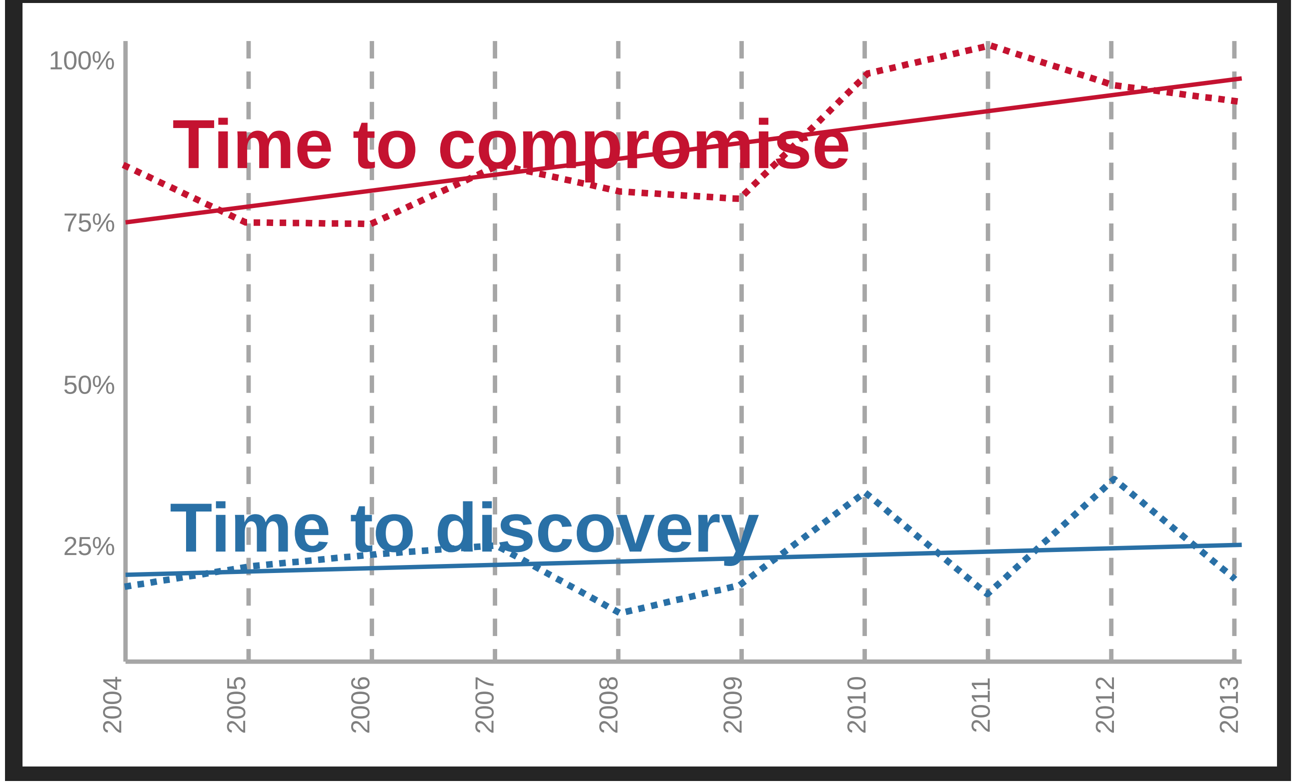
Complexity takes time. . .

Time to Detection

100

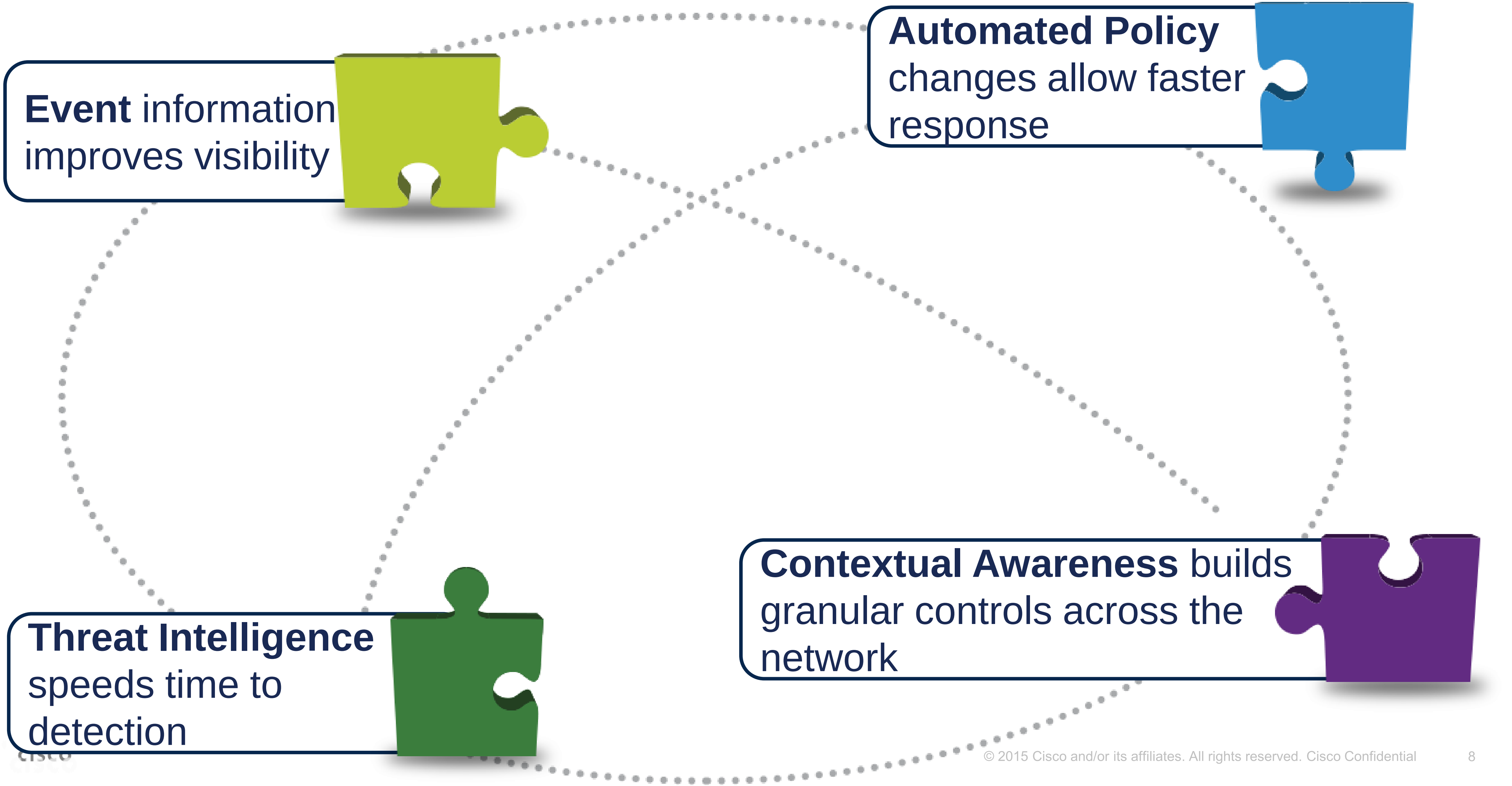
Industry Days

Percent of breaches where time to compromise (orange)/ time to discovery (blue) was days or less



Security Product Integration

What types of data do our product share?



Event information improves visibility

Automated Policy changes allow faster response

Threat Intelligence speeds time to detection

Contextual Awareness builds granular controls across the network

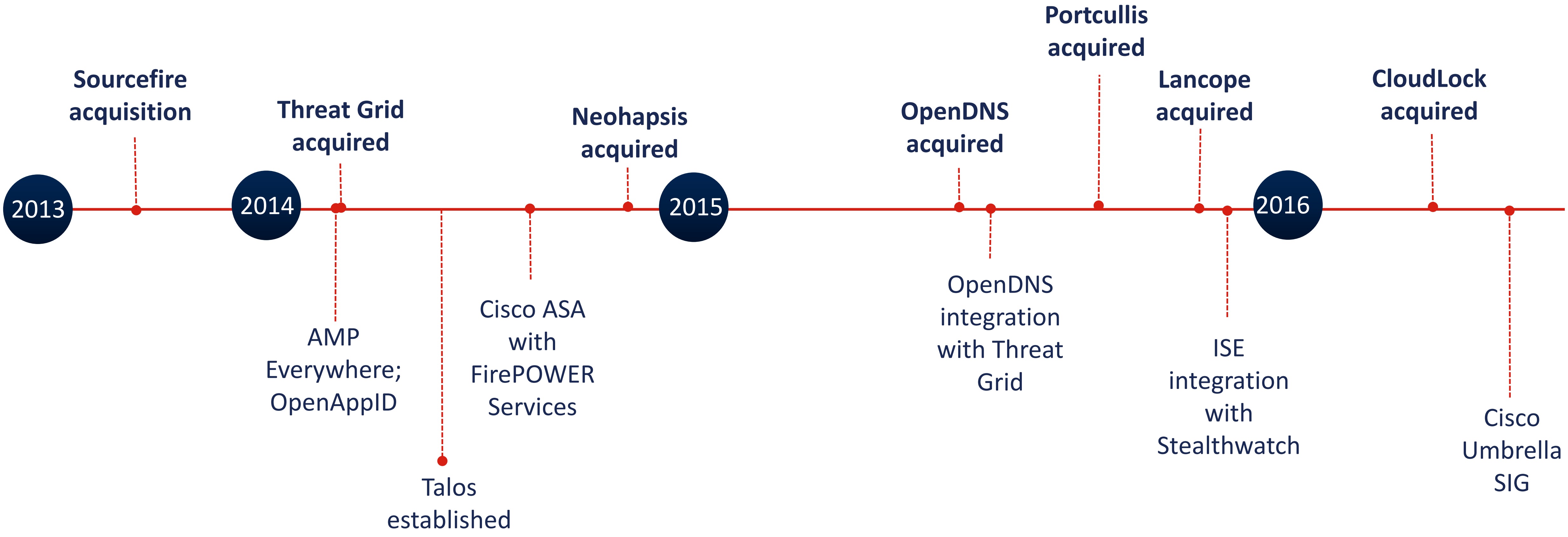
Lower TTD

Respond quickly

Simplify workflow

Do more with less

Key Milestones for Cisco Security



2013

Sourcefire acquisition

2014

Threat Grid acquired

AMP Everywhere; OpenAppID

Talos established

Cisco ASA with FirePOWER Services

Neohapsis acquired

2015

OpenDNS acquired

OpenDNS integration with Threat Grid

Portcullis acquired

Lancope acquired

ISE integration with Stealthwatch

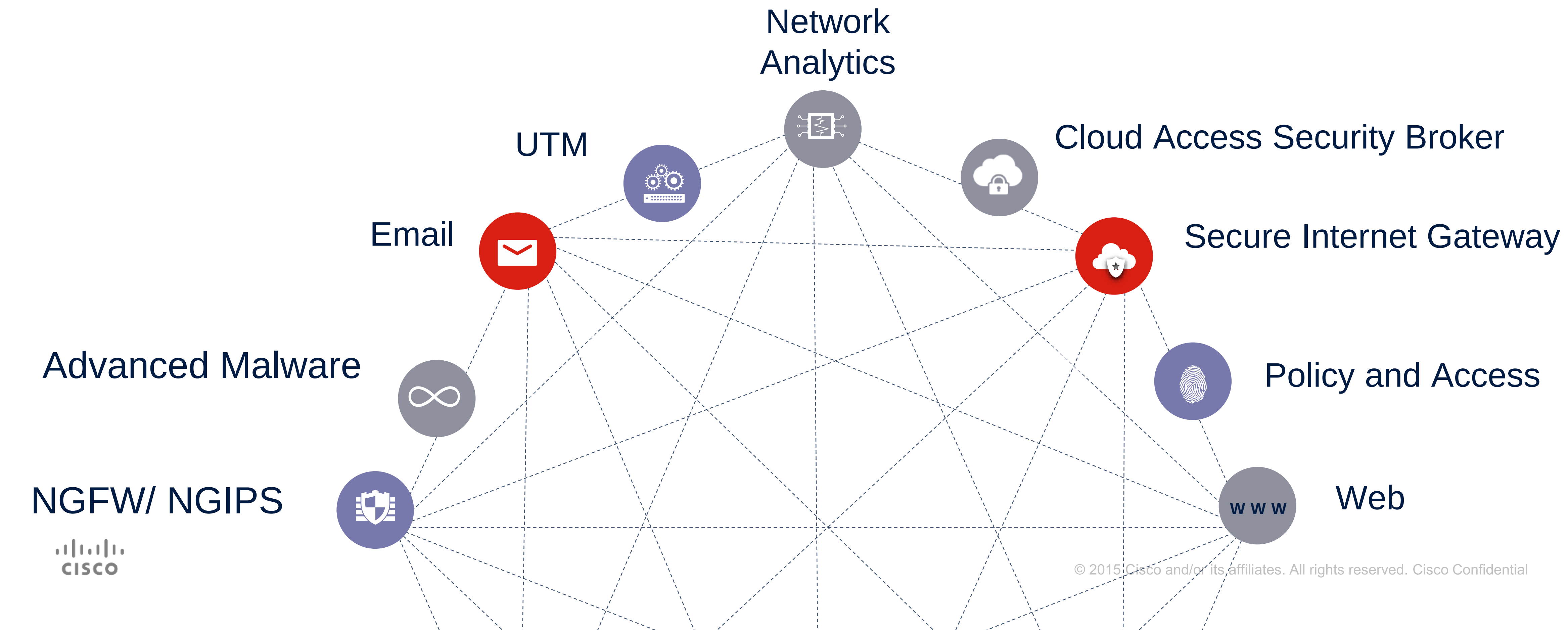
2016

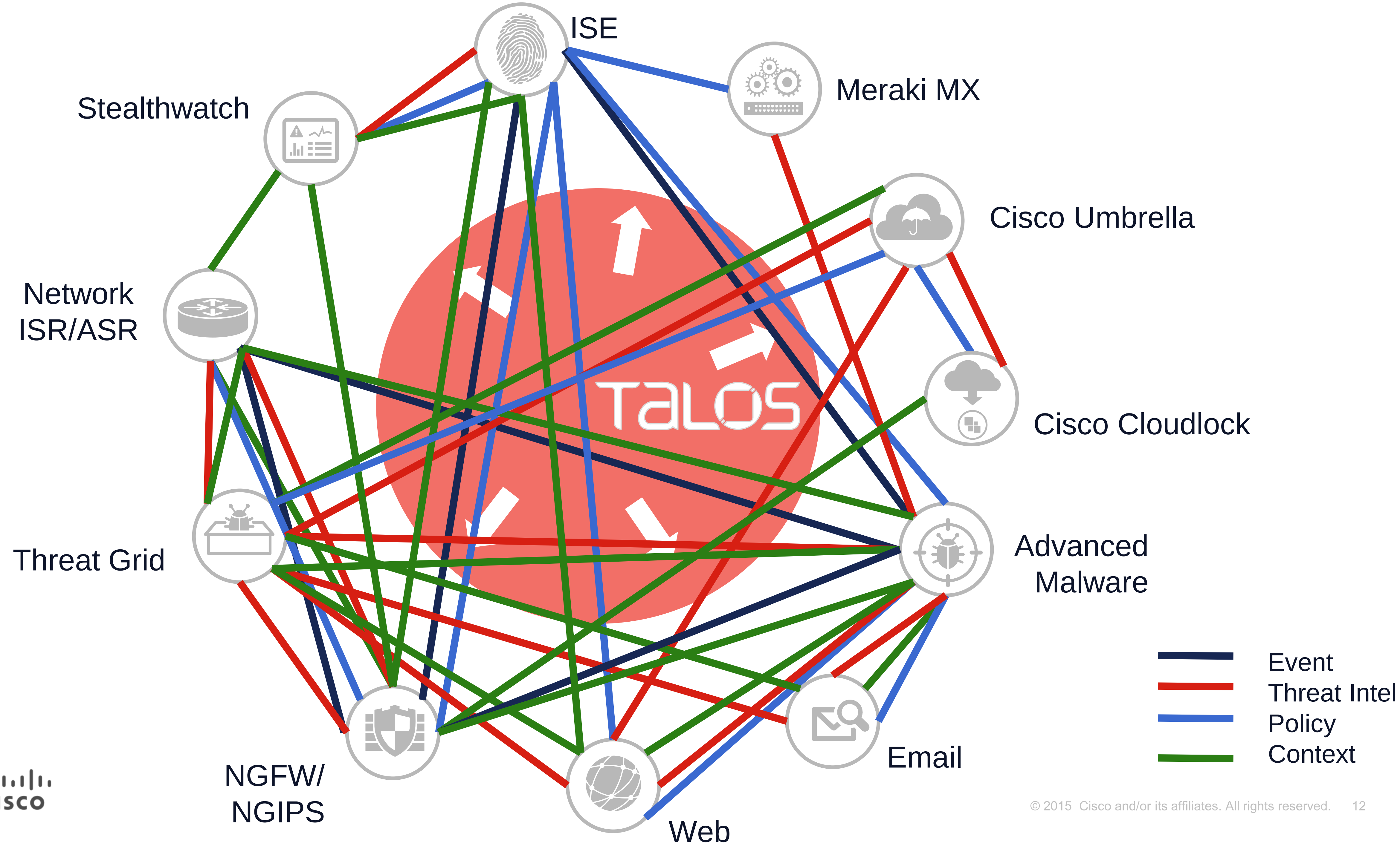
CloudLock acquired

Cisco Umbrella SIG

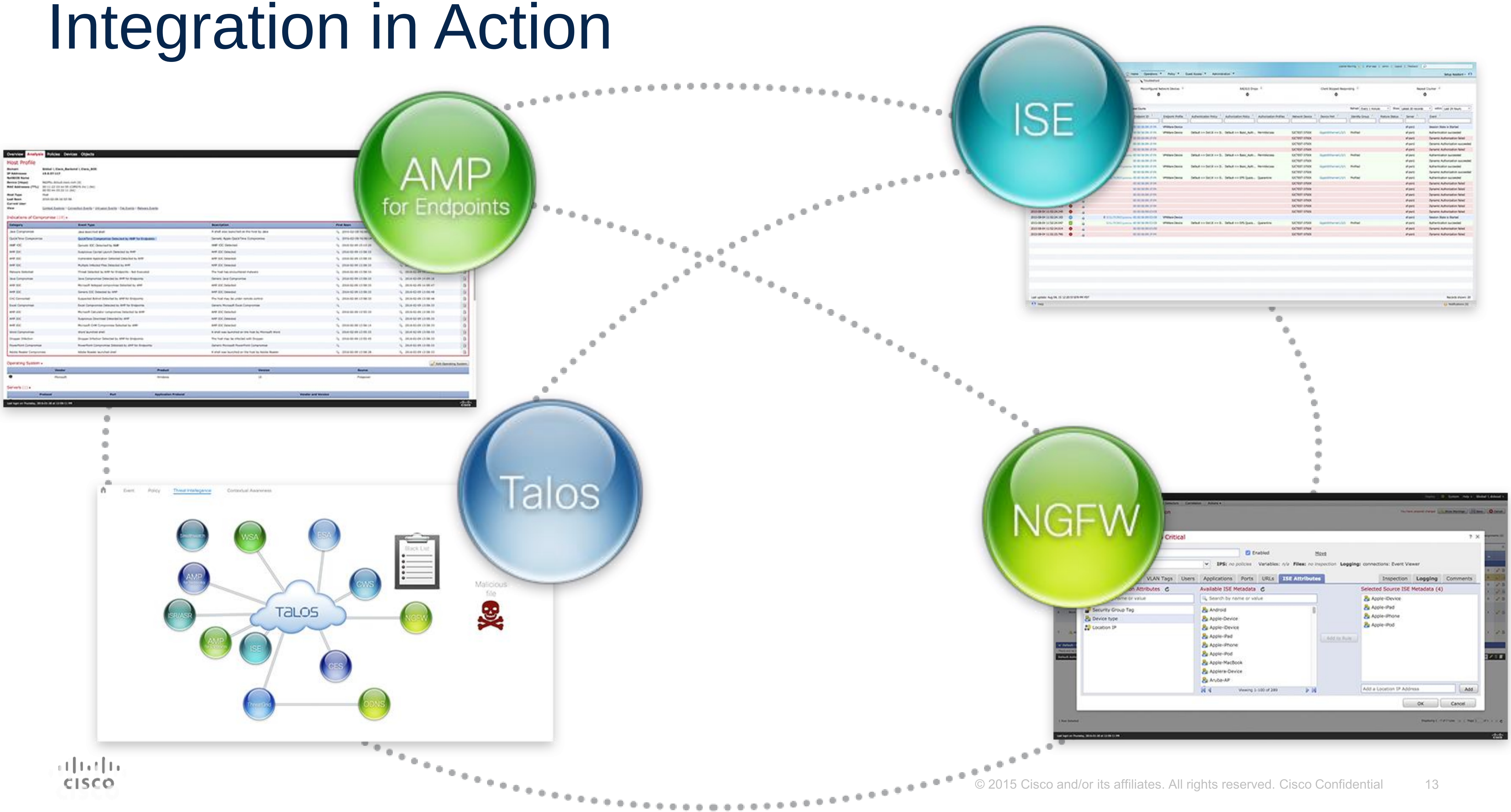
Premiere Portfolio in the Industry

Best of Breed and Integrated Architecture




ISE
Meraki MX
Stealthwatch
Cisco Umbrella
Network ISR/ASR
Talos
Cisco Cloudlock
Advanced Malware
Threat Grid
Email
NGFW/ NGIPS
Web
Event
Threat Intel
Policy
Context

Integration in Action



Talos: World-class Threat Research

Threats by the Numbers

19.7B
Threats Per Day

991M
Web + Malware Threats

221B
Total Threats

1.5M
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

2.6M
Blocks Per Sec

9.9B
Total Blocks Per Month

Intercommunication Among 3rd Party Products

Cisco Security Technical Alliances is…

A program covering multiple partner ecosystems in Cisco Security

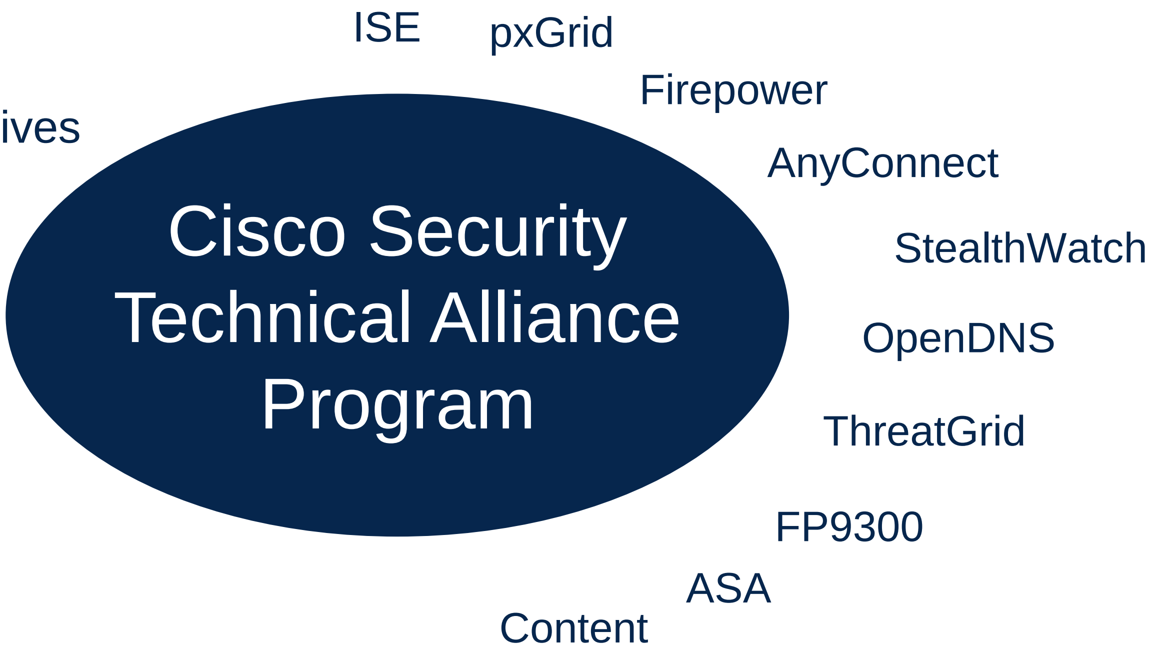
100 percent *focused* Cisco Security initiatives

Real integration benefit across portfolio

Coordinate *support* with key partners

Host community supported *code*

Identify candidates for *deeper integration*



Cisco Security Technical Alliance Program

ISE

pxGrid

Firepower

AnyConnect

StealthWatch

OpenDNS

ThreatGrid

FP9300

ASA

Content

Cisco Solution Partner Program (SPP)

DevNet

Fore more information go to http://www.cisco.com/go/csta

Integration Points Across the Security Portfolio

- eStreamer API
  - Send Firepower event data to SIEMs
- Host Input API
  - Collect vulnerability and other other host info
- Remediation API
  - Programmatic response to third parties from FireSIGHT
- JDBC Database Access API
  - Supports queries from other applications
- Read/Write API for Firepower
  - Supports FW and Risk Management technologies
- pxGrid
  - Bi-directional context sharing framework for ISE, ecosystem partners
- MDM API
  - Enables 3rd party MDM partners to make mobile device posture part of ISE access policy

- External Restful Services (ERS)
  - Adds 3rd party asset data to ISE inventory database
- AMP Cloud-based API
  - Externalize event data for all 3rd party apps
- ThreatGrid API
  - Hand off suspicious files for analysis
  - Automate submission of files for analysis
  - Create custom or batch threat feeds
- FirePOWER 9300 (SSP) REST API
  - Cisco and third party applications in service chain configuration
- Network Visibility Module (NVM)
  - AnyConnect provides IPFIX data
- Management API for ASA
  - Third party management of ASA, policy auditing
- Other Integration Points
  - Cloud, ESA, WSA

Integration and ecosystem partners

Vulnerability Management

- Outpost24
- RAPID7
- SAINT
- tenable network security
- QUALYS
- Greenbone
- Network Critical
- POSITIVE TECHNOLOGIES
- tripwire

Packet Brokering

- GARLAND
- Interface Masters TECHNOLOGIES Innovative Network Solutions
- A10
- IXIA
- VSS monitoring
- Gigamon

IAM/SSO

- SECUREAUTH
- NetIQ
- Ping Identity

Network Infrastructure & Policy Management

- HYTRUST Cloud Under Control
- embrane
- VCE THE VIRTUAL COMPUTING ENVIRONMENT COMPANY
- tufin Making Security Manageable
- Symantec
- algosec
- FIREMON
- skybox security
- CITRIX
- UBIqube
- f5

Performance Management & Visualization

- LiveAction Simplifying the Network
- hyperglance

Custom Detection

- radware
- SOPHOS
- P1 Security Priority One Security
- skyhigh
- elastica
- ARBOR NETWORKS

Mobility

- airwatch by vmware
- SOTI
- MobileIron
- Tangoe
- JAMF software
- SAP
- ABSOLUTE
- Good
- GLOBO
- MaaS360 by Fiberlink

Firewall/Access Control

- IMPERVA
- Infoblox
- BAYSHORE
- Check Point SOFTWARE TECHNOLOGIES LTD.

Packet Capture & Forensics

- NETSCOUT
- endace
- NEXT COMPUTING
- savvius

Remediation & Incident Response

- THREATCONNECT
- GUIDANCE SOFTWARE

SIEM & Analytics

- Huntsman
- EIQ
- ArcSight
- ACUITY SYSTEMS
- TIBCO
- E8 SECURITY
- Q1 Labs
- FIDELIS CYBERSECURITY
- BLACKHAWK NETWORK
- HAWK NETWORK DEFENSE
- splunk>
- Trustwave
- FORTSCALE
- LogRhythm
- BlackStratus
- invincea
- RSA SECURITY
- Symantec

CISCO

Services Brings it All Together

Cisco Security Services

Advisory

- Custom Threat Intelligence
- Cybersecurity Assessments

Integration

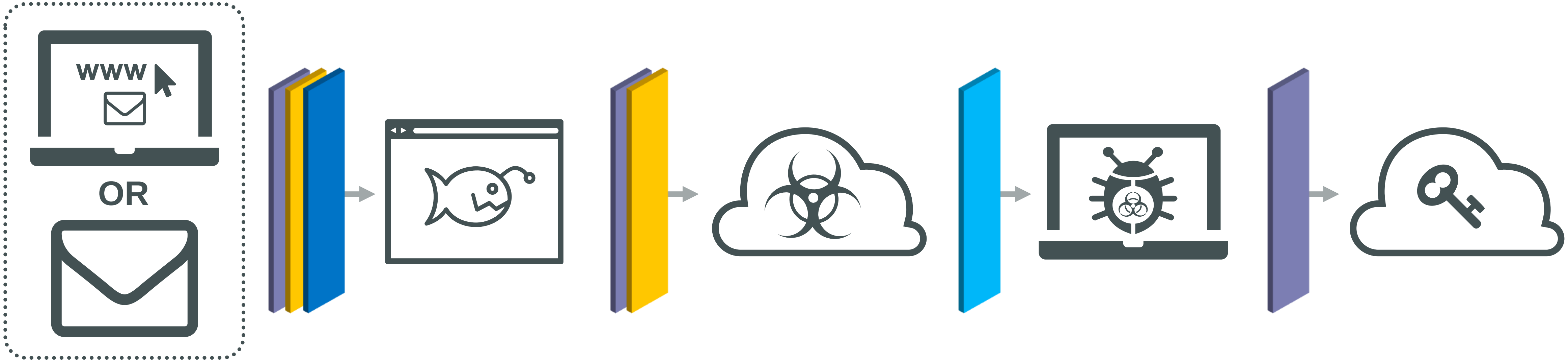
- Integration Services
- Security Optimization Services

Managed

- Managed Threat Defense
- Remote Managed Services

Most active volcano
Largest waterfall
Cleanest capital
Longest life expectancy
First democratically elected female president
Northern most botanical garden and golf course

Cisco Ransomware Defense - Quick Prevention



Umbrella blocks the request

NGFW blocks the connection

Email Security w/AMP blocks the phishing email

Umbrella blocks the request

NGFW blocks the connection

AMP for Endpoint blocks the file

Umbrella blocks the request to Encryption Key Infrastructure

● Umbrella ● Next-Gen Firewall ● Email w/AMP ● AMP Endpoint

Tiered Security Software Buying Models

Cisco ONE Software

“Use Case Driven”

- All Organizations with 1+ devices and/or 100+ users
- Less than 3 technologies
- Data Center, WAN, Access Domain Specific

Software Volume Purchasing

“Technology Driven”

- All Organizations with 100-1M Users/End Points
- 3+ Technologies
- Broad Security Portfolio

Security Advantage

“Budget Driven”

- Mid-to-Large Organizations with $200K+ Budget
- Flexible Consumption
- Complete Security Portfolio

Security ELA

” Architecture Driven”

- Large Organizations with $400K+ budget and/or 1,000+ users
- Unlimited consumption
- Complete Security Portfolio