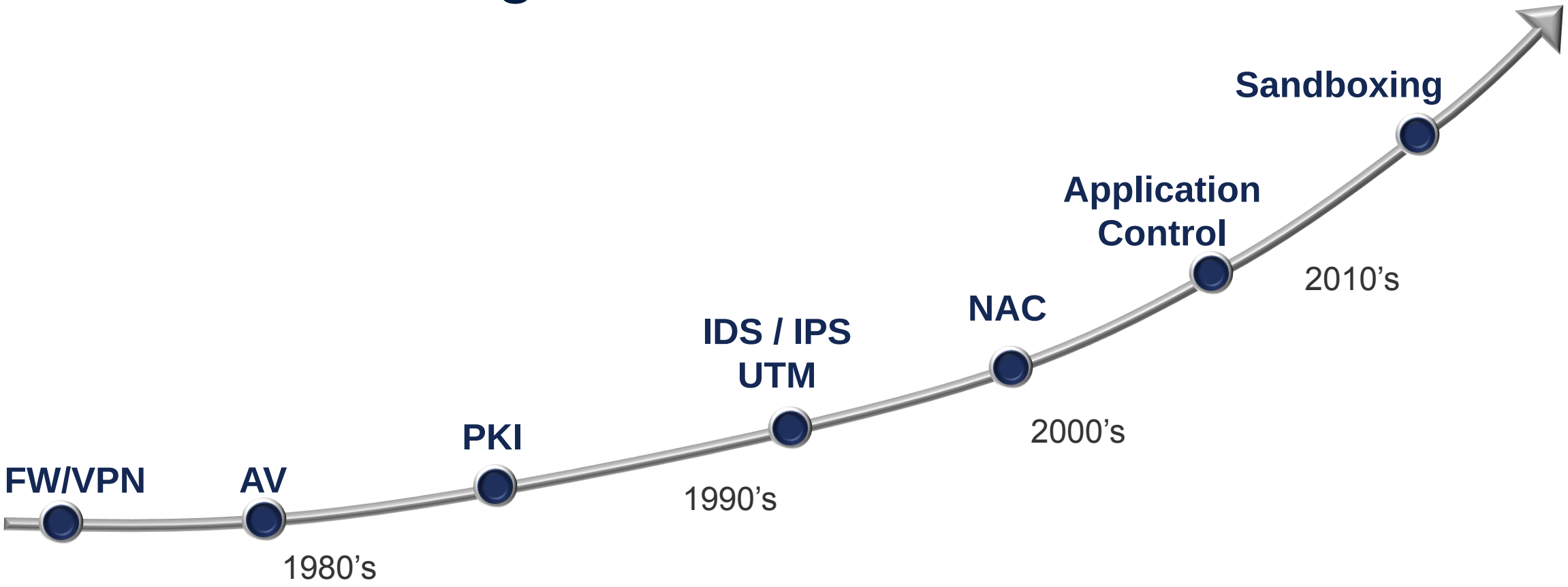
Aby se z toho bezpečnostní správci nezbláznili Cisco security integrace

Milan Habrcetl
Cisco CyberSecurity Specialist
Mikulov, 5. 9. 2017

Last 20 years of security: Got a problem?

Buy a Box

Same Old Song and Dance

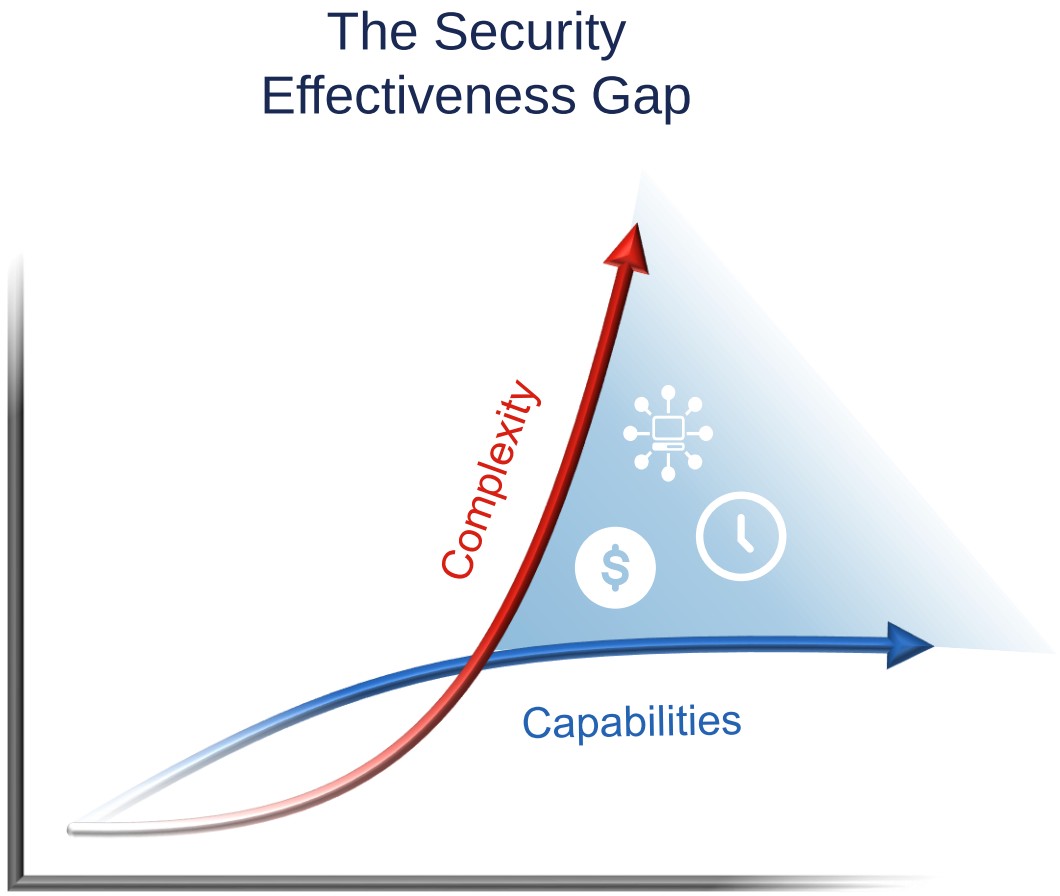


The Existing Security Stack…

Why a Security Architecture?

Ability to Defend Getting More Complex

- Attack Surface Diversity: Growing exponentially due to IoT, SaaS / IaaS, and personal device trends
- Threats: Continuous rise in sophistication of attackers combined with rapid evolution of attacker techniques and tools
- Detection: Efficacy of classical detection methods eroding
- User Behavior: No longer constrained to IT controlled places, apps or devices



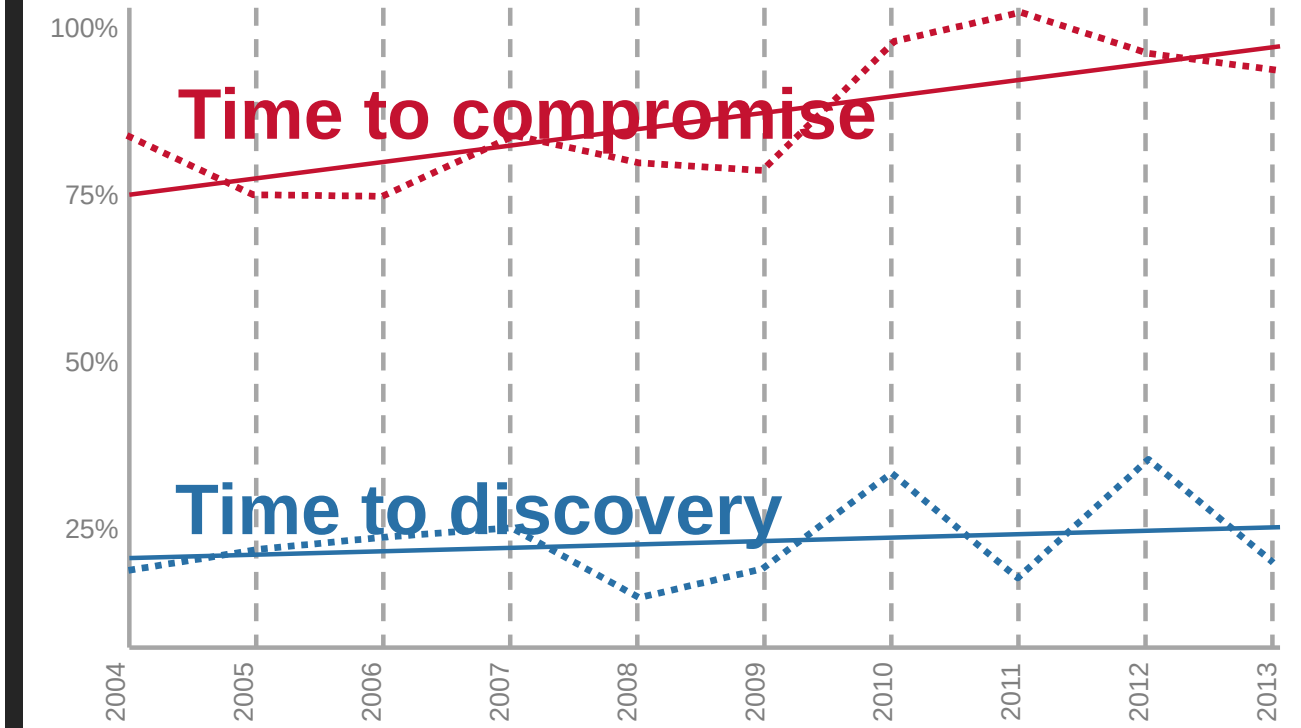
Industry Result

Time to Detection

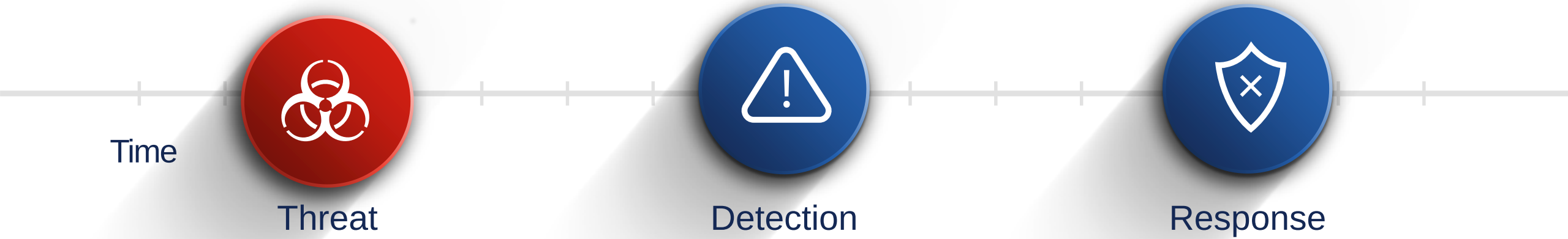
100

Industry Days

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

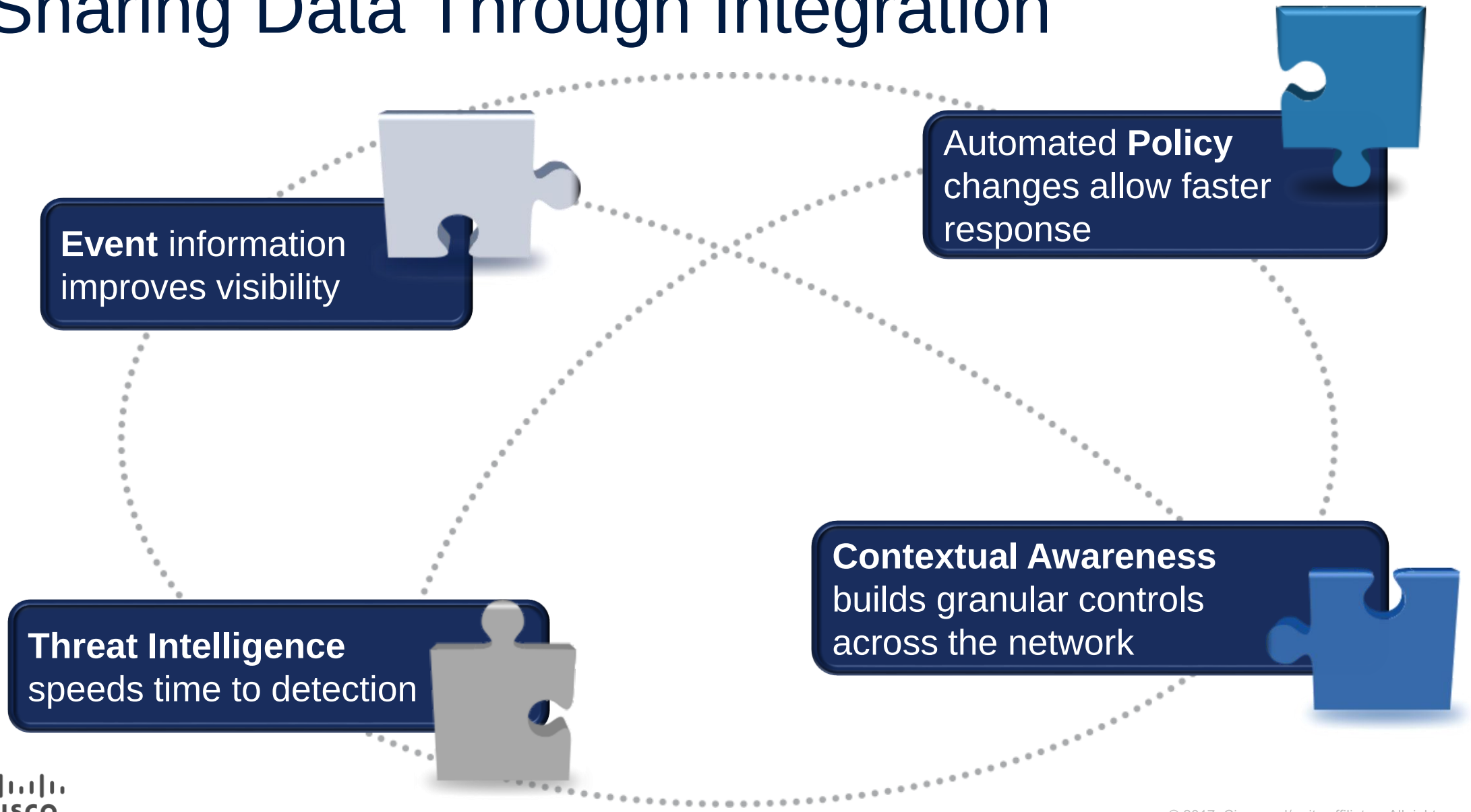


Is our security posture effective?

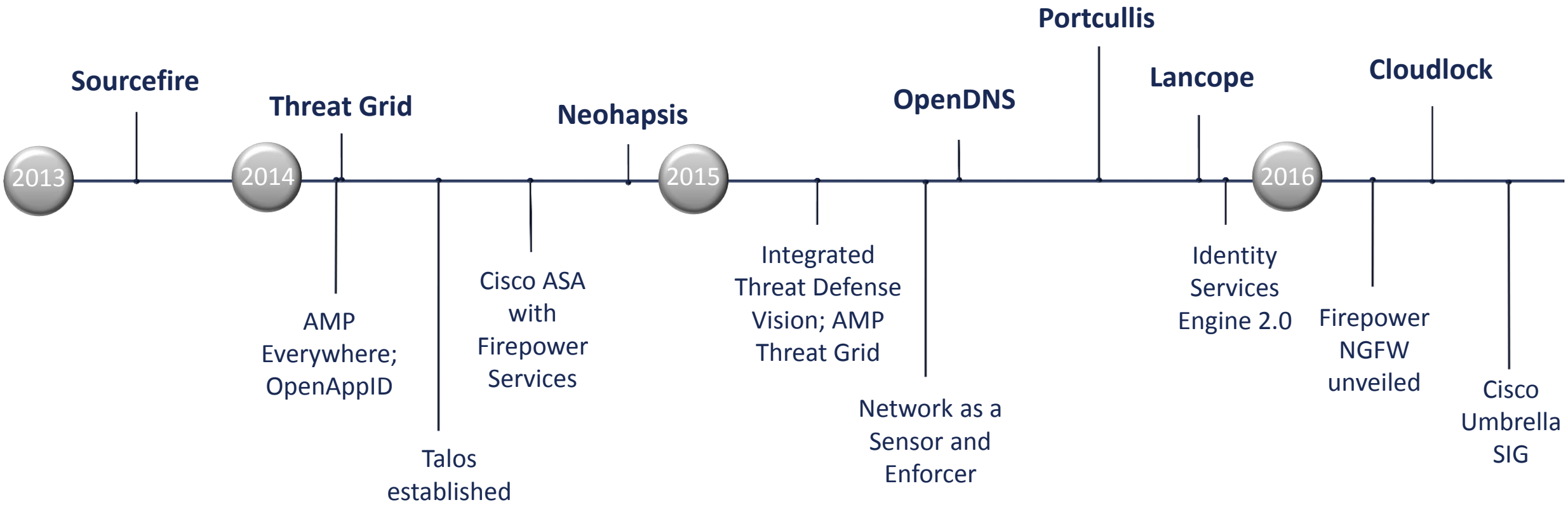


Integration = Effective Security

Sharing Data Through Integration

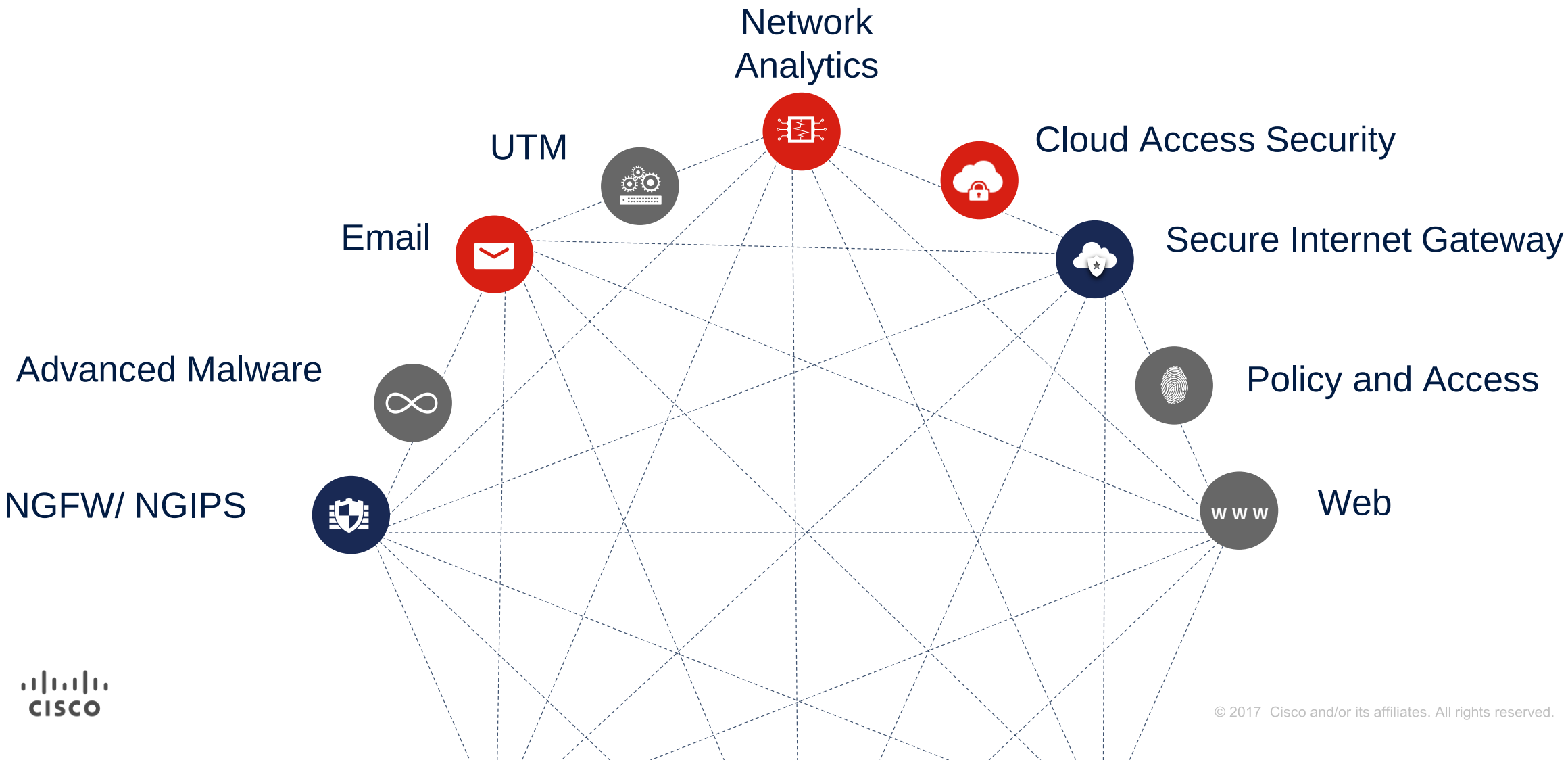


Integration has Driven Cisco's Portfolio Growth



Integrated Architectural Approach

Premiere Portfolio in the Industry



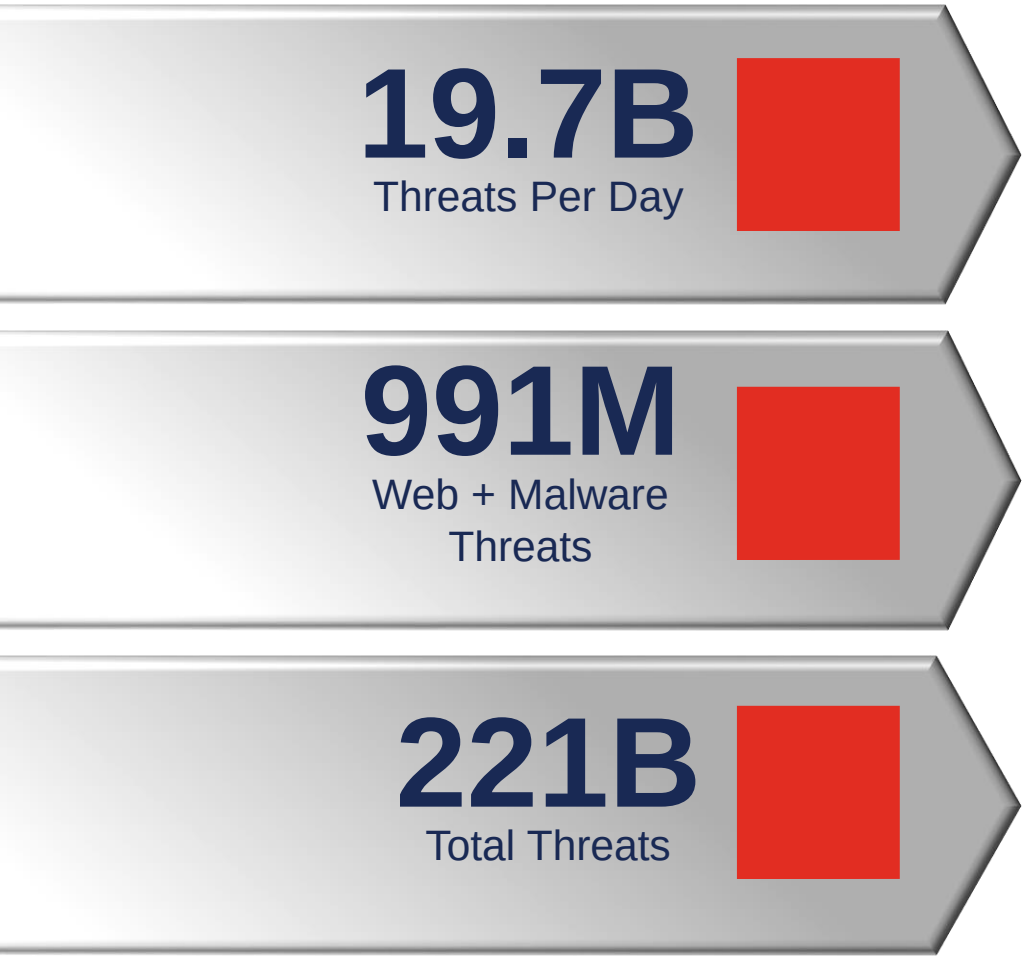
Best of Breed

PORTFOLIO

Integrated

ARCHITECTURE

Functional Integration: Talos Threat Intelligence



1.5M
Malware Samples Per Day

1B
Sender Base Reputation Queries Per Day

8.2B
Web Filtering Blocks Per Month

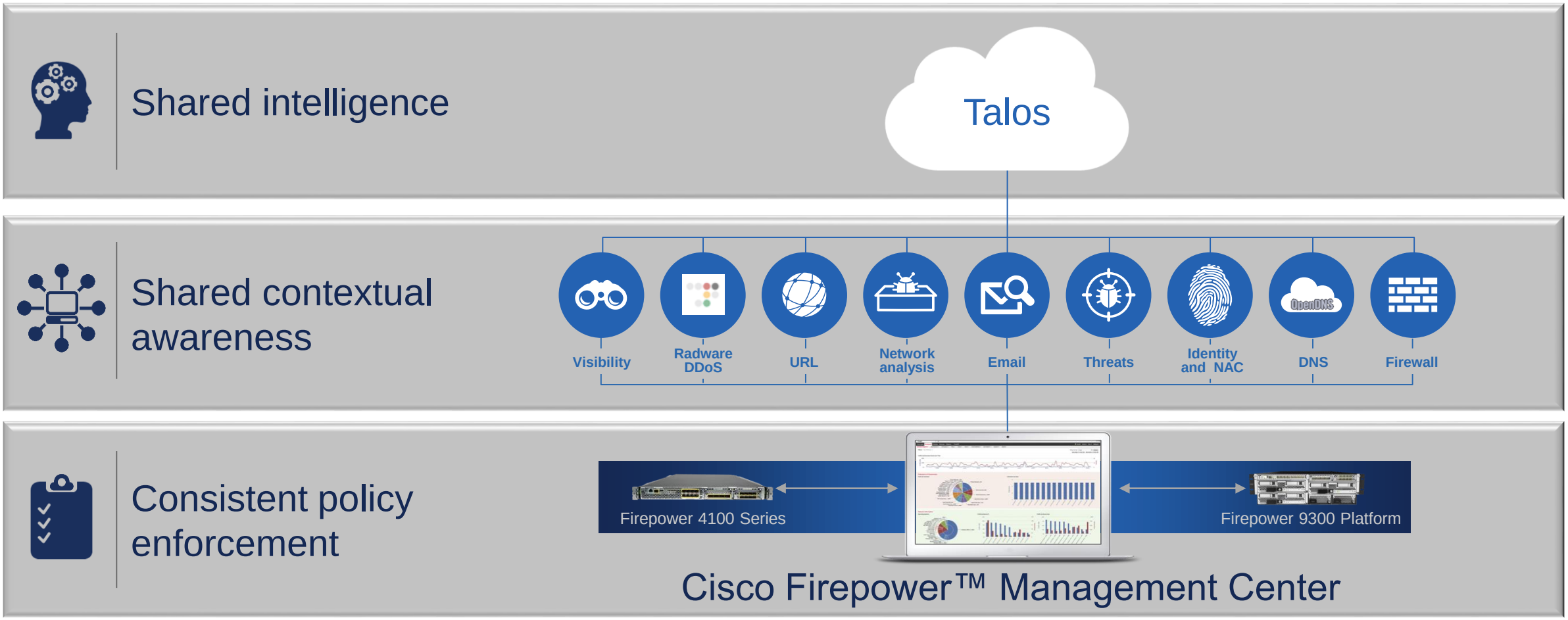
1.4M
AV Blocks Per Day

1.8B
Spyware Blocks Per Month

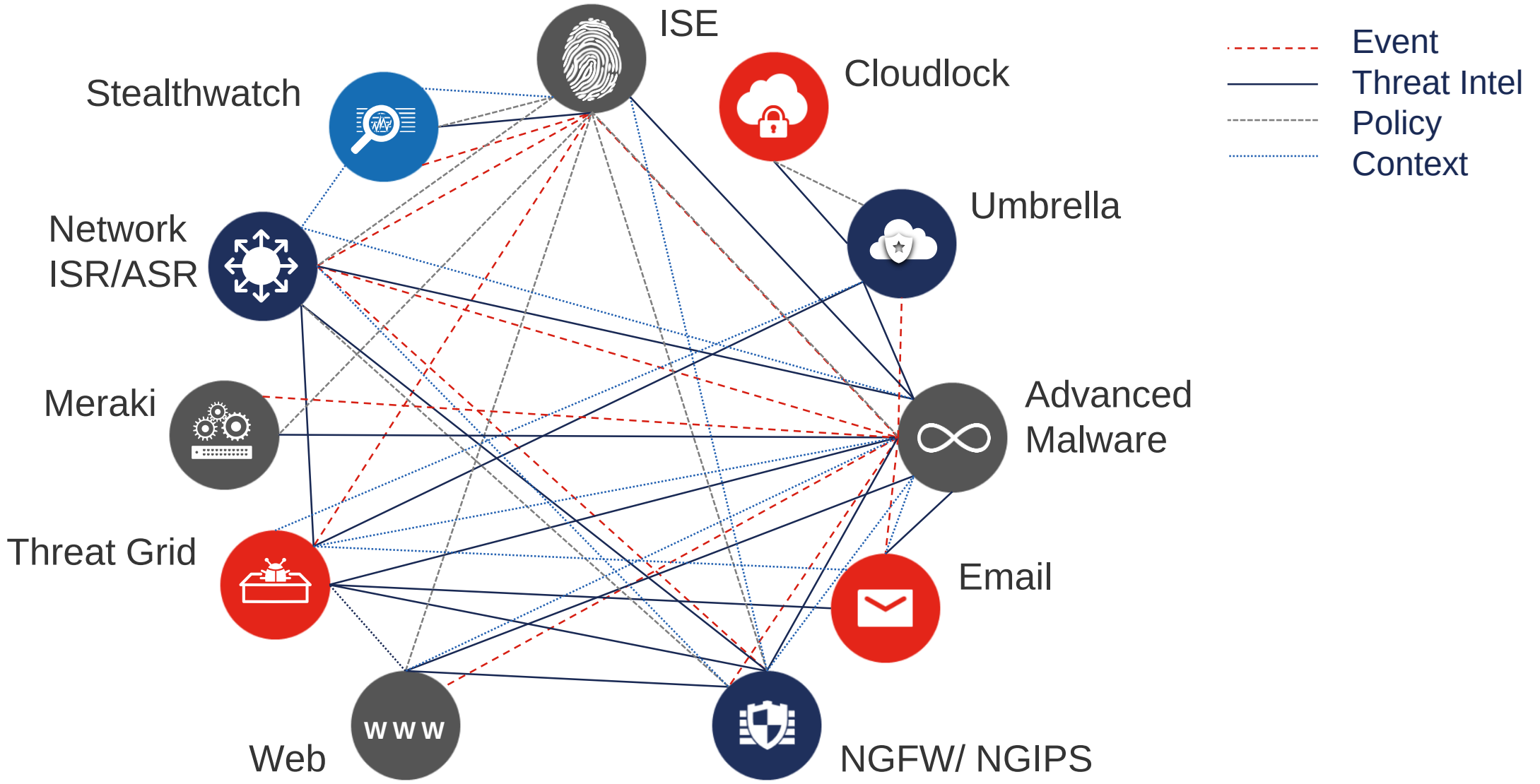
2.6M
Blocks Per Second

9.9B
Total Blocks Per Month

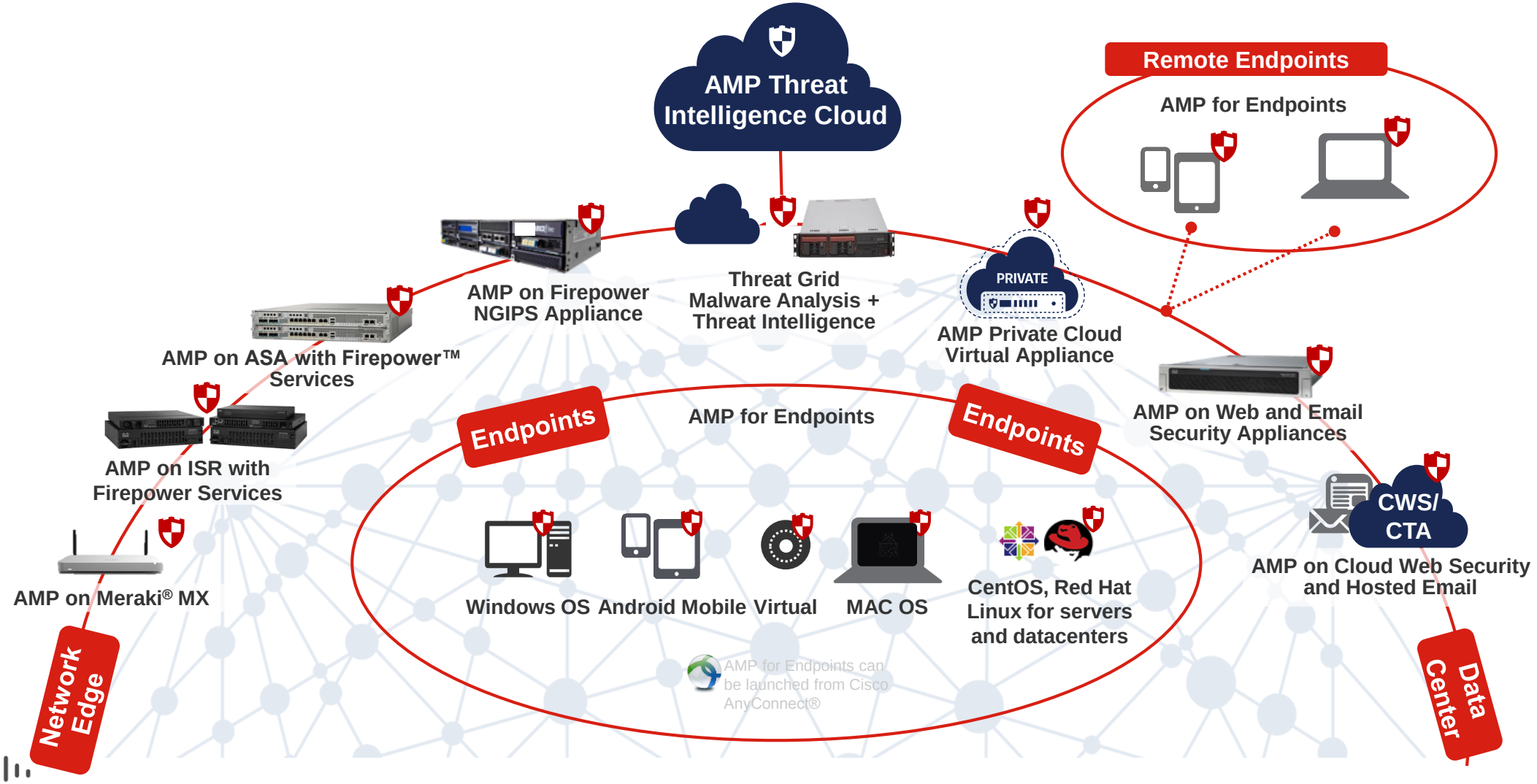
Functional Integration: Firepower Threat Defense



Solution Integration: Cisco Portfolio



Solution Integration: Advanced Malware Protection



Integration with 3rd Party Products

3rd Party Integration: CSTA

Cisco Security Technical Alliance

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*

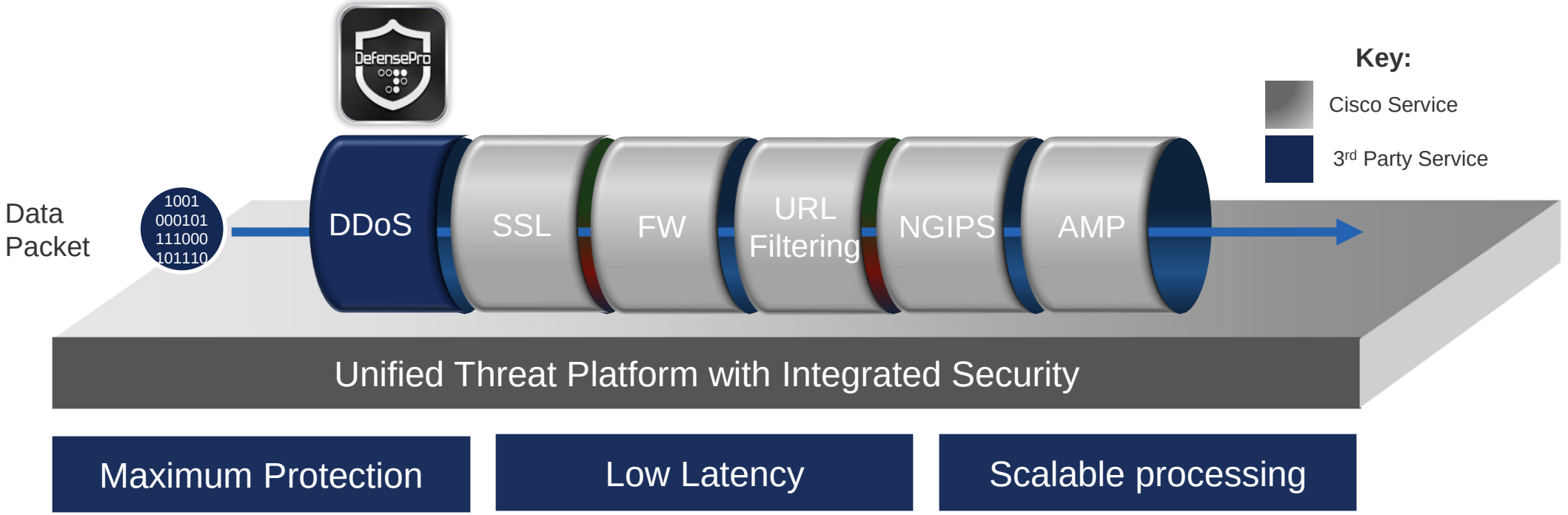
Cisco Solution Partner Program (SPP)

DevNet

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

3rd Party Integration: Radware on Firepower

- Integrated Radware Virtual DefensePro (vDP) in-line DDoS mitigates attacks
- Available on Cisco Firepower 4100 Series and Firepower 9300 platforms



Cisco Security Services

Advisory
- Custom Threat Intelligence
- Cybersecurity Assessments

Integration
- Integration Services
- Security Optimization Services

Managed
- Managed Threat Defense
- Remote Managed Services

Effective Security Needs to be

Simple

Security built into the network and designed to work together

Open

Integrate across the Cisco portfolio and 3rd party products

Automated

Instantaneous remediation

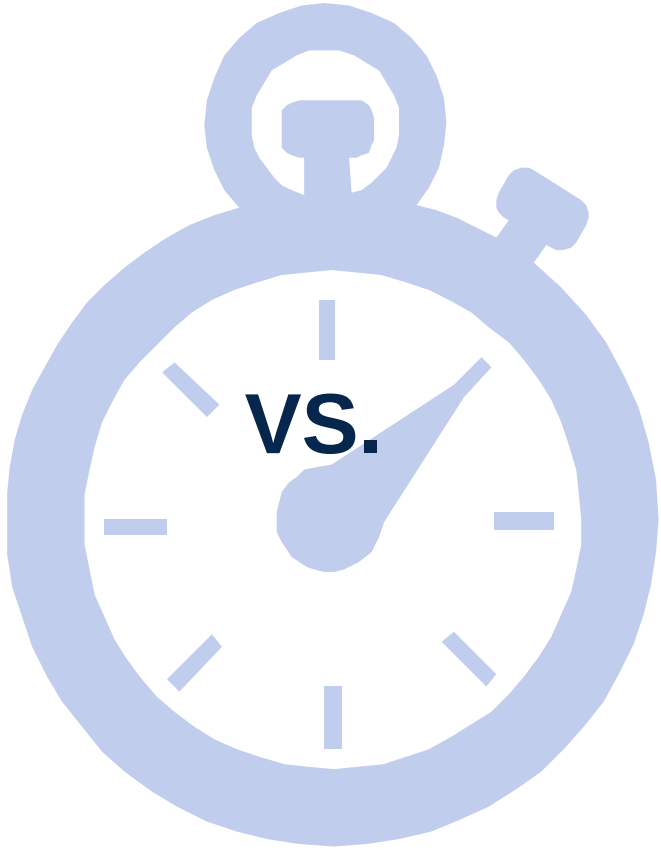
reduce time to detection

save time and money

Integrate Automate: Reduce Time to Detection

100

Industry Days



~3,5

Cisco Hours

*Source Cisco Cyber Security Report, 2017

Effective Security

simple | open | automated

Děkuji za pozornost