Cisco Next Generation Firewalls and IPS

Dragan Novakovic

Security Consulting Systems Engineer

dnovakov@cisco.com

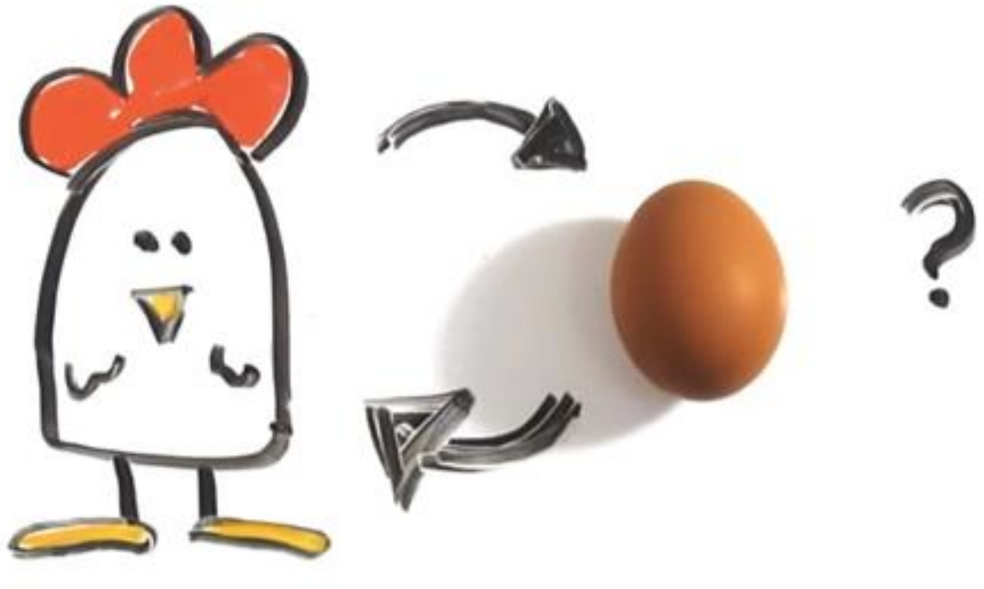
Today’s Agenda

- Firepower System Architecture Overview
- Platforms & Capabilities
- Management Options
- Firepower 6.1 New Capabilities

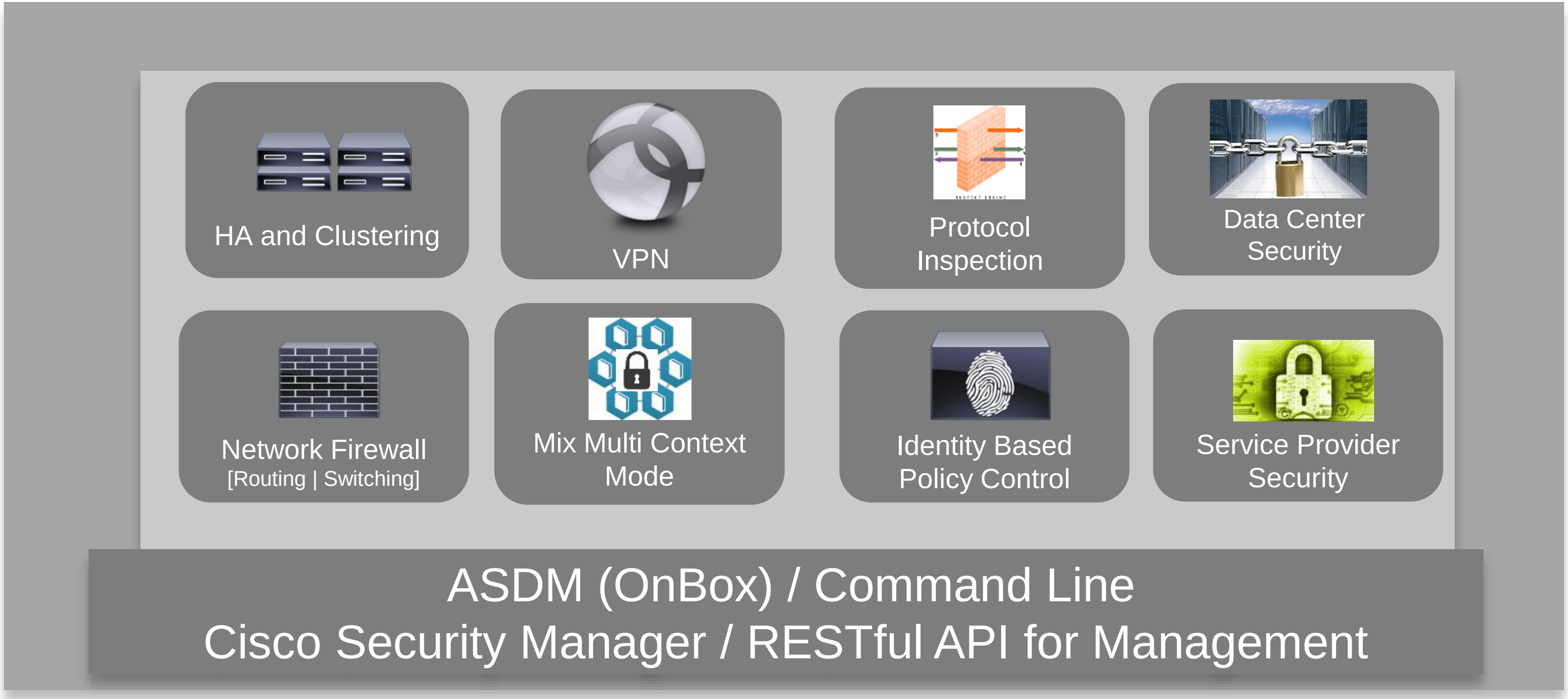
Systems Architecture Overview

How did we get here from there?

- Adaptive Security Appliance (ASA)
- FirePOWER NGIPS
- ASA with FirePOWER Services?
- Firepower NGFW?



ASA “Adaptive Security Appliance”



HA and Clustering

VPN

Protocol Inspection

Data Center Security

Network Firewall
[Routing | Switching]

Mix Multi Context Mode

Identity Based Policy Control

Service Provider Security

ASDM (OnBox) / Command Line
Cisco Security Manager / RESTful API for Management

Firepower NGIPS Platforms

- Firepower Next Generation IPS
  - Best of breed IPS
  - Based on open source Snort
  - Integrated Advanced Malware Protection

  - Acquired by Cisco in 2013

SNORT®

SOURCEfire®

firePOWER™

fireAMP™

Next Generation IPS platform - FirePower 8300

Single-pass, high-performance, low-latency

Flexible in Software

- Firepower NGIPS & AMP

Flexible in Hardware

- Modular for options in Interfaces, including 10GE and 40GE
- High-Performance:
  - 15-60Gbps (with 8350-8390)

Cost Effective

- Best in class for IPS by NSS Labs
- Best in class for NGFW by NSS Labs
- Best in class for Breach Detection by NSS Labs

REFERENCE

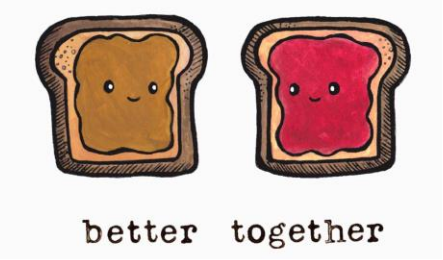
Cisco FirePOWER Platform Features

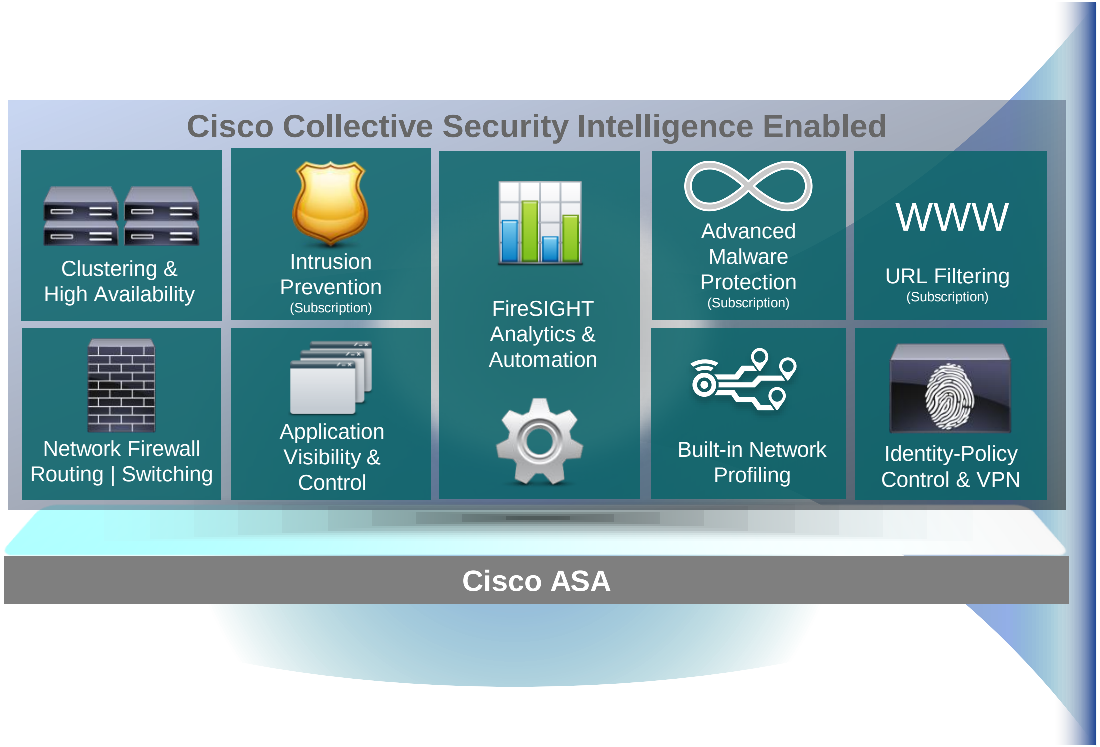
	Virtual	7000	7100	8100	8200/8300
1GE Interfaces		YES	YES	YES	YES
10GE Interfaces		NO	NO	YES	YES
40GE Interfaces		NO	NO	NO	YES
SFP Ports		NO	YES *	YES **	YES **
Hardware Bypass		YES	YES	YES	YES
Software Bypass	YES	YES	YES	YES	YES
Hardware Fast Pass		NO	NO	YES	YES
L3 Mode	NO	YES	YES	YES	YES

* 7115, 7125, and 7150 models only

** Fiber-to-SFP Tranceiver

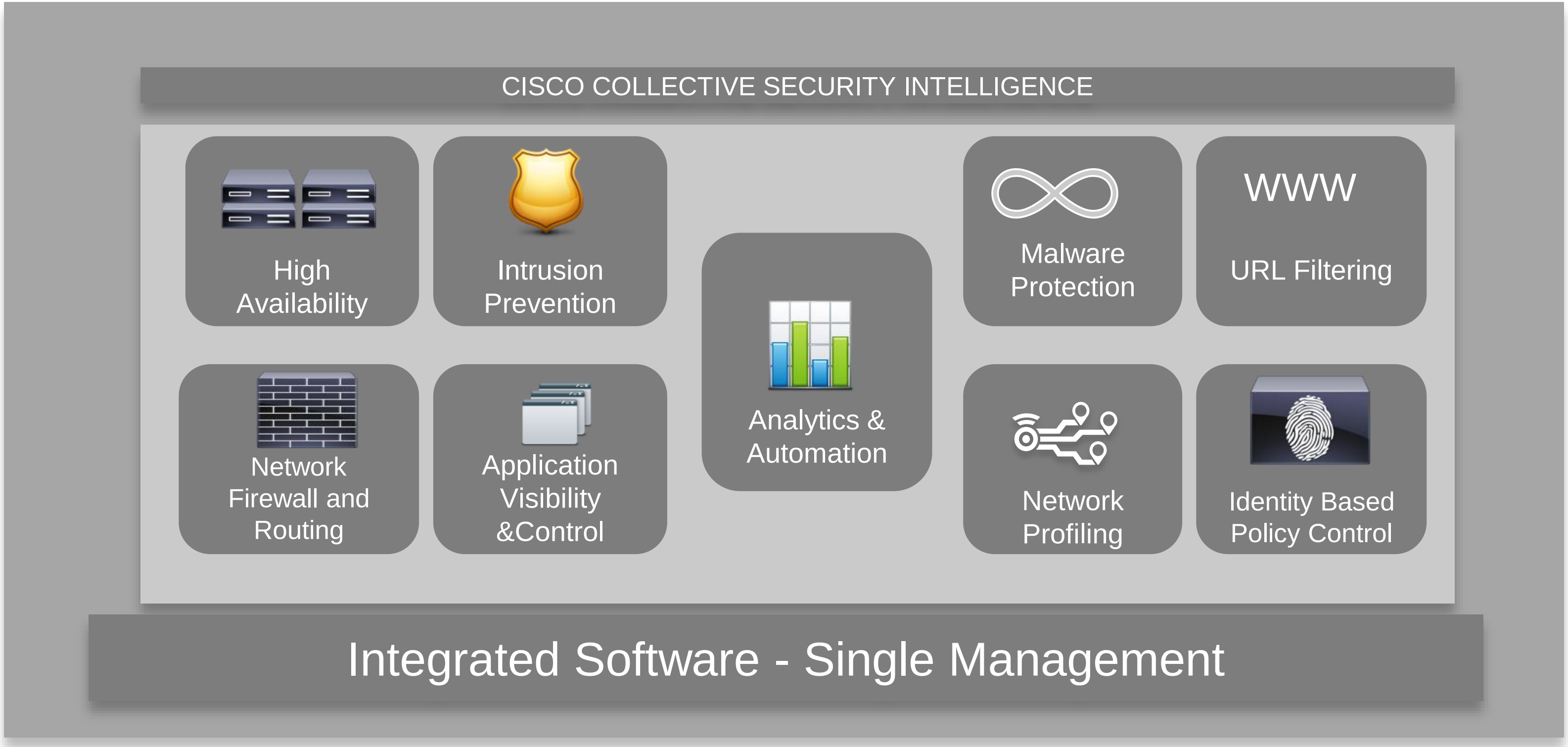
ASA with FirePOWER Services




Cisco Collective Security Intelligence Enabled
Clustering & High Availability
Intrusion Prevention (Subscription)
FireSIGHT Analytics & Automation
Advanced Malware Protection (Subscription)
WWW
URL Filtering (Subscription)
Network Firewall Routing | Switching
Application Visibility & Control
Built-in Network Profiling
Identity-Policy Control & VPN
Cisco ASA

- ▶ Cisco ASA is world's most widely deployed, enterprise-class stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced malware protection

Firepower Threat Defense



CISCO COLLECTIVE SECURITY INTELLIGENCE

High Availability

Intrusion Prevention

Network Firewall and Routing

Application Visibility &Control

Analytics & Automation

Malware Protection

URL Filtering

Network Profiling

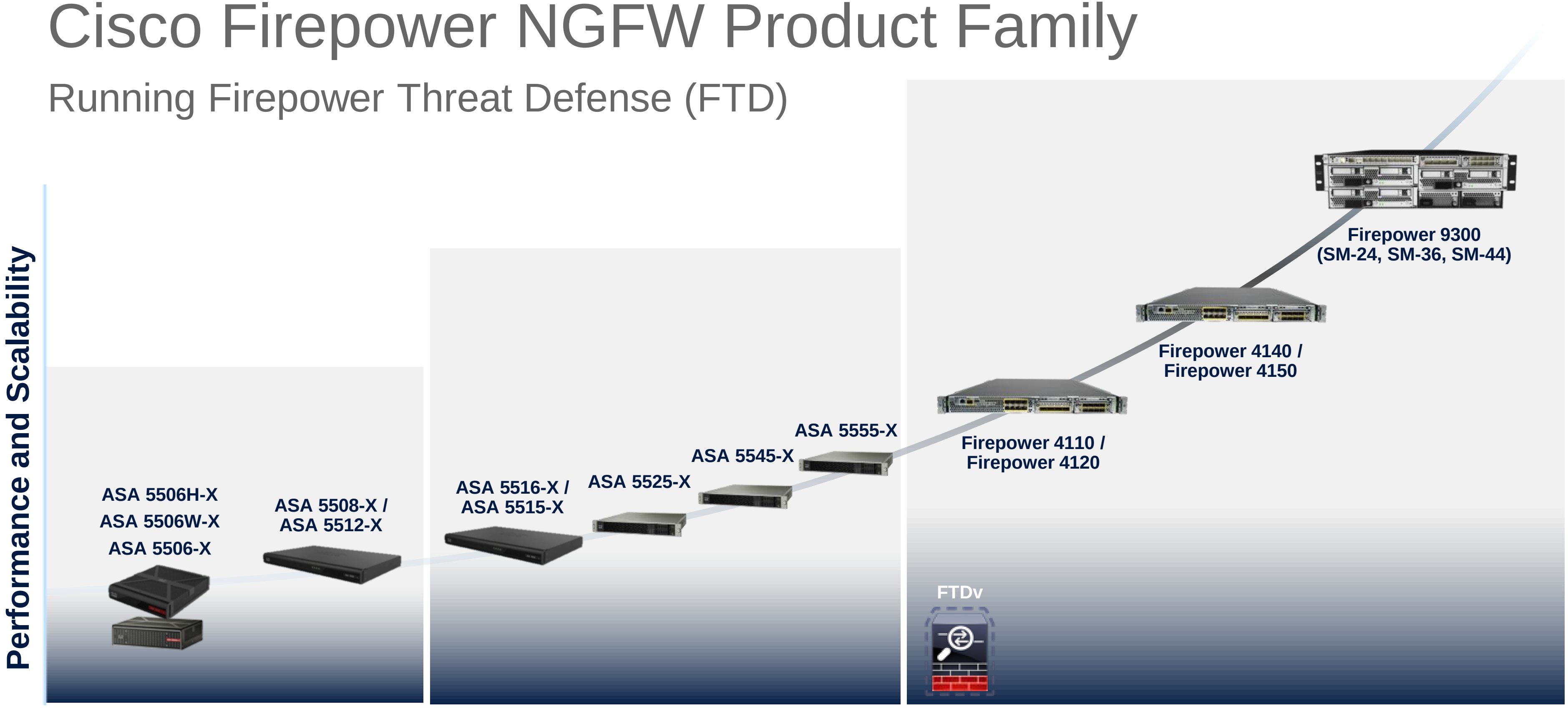
Identity Based Policy Control

Integrated Software - Single Management

Platforms & Capabilities

Cisco Firepower NGFW Product Family

Running Firepower Threat Defense (FTD)



Performance and Scalability

ASA 5506H-X
ASA 5506W-X
ASA 5506-X

ASA 5508-X /
ASA 5512-X

ASA 5516-X /
ASA 5515-X

ASA 5525-X

ASA 5545-X

ASA 5555-X

Firepower 4110 /
Firepower 4120

Firepower 4140 /
Firepower 4150

Firepower 9300
(SM-24, SM-36, SM-44)

FTDv

SMB & Distributed Enterprise

Commercial & Enterprise

Data Center, High Performance Computing, Service Provider

Cisco NGFW Platforms

Firepower Threat Defense for ASA 5500-X

250 Mb -> 1.75 Gb
(Max AVC throughput)

Firepower 4100 Series and Firepower 9300

41xx = 12 Gb -> 25 Gb
93xx = 25 Gb -> 100Gb

Firepower Services on ASA 5500-X and 5585-X

4.5 Gb -> 15 Gb
(Max AVC throughput)

NGFW capabilities all managed by Firepower Management Center

Firepower 4100 Series

Introducing four new high-performance models

Performance and Density Optimization

- 10-Gbps and 40-Gbps interfaces
- Up to 80-Gbps throughput
- 1-rack-unit (RU) form factor
- Low latency

Multiservice Security

- Integrated inspection engines for FW, NGIPS, Application Visibility and Control (AVC), URL, Cisco Advanced Malware Protection (AMP)
- Radware DefensePro DDoS
- ASA and other future third party

Unified Management

- Single management interface with Firepower Threat Defense
- Unified policy with inheritance
- Choice of management deployment options

Cisco Firepower 9300 Platform

High-speed, scalable security

Modular

Benefits
- Standards and interoperability
- Flexible architecture

Features
- Template-driven security
- Secure containerization for customer apps
- RESTful/JSON API
- Third-party orchestration and management

Multiservice Security

Benefits
- Integration of best-in-class security
- Dynamic service stitching

Features*
- Cisco® ASA container
- Cisco Firepower™ Threat Defense containers:
  - NGIPS, AMP, URL, AVC
- Third-party containers:
  - Radware DDoS
  - Other ecosystem partners

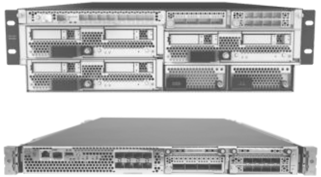
Carrier Class

Benefits
- Industry-leading performance:
  - 600% higher performance
  - 30% higher port density

Features
- Compact, 3RU form factor
- 10-Gbps/40-Gbps I/O; 100-Gbps ready
- Terabit backplane
- Low latency, intelligent fast path
- Network Equipment-Building System (NEBS) ready

Firepower NGFW Software

Cisco Firepower NGFW



Cisco Firepower™ NGFW

Stop more threats

Gain more insight

Detect earlier, act faster

Reduce complexity

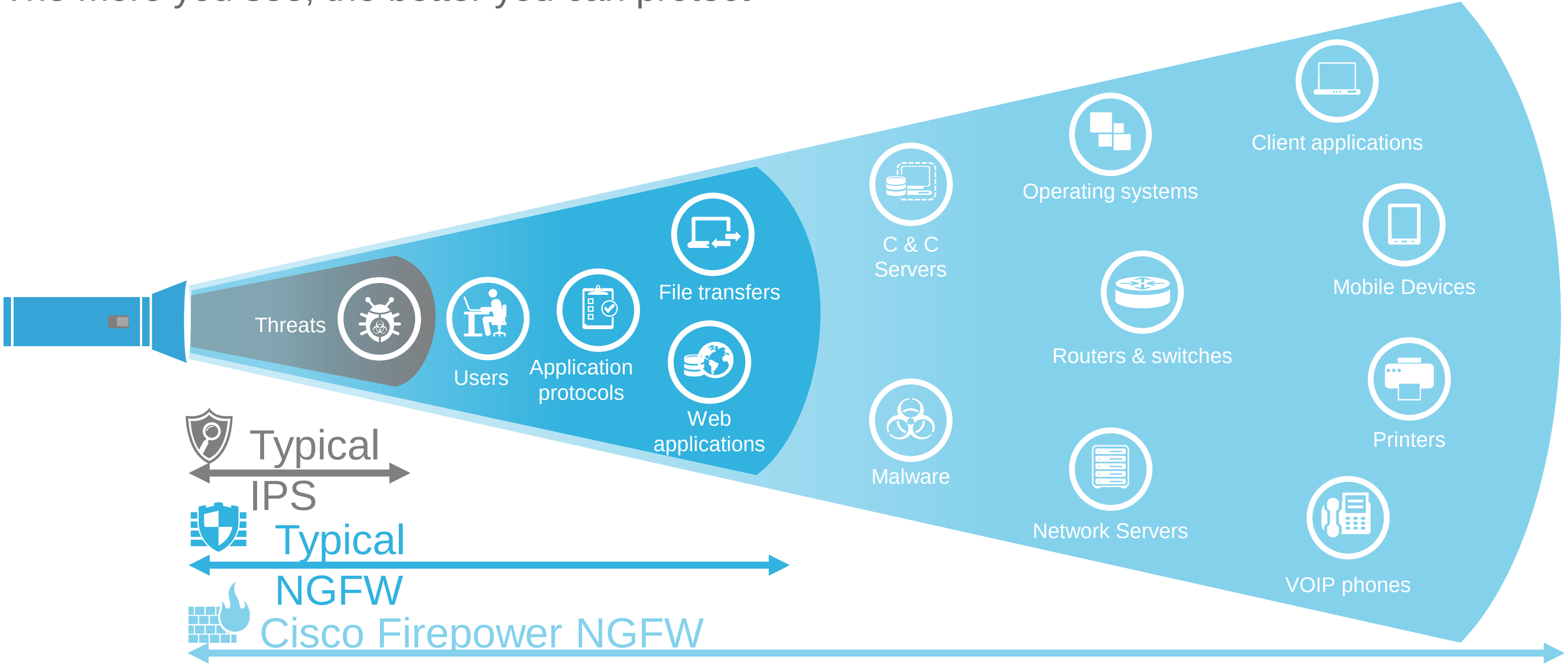
Get more from your network

Threat Focused

Fully Integrated

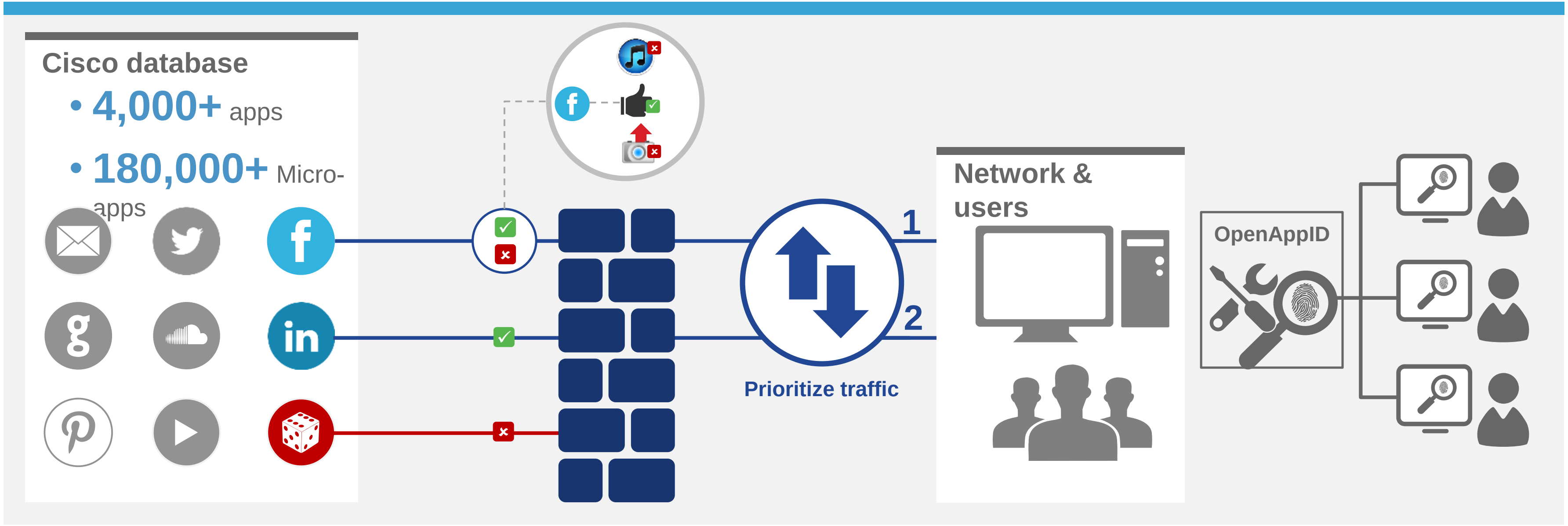
Offering extensive contextual visibility

The more you see, the better you can protect



Provide next-generation visibility into app usage

Application Visibility & Control



Cisco database

- **4,000+** apps
- **180,000+** Micro-apps

See and understand risks

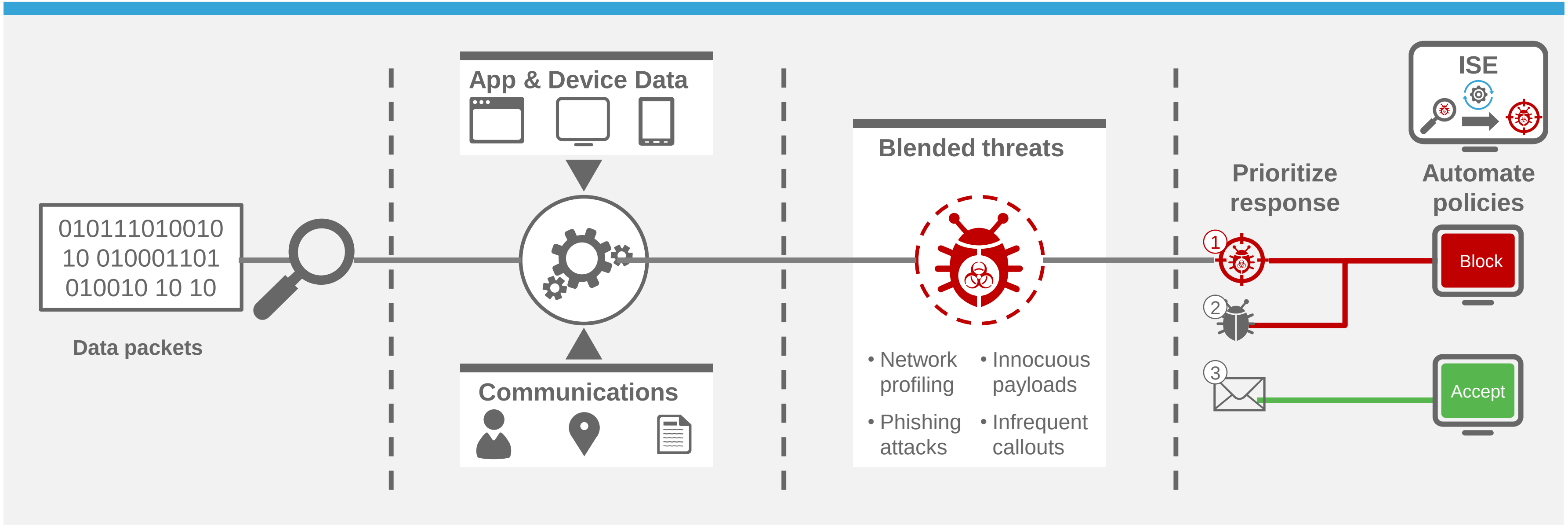
Enforce granular access control

Prioritize traffic and limit rates

Create detectors for custom apps

Understand threat details and quickly respond

Next-Generation Intrusion Prevention System (NGIPS)



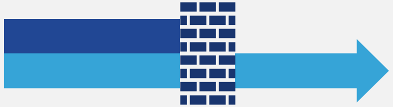
Scan network traffic | Correlate data | Detect stealthy threats | Respond based on priority

Pick from many deployment modes

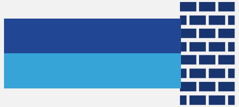
Firewall deployment modes

Inline or Passive

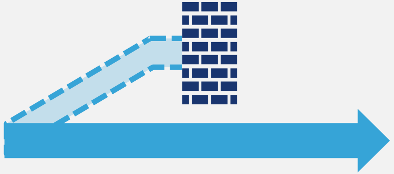
Inline



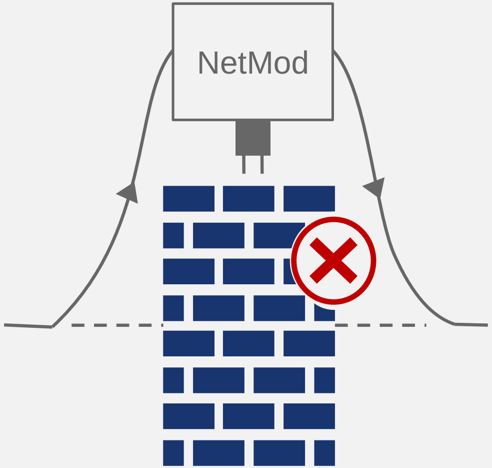
Inline Tap



Passive

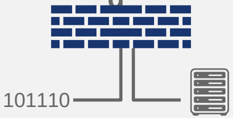


Fail-to-wire NetMods

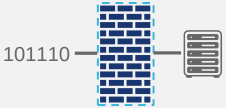


Additional options

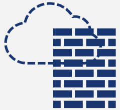
Route
d



Transparent

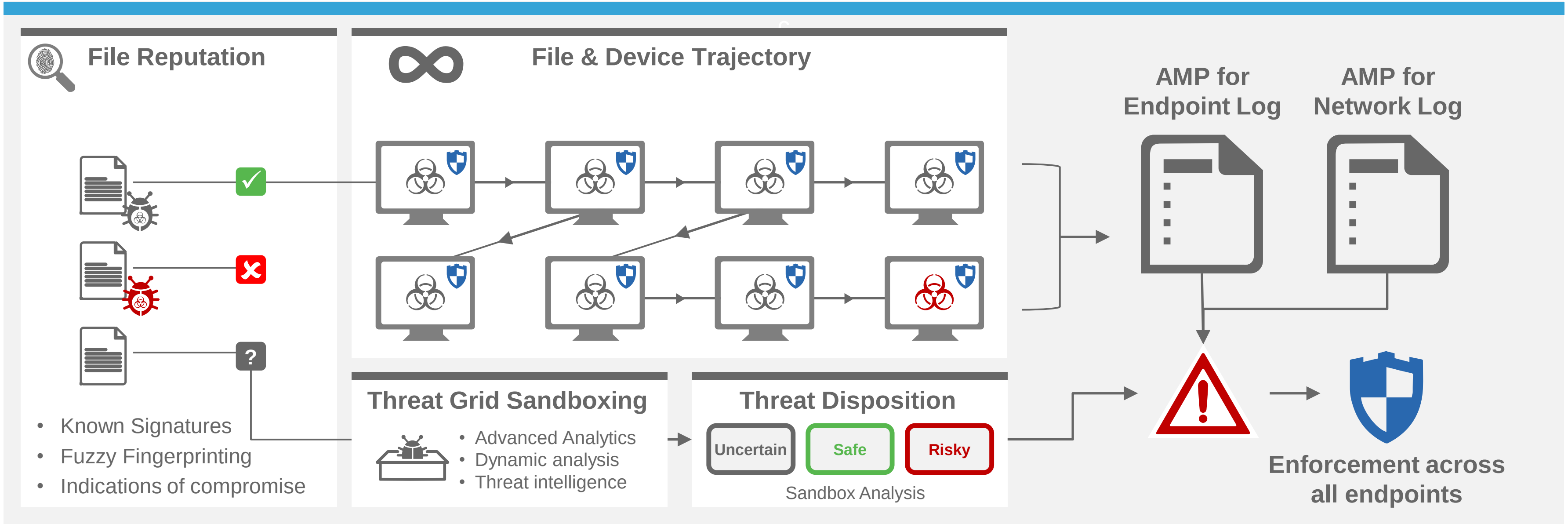


Virtual or Physical



Uncover hidden threats in the environment

Advanced Malware Protection (AMP)



Block known malware

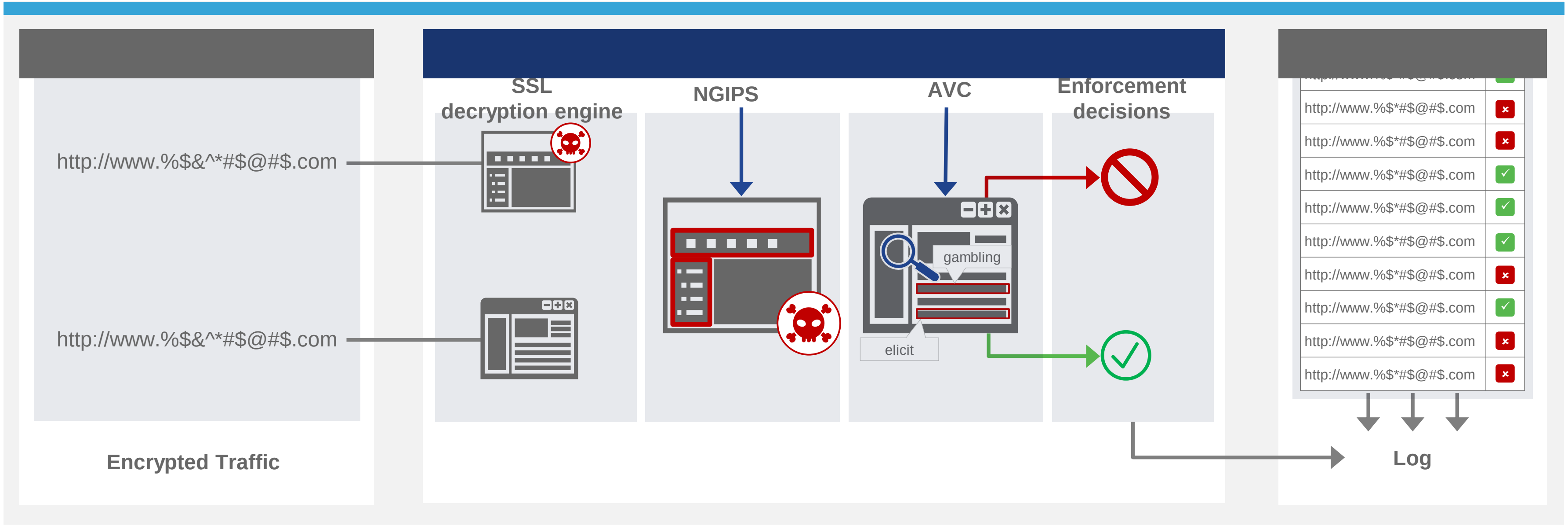
Investigate files safely

Detect new threats

Respond to alerts

Uncover hidden threats at the edge

SSL decryption engine



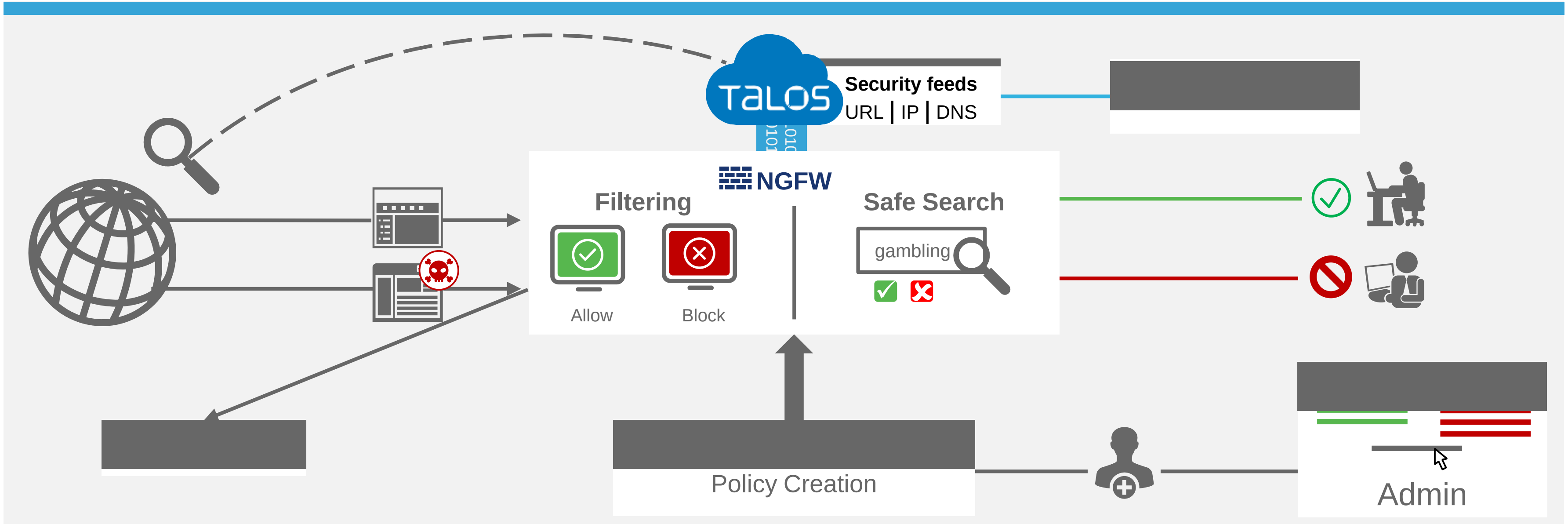
Decrypt **3.5 Gbps** traffic over **five million** simultaneous flows

Inspect deciphered packets

Track and log all SSL sessions

Block or allow access to URLs and domains

Web controls



Classify **280M+** URLs

Filter sites using **80+** categories

Manage “allow/block” lists easily

Block latest malicious URLs

Stop known threats from getting in

Security Intelligence

TALOS

URL Based

Block risky sites using a classified database of

270 million+

known URLs

IP Based

Filter out bad IPs using a blacklist of

70,000+

known IPs

DNS Based

Get real-time threat intelligence based on

80 billion+

daily DNS requests

Understand risks using reputation scoring

See more through industry-leading research

Get real-time protection against global threats

Talos

TALOS

Threat Intelligence

1.5 million daily malware samples

600 billion daily email messages

16 billion daily web requests

Security Coverage

Endpoints

WWW Web

Networks

NGIPS

Devices

Research Response

250+ Researchers

24 x 7 x 365 Operations

Identify advanced threats

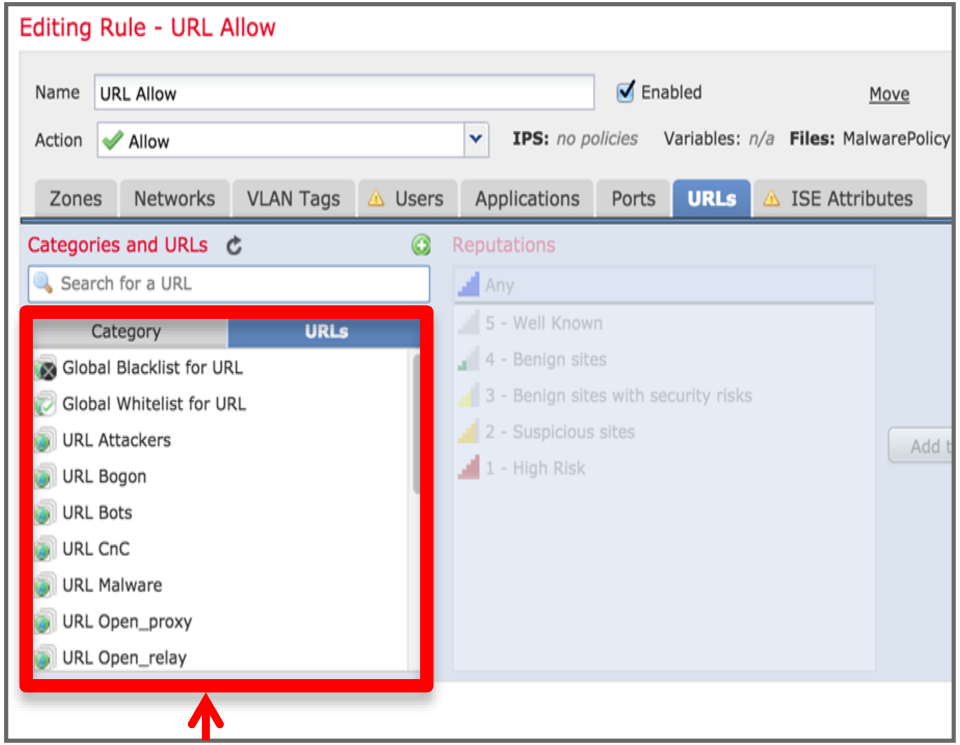
Get specific intelligence

Catch stealthy threats

Stay protected with updates

URL-Based Security Intelligence

- Extension of IP-based SI
- TALOS dynamic feed, 3rd party feeds and lists
- Multiple categories: Malware, Phishing, CnC,…
- Multiple Actions: Allow, Monitor, Block, Interactive Block,…
- Policy configured via Access Rules or black-list
- IoC tags for CnC and Malware URLs
- New Dashboard widget for UR SI
- Black/White-list URL with one click



Editing Rule - URL Allow

Name: URL Allow ☑ Enabled Move

Action: ✓ Allow IPS: *no policies* Variables: *n/a* Files: MalwarePolicy

Categories and URLs

Search for a URL

Category	URLs
Global Blacklist for URL	
Global Whitelist for URL	
URL Attackers	
URL Bogon	
URL Bots	
URL CnC	
URL Malware	
URL Open_proxy	
URL Open_relay	

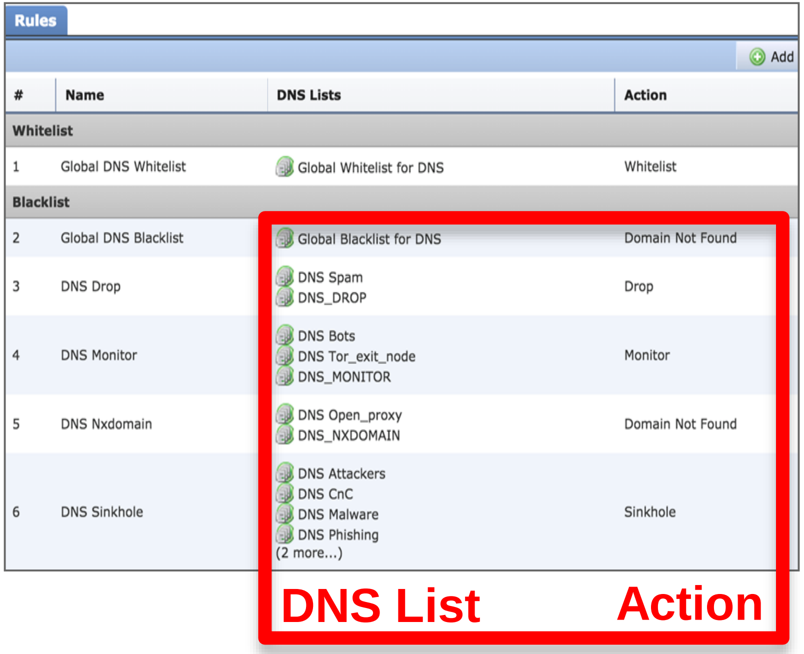
Reputations

- Any
- 5 - Well Known
- 4 - Benign sites
- 3 - Benign sites with security risks
- 2 - Suspicious sites
- 1 - High Risk

URL-SI Categories

DNS Inspection

- Security Intelligence support for domains
- Addresses challenges with fast-flux domains
- Cisco provided and user defined DNS lists: CnC, Spam, Malware, Phishing
- Multiple Actions: Block, Domain Not Found, Sinkhole, Monitor
- Indications of Compromise extended with DNS Security Intelligence
- New Dashboard widget for DNS SI



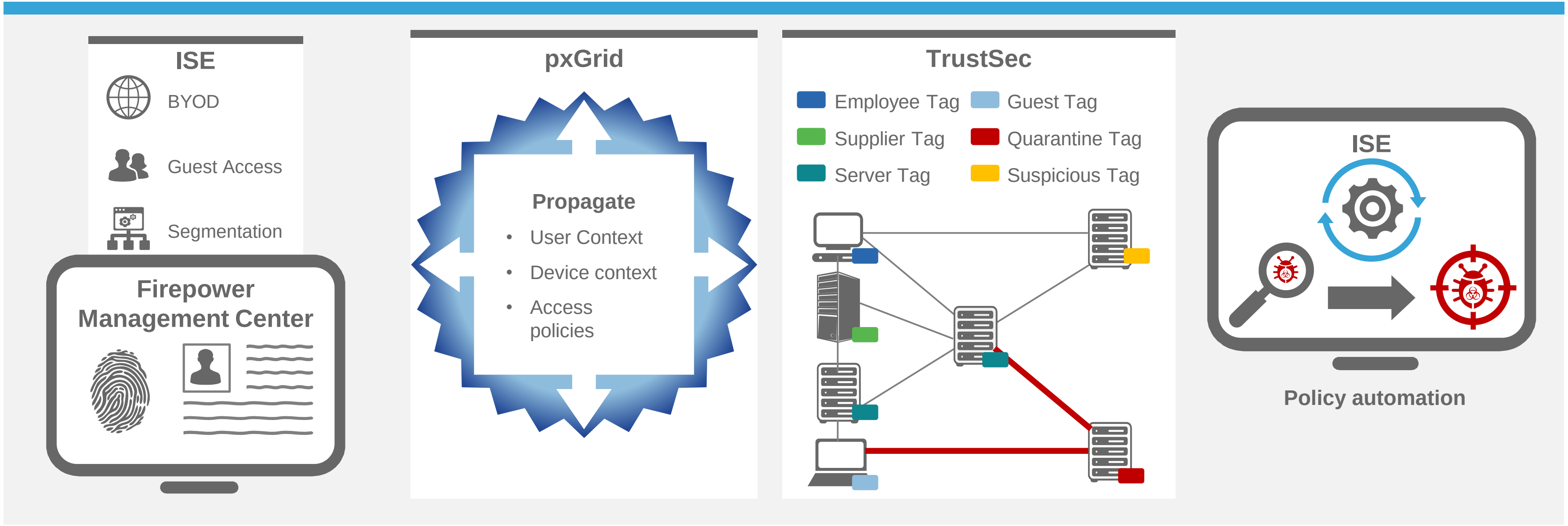
#	Name	DNS Lists	Action
Whitelist			
1	Global DNS Whitelist	Global Whitelist for DNS	Whitelist
Blacklist			
2	Global DNS Blacklist	Global Blacklist for DNS	Domain Not Found
3	DNS Drop	DNS Spam DNS_DROP	Drop
4	DNS Monitor	DNS Bots DNS Tor_exit_node DNS_MONITOR	Monitor
5	DNS Nxdomain	DNS Open_proxy DNS_NXDOMAIN	Domain Not Found
6	DNS Sinkhole	DNS Attackers DNS CnC DNS Malware DNS Phishing (2 more...)	Sinkhole

DNS List

Action

Ensure compliance before granting access

Identity Services Engine (ISE)



ISE

- BYOD
- Guest Access
- Segmentation

Firepower Management Center

pxGrid

Propagate

- User Context
- Device context
- Access policies

TrustSec

🟦 Employee Tag	🟦 Guest Tag
🟩 Supplier Tag	🟥 Quarantine Tag
🟦 Server Tag	🟨 Suspicious Tag

ISE

Policy automation

Set access control policies

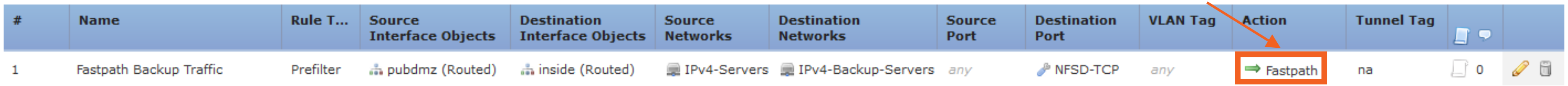
Propagate rules and context

Establish a secure network

Remediate breaches automatically

FTD Flow Offload

- Trusted flow processing with limited security visibility
  - Maximize single-flow throughput and packet rate, minimize latency
  - High performance compute, frequency trading, demanding data center applications
- Static hardware-based offload in Smart NIC for FTD
  - Automatically enabled when rule in Prefilter Policy uses the Fastpath action



#	Name	Rule T...	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Tag		
1	Fastpath Backup Traffic	Prefilter	pubdmz (Routed)	inside (Routed)	IPv4-Servers	IPv4-Backup-Servers	any	NFSD-TCP	any	Fastpath	na	0	

  - Targeting 30Gbps+ per single flow (TCP/UDP) and 2.9us of 64-byte UDP latency
  - Unicast IPv4 TCP/UDP/GRE and VLAN encapsulation only, no CMD/SGT
- Conditional offloading and selective inspection in the future

Management Platform Options

Easily manage NGFWs across multiple sites

Firepower Management Center

Centralized management for multi-site deployments

- Multi-domain management
- Role-based access control
- High availability
- APIs and pxGrid integration
- Firewall & AVC
- NGIPS
- AMP
- Security Intelligence

…Available in physical and virtual options

Manage across many sites

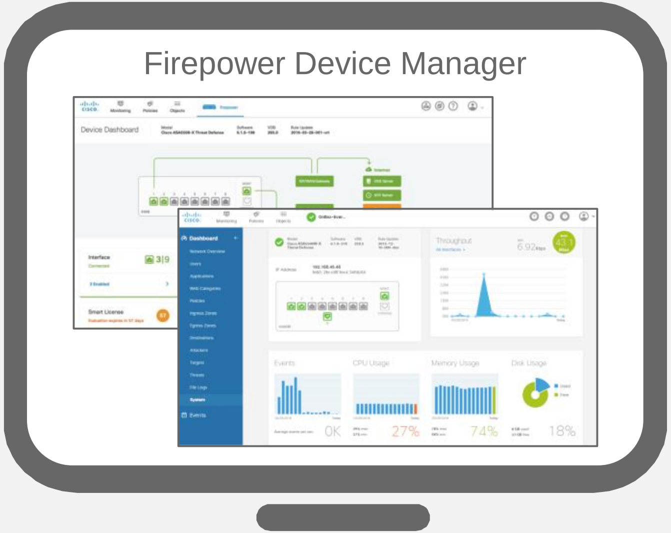
Control access and set policies

Investigate incidents

Prioritize response

Easily manage individual NGFWs

Firepower Device Manager



Integrated on-box option for single instance deployment

- Easy set-up
- Role-based access control
- High availability
- Physical and virtual options
- NAT and Routing
- Intrusion and Malware prevention
- Device monitoring
- VPN support

Set up easily

Control access and set policies

Investigate incidents

Prioritize response

New Capabilities in 6.1 Release

New capabilities in 6.1

Enterprise Management

Geo-location + Whois lookup

AMP Private Cloud

FMC HA

ISE remediation

Interface objects

REST API

VDI User Input API

KVM Virtualization Support

Integrated risk reports

Event QoS

Threat Innovation

True-IP Policy

SSL ClientHello

YouTube EDU enforcement

Safe Search Enforcement

Active authentication enhancements

Citrix VDI Authentication

Common Across Firepower Platforms

Unified Image

Inline Security Group Tags (SGT)

Shared NAT

Rate limiting
Prefilter Policies

Site-to-site VPN support
Routing enhancements

Firepower Device Manager (on box manager)

Traffic Rate Limiting

Threat Defense Only

Available in multiple deployment options

Physical, virtual, and cloud options

- AWS
- Azure

Also available as standalone solutions

NGIPS only

Dedicated AMP

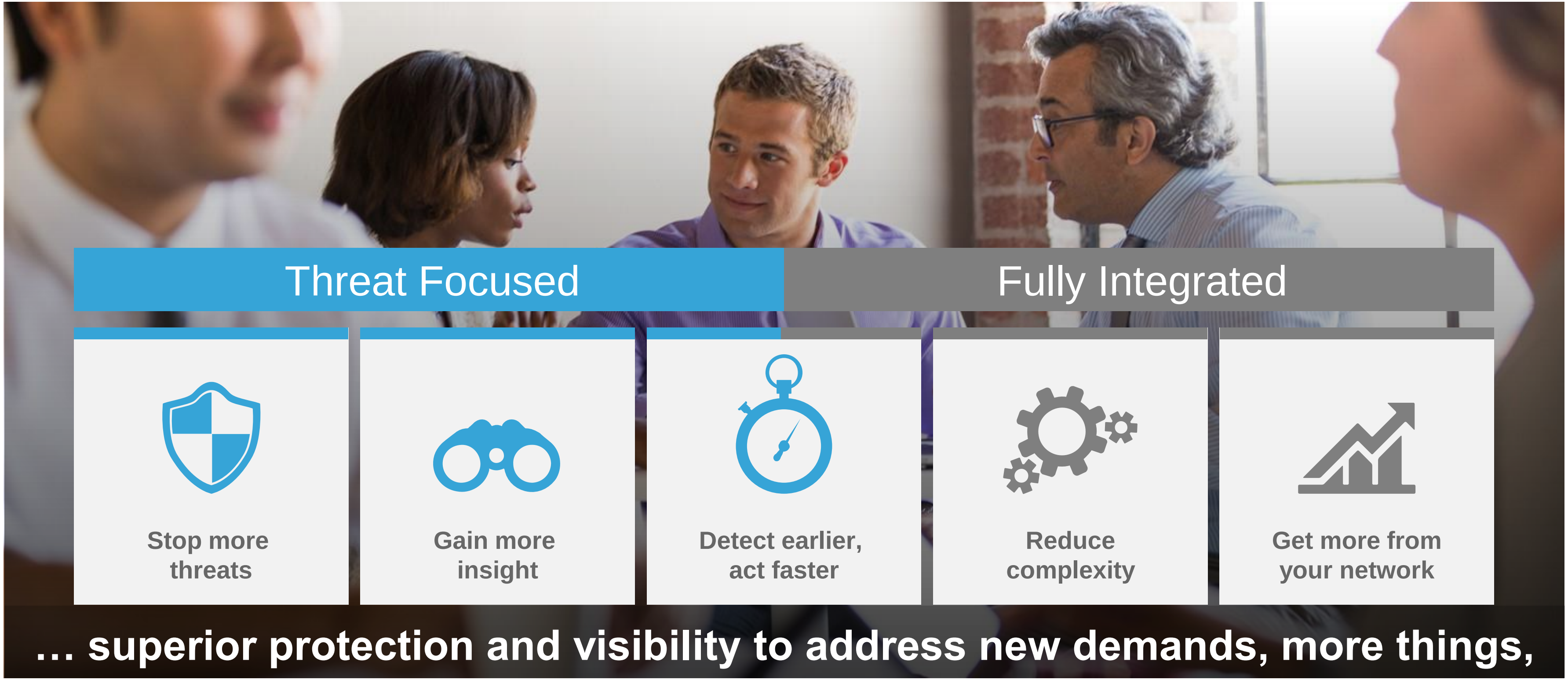
And on high-end performance appliances…

Cisco Firepower™ 4100 Series and 9300

Cisco Firepower Threat Defense on ASA 5500-X

Cisco FirePOWER™ Services on ASA 5585-X

Only Cisco delivers…



Threat Focused

Fully Integrated

- Stop more threats
- Gain more insight
- Detect earlier, act faster
- Reduce complexity
- Get more from your network

… superior protection and visibility to address new demands, more things,

Thank you