Intelligent Cybersecurity for the Real World

Christopher Young

Senior Vice President, Security Business Group

@youngdchris

The Security Problem
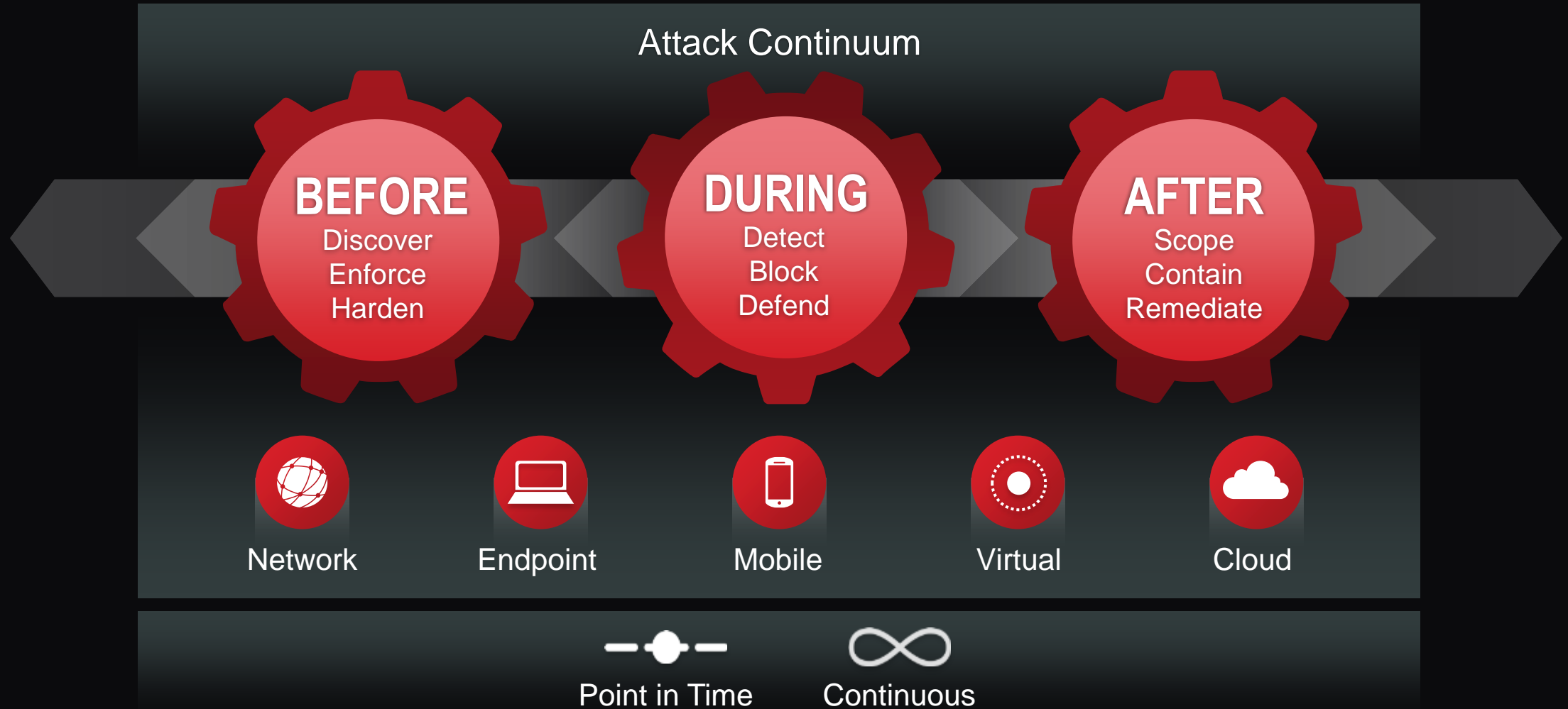

Changing
Business Models

Dynamic
Threat Landscape

Complexity
and Fragmentation

The New Security Model

Attack Continuum

BEFORE
Discover
Enforce
Harden

DURING
Detect
Block
Defend

AFTER
Scope
Contain
Remediate

Network

Endpoint

Mobile

Virtual

Cloud

Point in Time

Continuous

Cisco Acquires Sourcefire Customer Benefits

Increases Cisco's Security Depth and Talent

Accelerates delivery of Long Term Platform Strategy

TTM for Internet of Things Security Offers

Advanced Malware Protection - File Analysis

Rapid DC Integration (vIPS & vAVC)
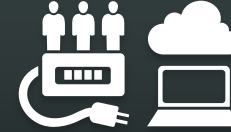
Strategic Imperatives

Visibility-Driven	Threat-Focused	Platform-Based
Network-Integrated, Broad Sensor Base, Context and Automation	Continuous Advanced Threat Protection, Cloud-Based Security Intelligence	Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network   Endpoint   Mobile   Virtual   Cloud
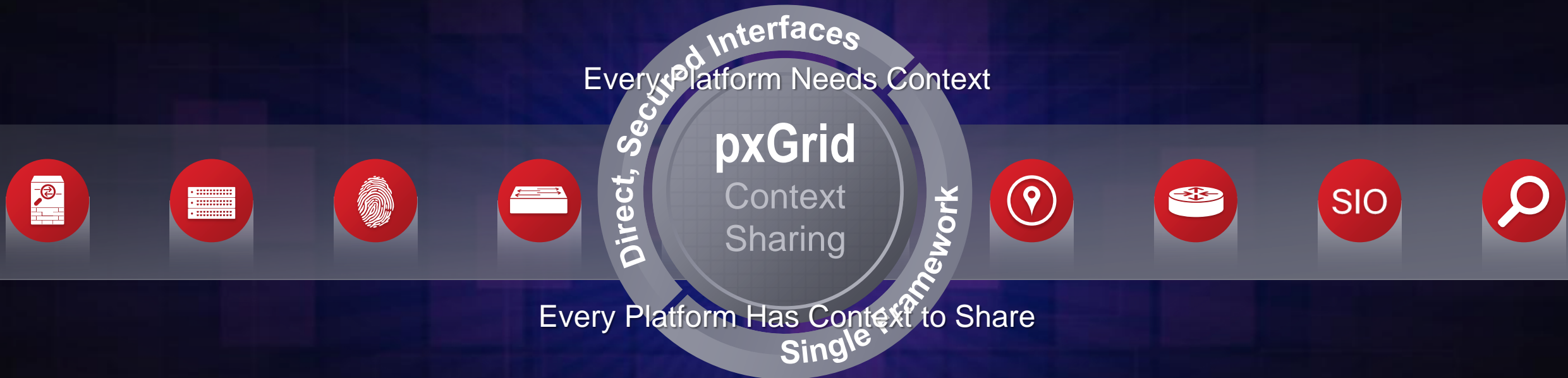
Cisco Sees More Than the Competition

Visibility-Driven: Threat and Context Intelligence Sharing

Every Platform Needs Context

Secured Interfaces

Direct, **Single Framework**

pxGrid

Context Sharing

Every Platform Has Context to Share

Visibility-Driven
Cisco Identity Services Engine (ISE)
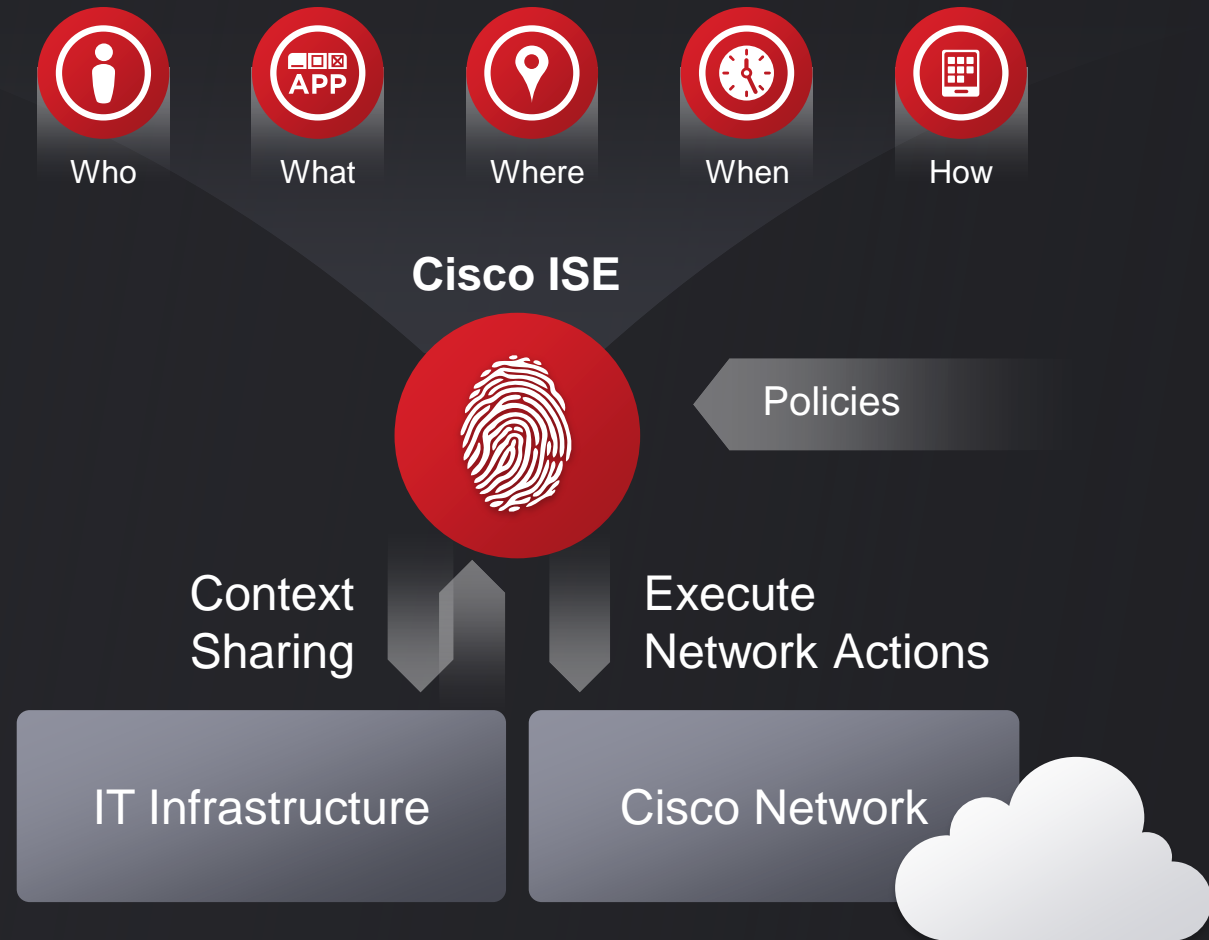
Benefits of ISE

Deep network and security insight

More granular control over BYOD
and sensitive users/groups

Clarify what network and security events
are important, and make them actionable

Unify policy silos

Scale to hundreds of thousands of endpoints

Who   What   Where   When   How

Cisco ISE

Policies

Context
Sharing

Execute
Network Actions

IT Infrastructure

Cisco Network

Threat-Focused

Detect, Understand, and Stop Threats

Who

What
APP

Where

When

How

Collective Security
Intelligence

?

Threat
Identified

Event History

Recorded

Context

ISE + Network, Appliances (NGFW/NGIPS)

Enforcement

AMP, CWS, Appliances

Continuous Advanced Threat Protection

Who

What

Where

When

How

Collective Security Intelligence

Event History

Context

ISE + Network, Appliances (NGFW/NGIPS)

Enforcement

AMP, CWS, Appliances

Continuous Analysis

AMP, Threat Defense

Today's Security Appliances

Traditional Firewall Functions

VPN Functions

Context-Aware Functions

IPS Functions

Malware Functions
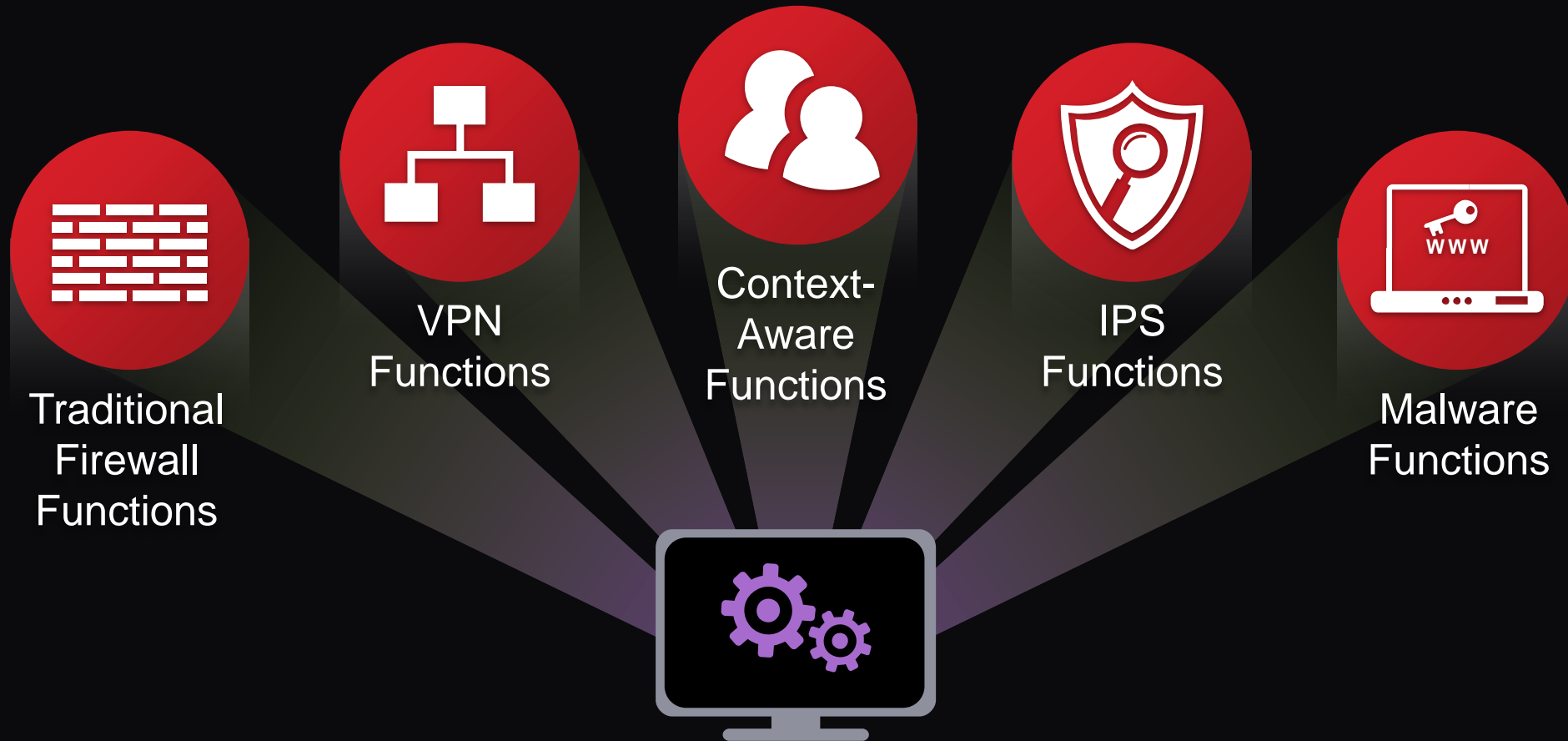
The Security Perimeter in the Cloud

Collective Security Intelligence

- Telemetry Data
- Threat Research
- Advanced Analytics

The Distributed Perimeter

Cloud Connected Network

- Mobile
- Router
- Firewall

3M+
Cloud Web Security Users

6 GB
Web Traffic Examined, Protected Every Hour

75M
Unique Hits Every Hour

10M
Blocks Enforced Every Hour

Develop Ecosystems for Cisco Security

Partner to Deliver Complete Solutions
Mobility (MDM), Threat (SIEM), Cloud

Develop SSP Partner Ecosystem
Open Platform Architecture Enables

Embed Security in Broader IT Solutions
ISE as "Context Directory Service"

Drive the Value of the Network
Lancope, Network as a Sensor

Cisco Current Partner Ecosystem

CITRIX®
Mobile Iron®
SAP®
Lancope — Network Performance + Security Monitoring™
TIBCO® — The Power of Now®
MaaS360® by Fiberlink
splunk>
Good
RAPID7
QUALYS®
airwatch™
Symantec™
IBM
HP
ArcSight
LogRhythm
Q1 Labs
NETSCOUT®

security is core to the
fabric @ cisco

ACI Announcement

APPLICATION-CENTRIC INFRASTRUCTURE

NEXUS 9000 SERIES

APPLICATION POLICY INFRASTRUCTURE CONTROLLER

INDUSTRY LEADING ECOSYSTEM
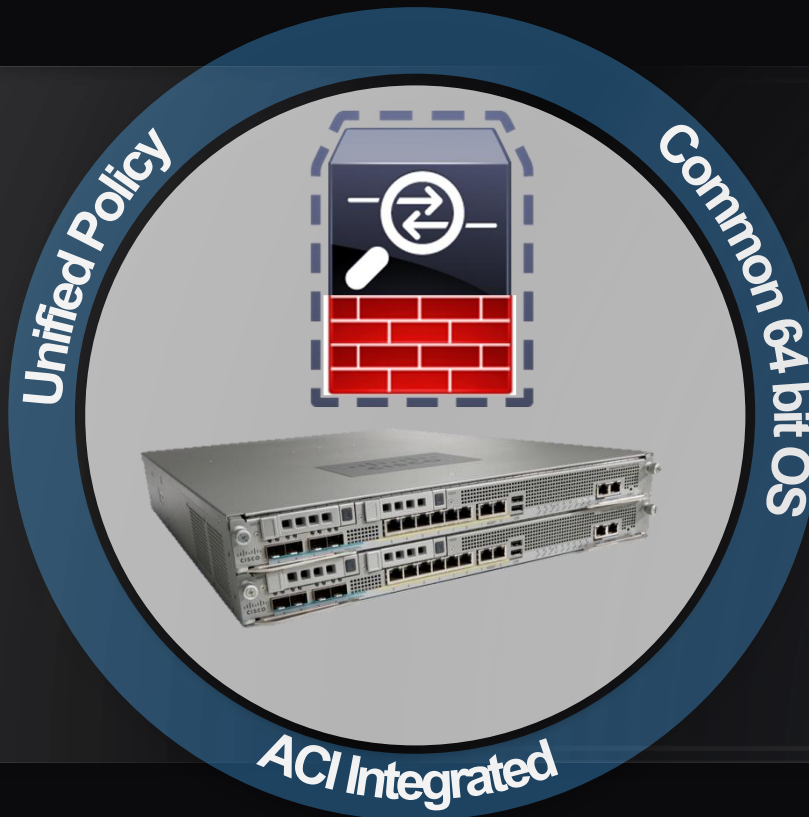
OPEN STANDARDS OPEN SOURCE

ACI Security Starts with the ASA

ASA

VIRTUAL

PHYSICAL

vmware® KVM

Xen Microsoft Hyper-V

ASAv

Full ASA Feature Set
Hypervisor Independent
Virtual Switch Agnostic
Dynamic Scalability

Unified Policy

Common 64 bit OS

ACI Integrated

ASA 5585-X

16 Way Clustering with
State Synchronization
Scalable to **640Gbps**

Available in 1HCY14

New Open Specification on TrustSec

Network Access Control and Segmentation Technology

Customer Problems

Expanding Attack Surface (Mobility, Virtualization, APTs, IoT)

Security Changes = Complex Network Re-Architecture

Managing Volumes of Firewall Rules and ACLs

What TrustSec Solves

Secure/Segment the Network Against Unauthorized Access

Business Assets Map to Simple and Automated Access Policies

Automated FW/ACL Policy Administration for Granting Access

Policy Defined by Business Asset

Source	Protected Assets		
	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Network Embedded Enforcement

Switch   Router   DC FW   DC Switch

Flexible and Scalable Policy Enforcement

TrustSec 4.0 Supports Full Data Center, Campus and Branch Deployments

Thank You