Cisco *Threat Centric Security Model*

Joey Kuo
安全事業部　產品經理

Jan 2015

Threat Centric Security Model is Needed

Defend, Discover, Remediate against Threats

The Threat Centric Security Model

Looking beyond a single silver bullet

- Firewall - ASA
- NGFW – ASA with Firepower
- ISE
- UTM - Meraki

- NGIPS - SourceFire
- Ironport Web Security
- Ironport Email Security

- Advanced Malware Protection - AMP
- Network Behavior Analysis - StealthWatch

‘Defense-in-Depth’ Security Alone Is Not Enough

Siloed Approach

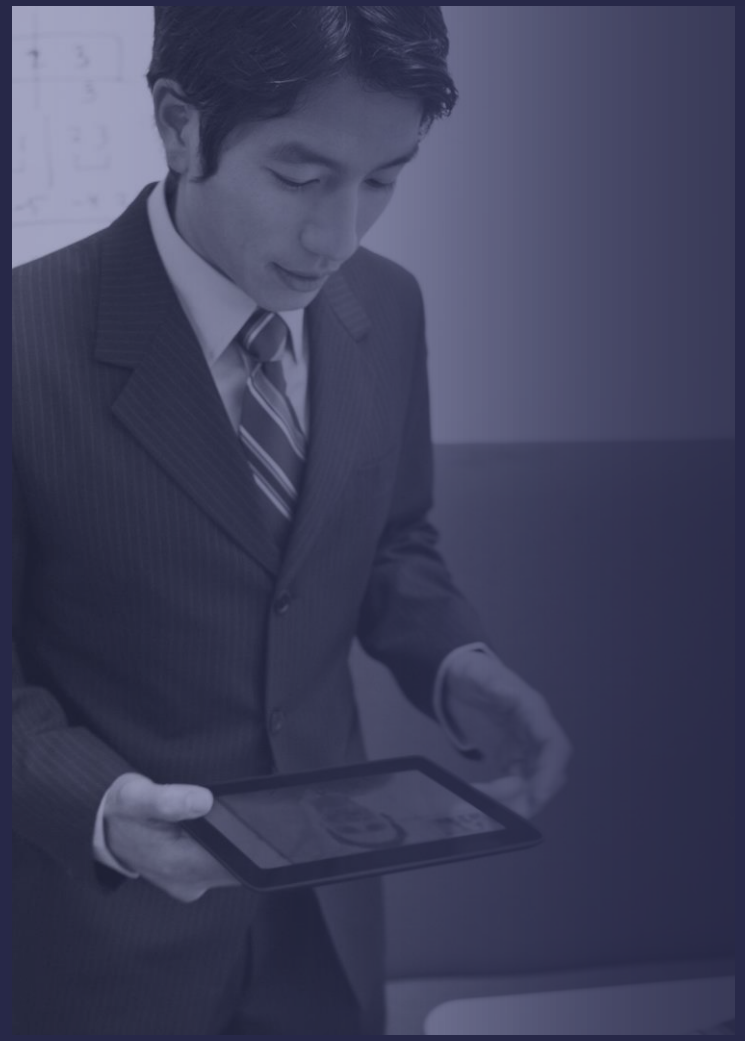
Increased complexity and reduced effectiveness

Poor Visibility

Undetected multivector and advanced threats

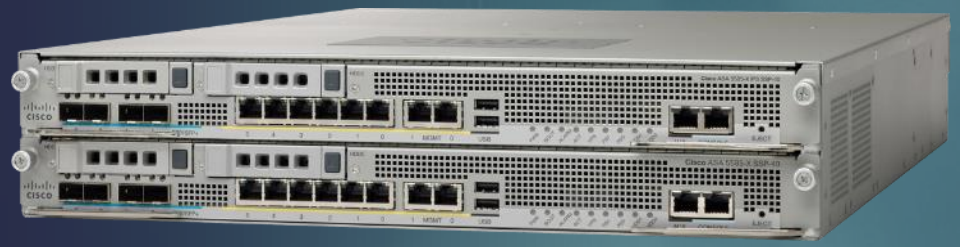
Manual and Static

Slow, manual inefficient response



Industry’s First Threat-Focused NGFW

ASA with Firepower



#1 Cisco Security announcement of the year!

Proven Cisco ASA firewalling

+

Industry leading NGIPS and AMP

=

Cisco ASA with FirePOWER Services

- *Integrating* defense layers helps organizations get the best visibility
- Enable dynamic controls to automatically adapt
- Protect against advanced threats across the entire attack continuum

The Problem with Legacy Next-Generation Firewalls

Focus on the Apps…	…but miss the threat

Legacy NGFWs can reduce attack surface area but advanced malware often evades security controls.

Superior Integrated & Multilayered Protection

World's most widely deployed, enterprise-class ASA stateful firewall

Granular Cisco® Application Visibility and Control (AVC)

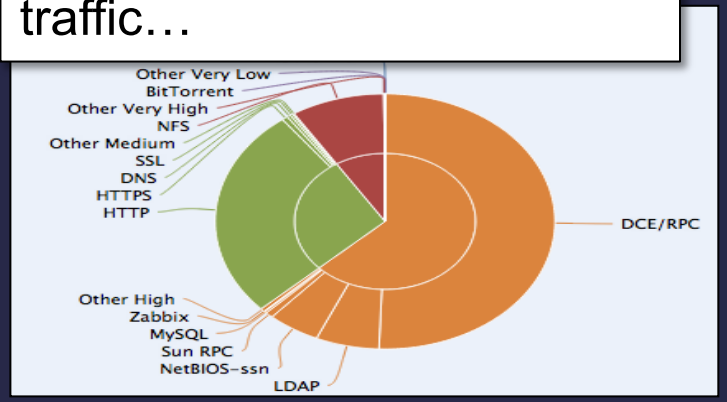
Industry-leading FirePOWER next-generation IPS (NGIPS)

Reputation- and category-based URL filtering

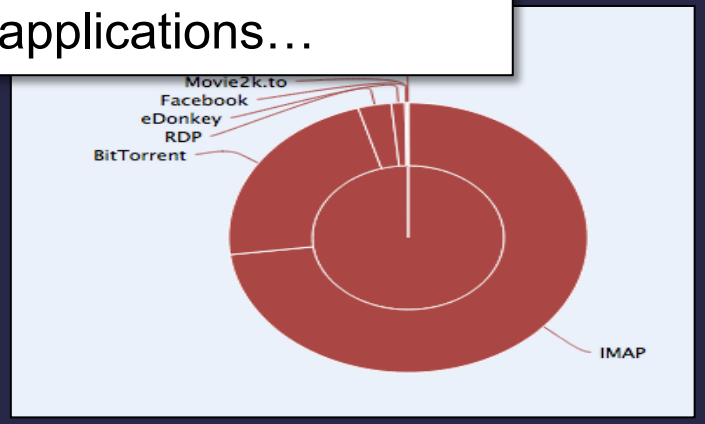
Advanced malware protection

Visibility (可視性） - See Everything

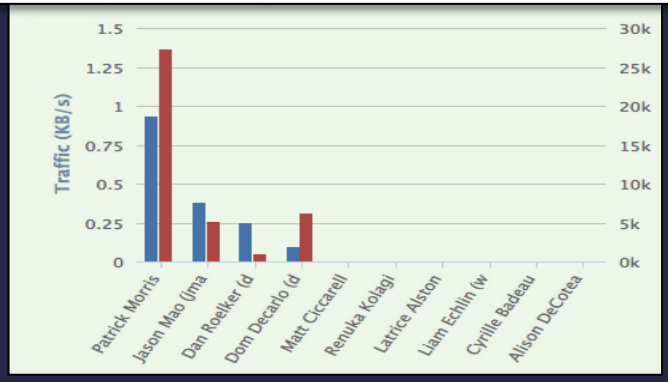
Browse all application traffic…



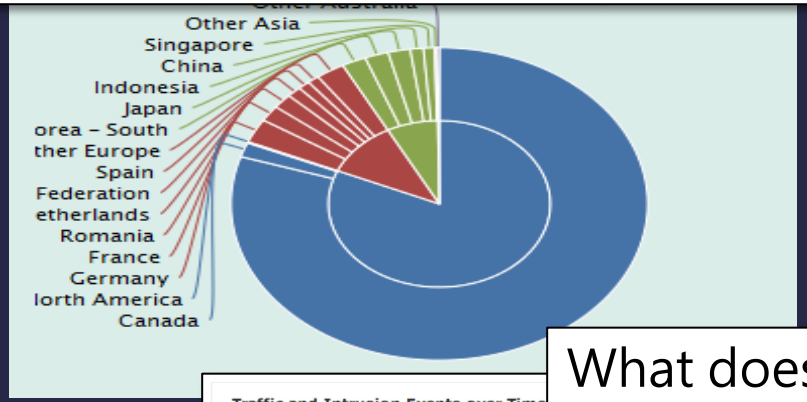
Look for risky applications…



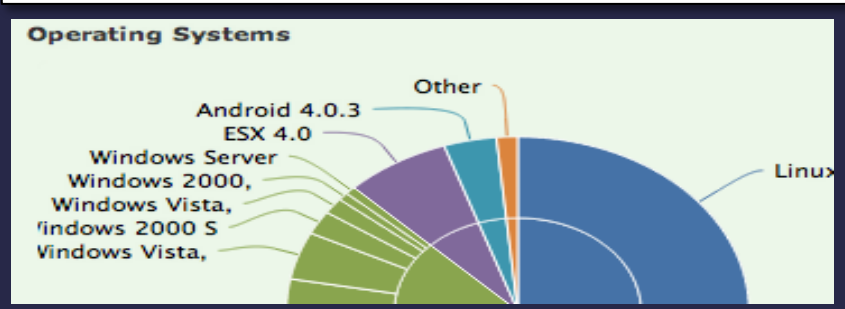
Who is using them?



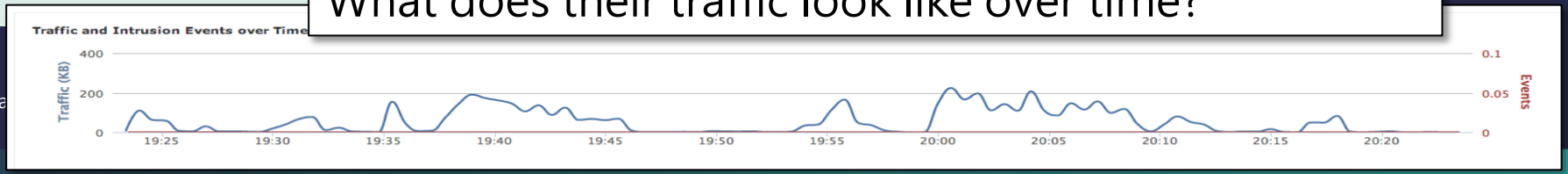
Connections by Initiator Country



On what operating systems?



What does their traffic look like over time?



Visibility (可視性） - Application Control

Control access for applications, users and devices

"Employees may view Facebook, but only Marketing may post to it"

"No one may use peer-to-peer file sharing apps"

Over 3,000 apps, devices, and more!

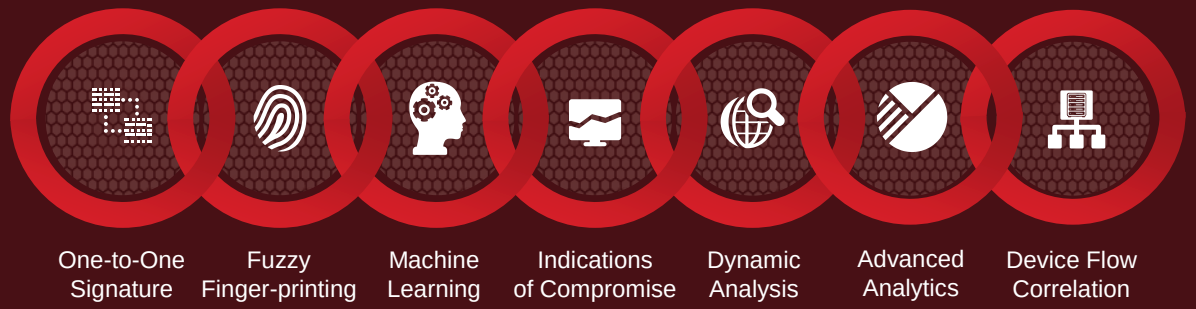
Advance Persistence Threat / Advanced Malware

Is now a tool for financial gain

- Uses formal Development Techniques
  - Sandbox aware
  - Quality Assurance to evade detection
  - 24/7 Tech support available
- Has become a math problem
  - End Point AV Signatures ~20 Million
  - Total KNOWN Malware Samples ~100 M
  - AV Efficacy Rate ~50%

Retrospective (可回朔）持續分析　及 Point-in-Time Detection 一次性偵測

Point-in-Time Detection



File Reputation & Sandboxing

Retrospective Security

Breadth and Control points:

- Email
- Network
- Endpoints
- IPS
- Web
- Devices

Telemetry Stream

- File Fingerprint and Metadata
- File and Network I/O
- Process Information

Continuous feed

Continuous Analysis

Overview | Analysis | Policies | Devices | Objects | FireAMP

Context Explorer | Connections ▾ | Intrusions ▾ | Files ▸ Network File Trajectory | Hosts ▾ | Users ▾ | Vulnerabilities ▾

Network File Trajectory for 0517f034...588e1374

File SHA-256	0517f034...588e1374	**First Seen**	
File Name	WindowsMediaInstaller.exe	**Last Seen**	
File Type	MSEXE	**Event Count**	
File Category	Executables	**Seen On**	
Current Disposition	Malware	**Seen On Breakdown**	
Threat Score	●●●○ High		

Trajectory

Time 2013-12-06 18:17:27
Event Type File Sent
IP Address 10.4.10.183
Blocked Recipient 10.5.11.8
File Name WindowsMediaInstaller.exe
Disposition Malware
Action Malware Block
Application Protocol HTTP
Client Firefox

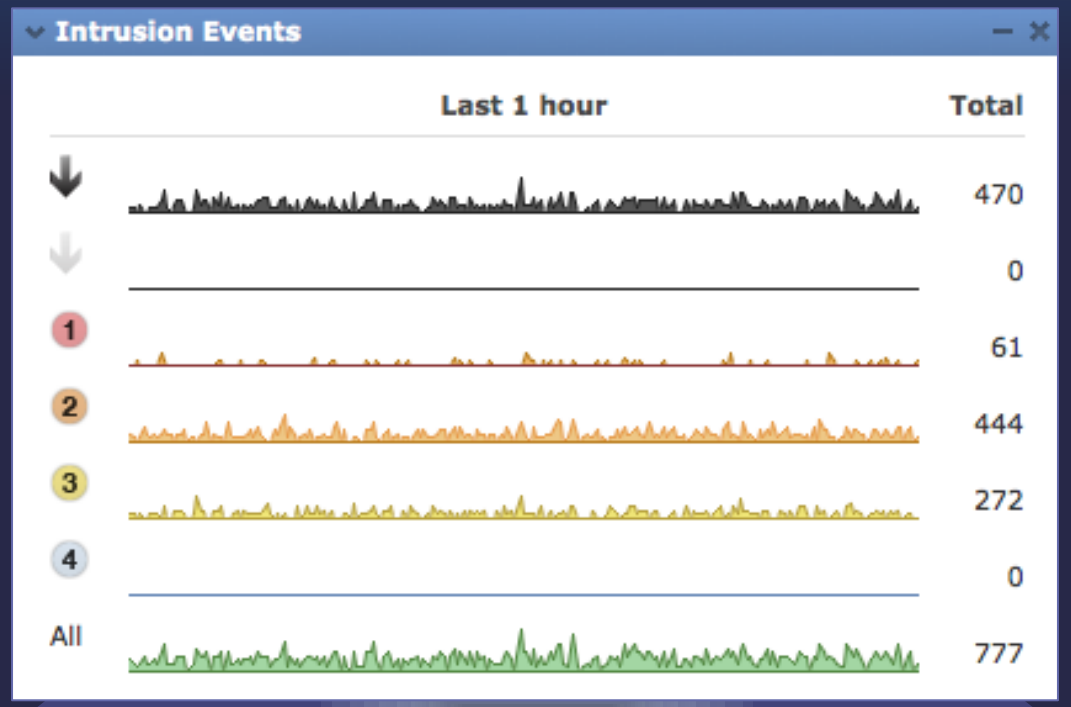
Events Transfer | Block | Create | Move | etrospective | Quarantine

Dispositions Unknown | Malware | Clean | Custom | Unavailable

8 hours after the first attack, the Malware tries to re-enter the system through the original point of entry but is recognized and blocked.

Correlation & Automation (自動化及關聯分析)
Cost Saving

Correlates all intrusion events
to an impact of the attack against the target



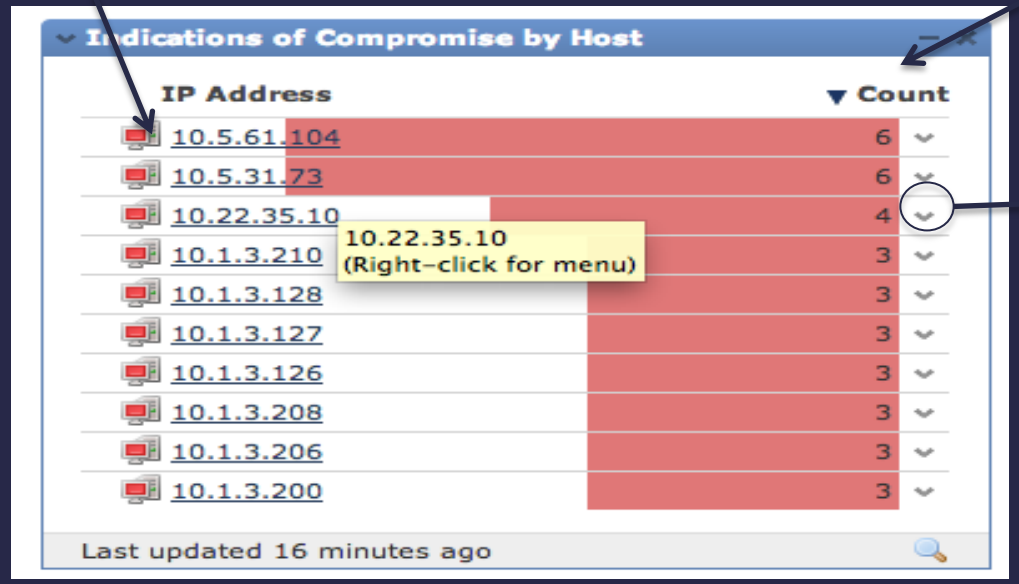
Impact Flag	Administrator Action	Why
1	Act immediately, vulnerable	Event corresponds to vulnerability mapped to host
2	Investigate, potentially vulnerable	Relevant port open or protocol in use, but no vuln mapped
3	Good to know, currently not vulnerable	Relevant port not open or protocol not in use
4	Good to know, unknown target	Monitored network, but unknown host
0	Good to know, unknown network	Unmonitored network

Indicators of Compromise (感染指標）Dashboard

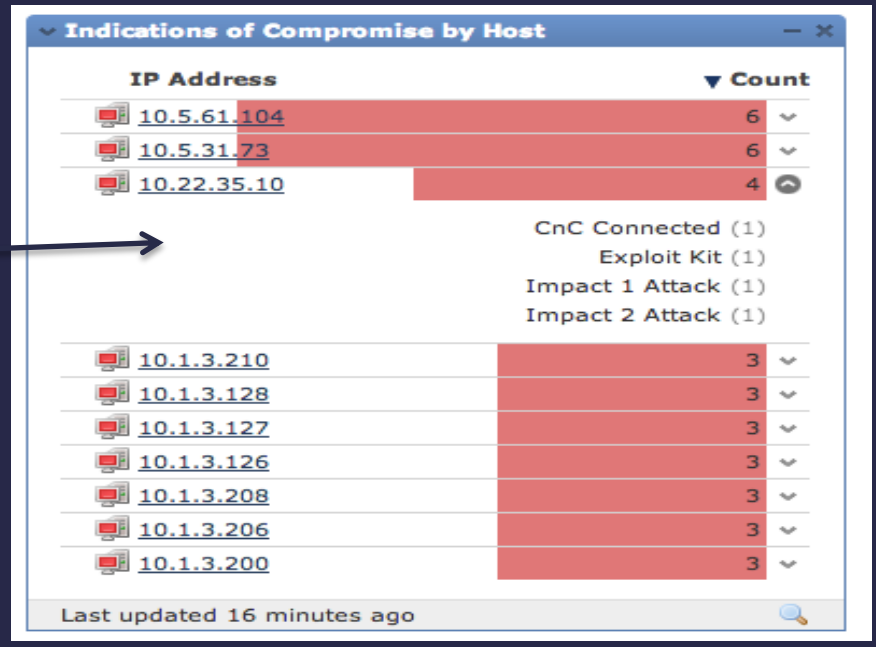
Because IOCs enable a quick way of classifying a host’ s potentially compromised state, having this data on a dashboard is desirable

Host

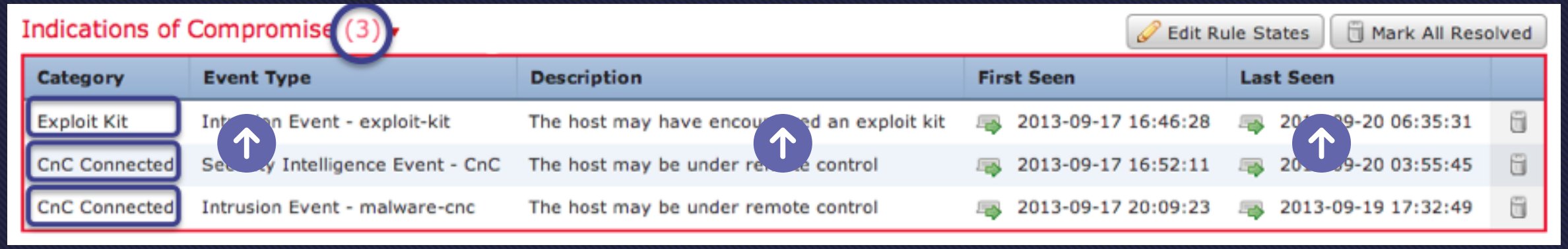
Number of IOCs set against the host



Click to expand



Indications of Compromise (IoCs)

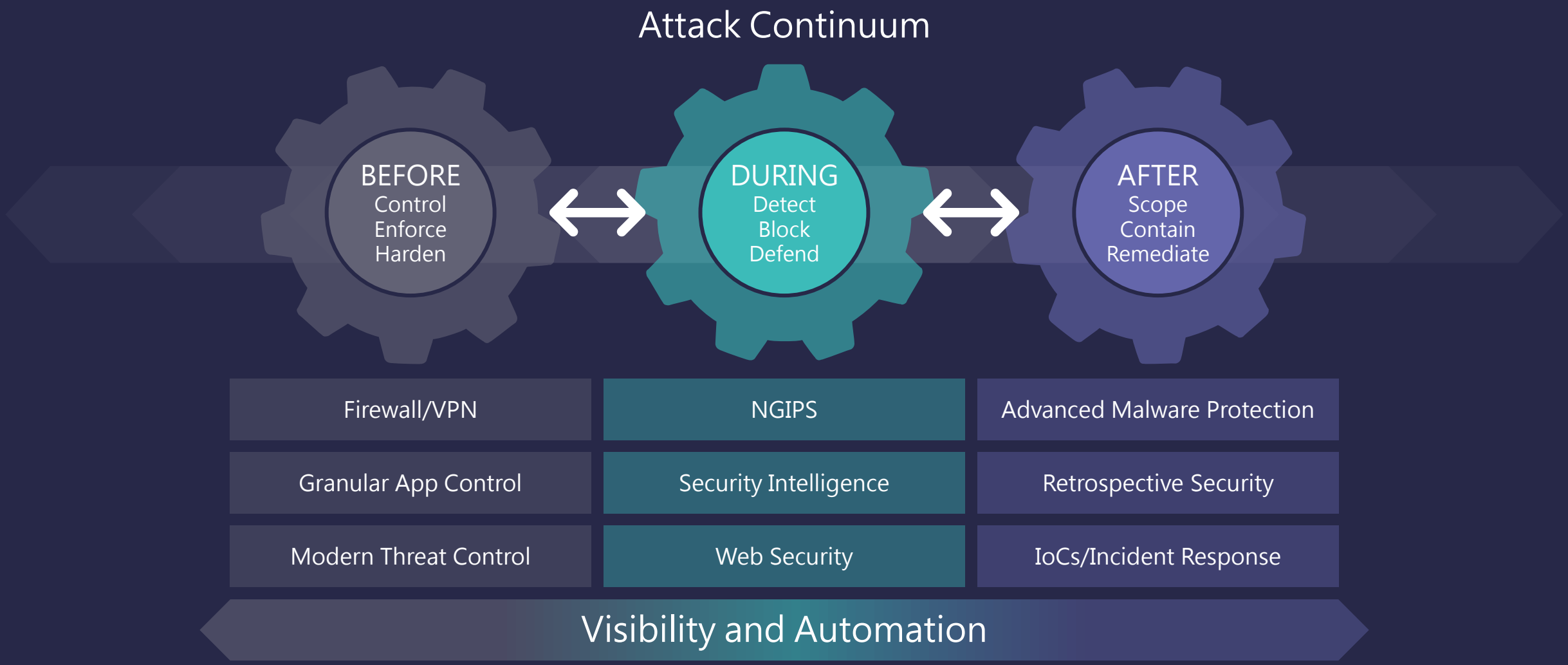


Exploit Kits
Web App Attacks
CnC Connections
Admin Privilege Escalations

to Known CnC IPs

Office/PDF/Java Compromises
Malware Executions
Dropper Infections

Integrated Threat Defense Across the Attack Continuum



Cisco ASA with FirePOWER Services

A New, Adaptive, Threat-Focused NGFW

Integrated Threat Defense
（威脅導向的新世代防火牆）

Best-in-class, multilayered protection
in a single device

Superior Visibility (可視性）

Full contextual awareness
to eliminate gaps

Automation （自動化）

Simplified operations and dynami
response and remediation

Retrospective （可回朔）

Cisco Advanced Malware Protection
Provide continuous analysis

How to Build Security Solution
Sourcefire on ASA with FireSIGHT Management Center

Customer Scenario

A medium to enterprise sized customer would like to purchase ASA with Sourcefire and a FireSIGHT Management Center.

They would like to order 1 additional ASA for backup/High Availability.

The Cisco Solution

Platform

- ASA FirePOWER Chassis
- Virtual FireSIGHT Management Center

Platform Support (SMARTnet)

- SMARTnet Support
- Software Support for Management Center

Content Subscriptions with Support (1 & 3 years)*

- ASA IPS+Apps License
- Advanced Malware Protection

SKUs for the Quote

2 ASA Bundles

1.0 ASA5585-S40F40-BUN
- 1.1 ASA5585-S40F40-K9
  - 1.1.0.1CON-SNT-A85S4F49
- 1.2 L-ASA5585-40-TAM=

1 Virtual FireSIGHT Management Center

2.0 FS-VMW-SW
- 2.0.1 CON-SAU-FS1500

Sourcefire on GPL NOW!!!

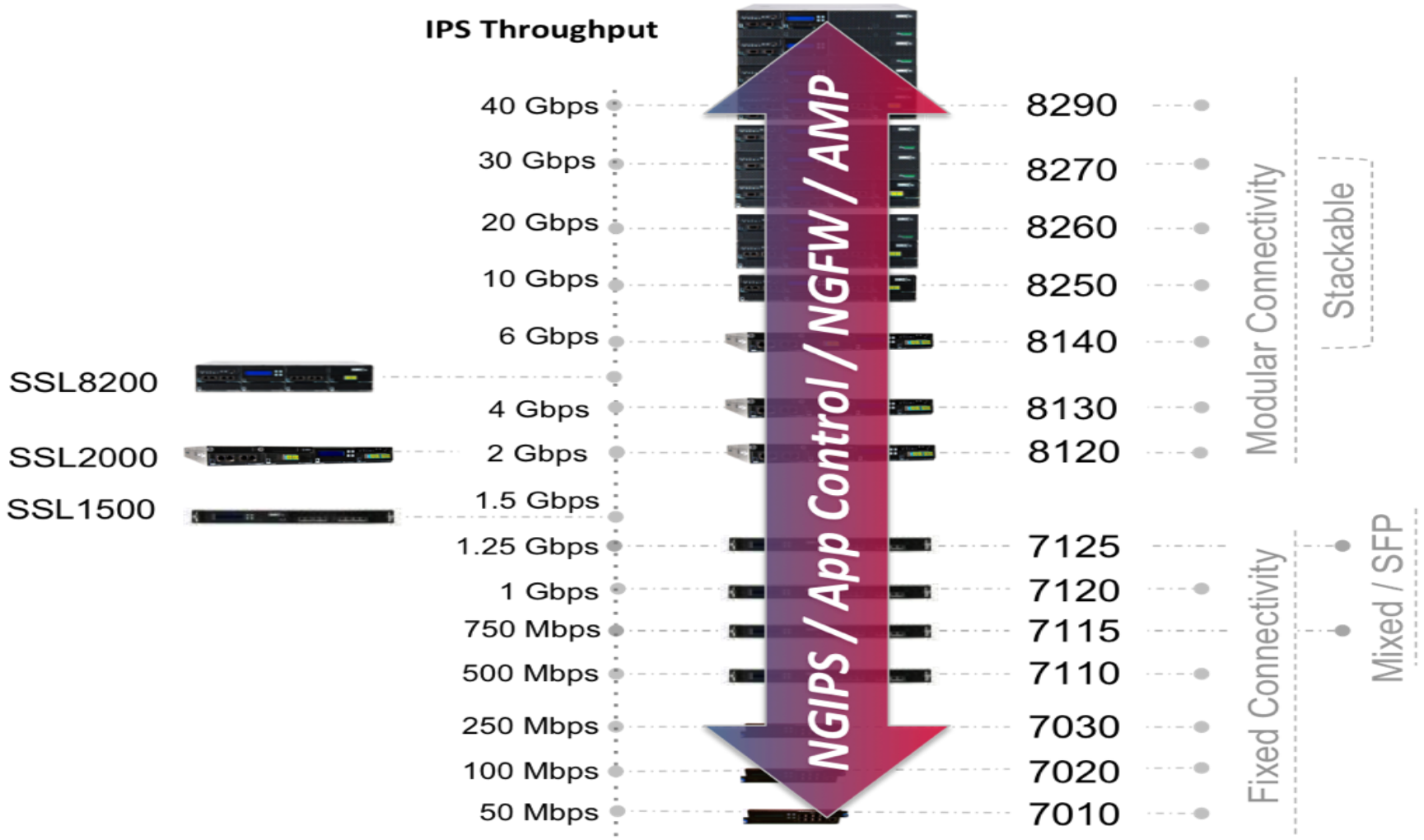
Sourcefire FirePOWER™

- Industry-best
  Intrusion Prevention
- Real-time
  Contextual Awareness
- Full Stack Visibility
- Intelligent Security Automation with FireSIGHT™
- Unparalleled Performance and Scalability
- Easily add Application Control, URL Filtering and Advanced Malware Protection with optional subscription licenses

FirePOWER™ Appliances Summary

All appliances include:

- Integrated lights-out management
- Sourcefire acceleration technology
- LCD display

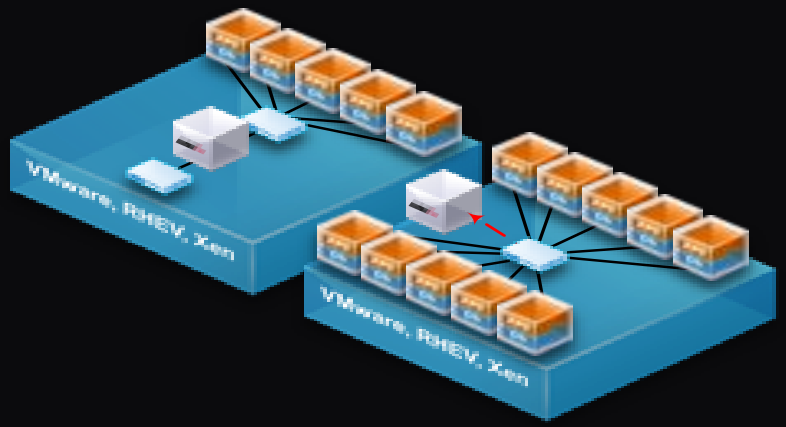


Fire Sight Appliances

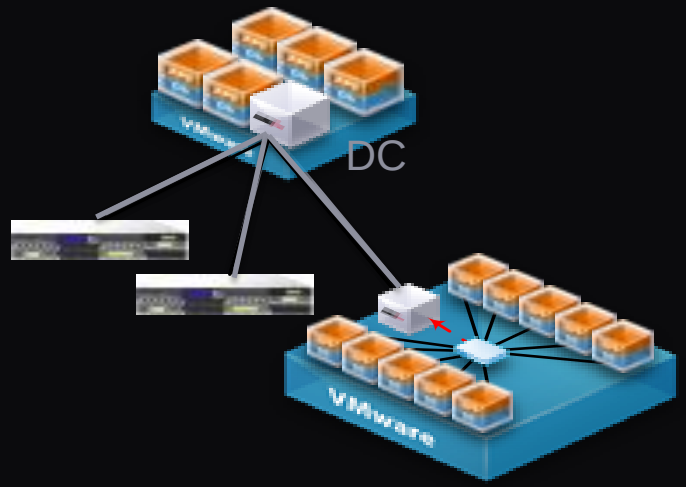
	FS750	FS1500	FS3500
Max. Devices Managed*	10	35	150
Max. IPS Events	20M	30M	150M
Event Storage	100 GB	125 GB	400 GB
Max. Network Map (hosts | users)	2k | 2k	50k | 50k	300k | 300k
Max. Flow Rate (flows/second)	2000 fps	6000 fps	10000 fps
High Availability Features	Lights-out Management (LOM)	RAID 1, LOM, High Availability pairing (HA)	RAID 5, LOM, HA, Redundant AC Power

* Max number of devices is dependent upon sensor type and event rate

Network Virtual Appliances



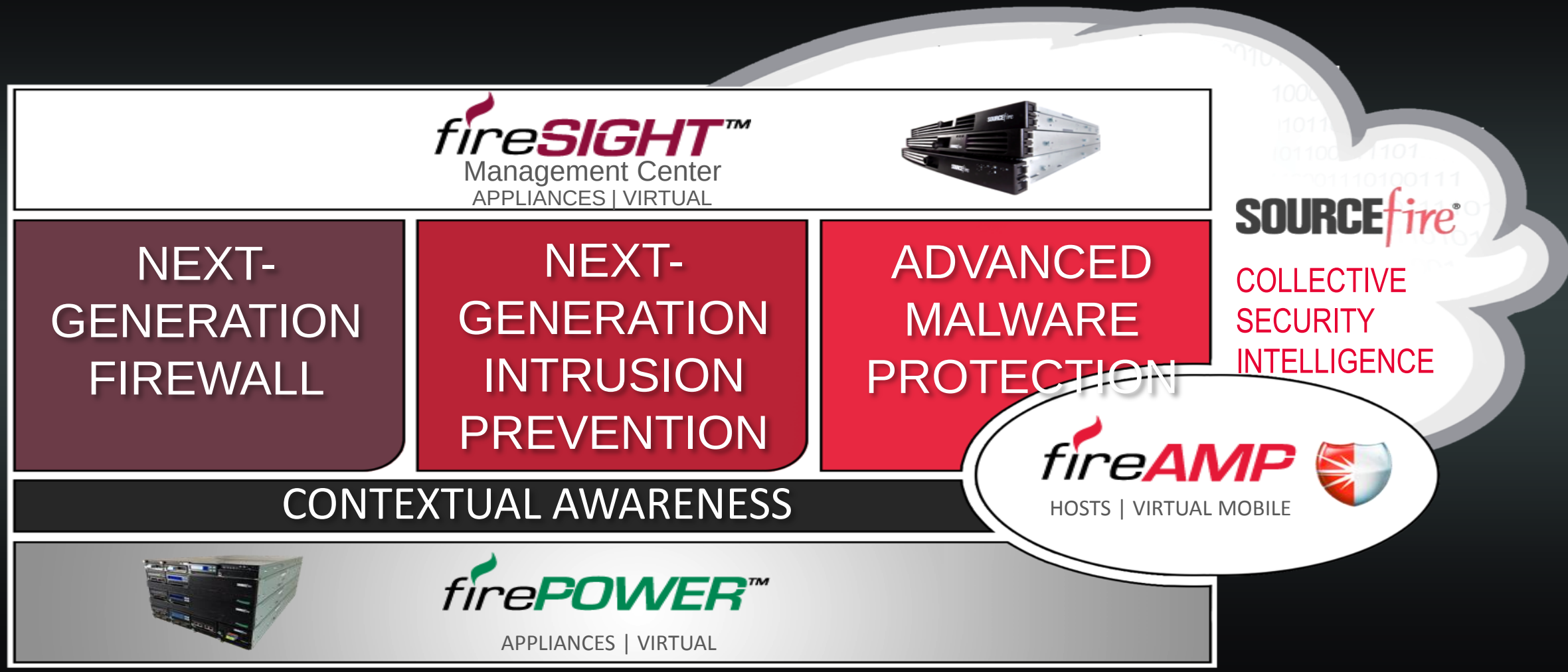
- Virtual Sensor
  - Inline or passive deployment
  - Full NGIPS Capabilities
  - Deployed as virtual appliance
  - Use Cases
    - SNORT Conversion
    - Small / Remote Sites
    - Virtualized workloads (PCI)



- Virtual Defense Center
  - Manages up to 25 sensors
    - physical and virtual
    - single pane-of-glass
  - Use Cases
    - Rapid Evaluation
    - Pre-production Testing
    - Service Providers

NOTE: Supports ESX(i) 4.x and 5.x on Sourcefire 5.x platforms. Supports RHEV 3.0 and Xen 3.3.2/3.4.2 on Soucefire 4.x platforms only.

Sourcefire's Security Solutions



How to Configure a Sample Security Order

How to Configure a Sample Security Order

Customer Scenario

A medium-sized customer with 3 different locations in the US needs to build a brand new Security solution.

They know they need an Intrusion Protection System and URL Filtering and would like 24x7 support. Given this is new technology, the customer doesn't have the knowledge, experience, or time to implement the solution successfully.

The Cisco Solution

Platform

- FirePOWER 7000 Appliance
- FireSIGHT Management Center

Platform Support (SMARTnet)

- SMARTnet Support
- Software Application Upgrades

Content Subscriptions with Support (1 & 3 years)*

- IPS+Apps and URL Filtering

Other Services

- Kickstart

SKUs for the Quote

1 Management Center
1.0 FS750-K9
1.0.1 CON-SNT-FS750
1.3 FS750-FSIGHT-LIC
1.3.0.1 CON-SAU-FS750

3 FirePOWER FP7010
2.0 FP7010-K9
2.0.1 CON-SNT-FP7010
3.0 FP7010-TAC-LIC=

Kickstart
4.0 ASF-CORE-FW-DEP

Cisco Identity Services Engine 1.3

Delivering Control with Context Across the Extended Network

Table 6. Cisco ISE Services, Licenses, and Software

Cisco ISE Feature or Service	License			
	Base	Plus	Apex	Mobility
Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass	Yes			Yes
Web authentication (local, central, device registration)	Yes			Yes
MACsec (all)	Yes			Yes
Guest portal and sponsor services	Yes			Yes
Representational state transfer (monitoring) APIs	Yes			Yes
External RESTful services (CRUD)-capable APIs	Yes			Yes
Security group tagging (Cisco TrustSec® SGT)	Yes			Yes
Profiling		Yes		Yes
Profiler feed service		Yes		Yes
Device registration (My Devices portal) and provisioning (for bring-your-own-device [BYOD] initiatives)		Yes		Yes
Context sharing (Cisco pxGrid)		Yes		Yes
Endpoint Protection Services (EPS)		Yes		Yes
Posture (endpoint compliance and remediation)			Yes	Yes
Enterprise mobility management and mobile device management (EMM and MDM) integration			Yes	Yes
Cisco AnyConnect Unified Agent (requires Cisco AnyConnect Apex license; see below)			Yes	Yes
Wired access control	Yes	Yes	Yes	
Under ATP control (Certified Partners)	Yes	Yes	Yes	

Cisco AnyConnect 4.0

Control with Context for Endpoint Access

November 2014

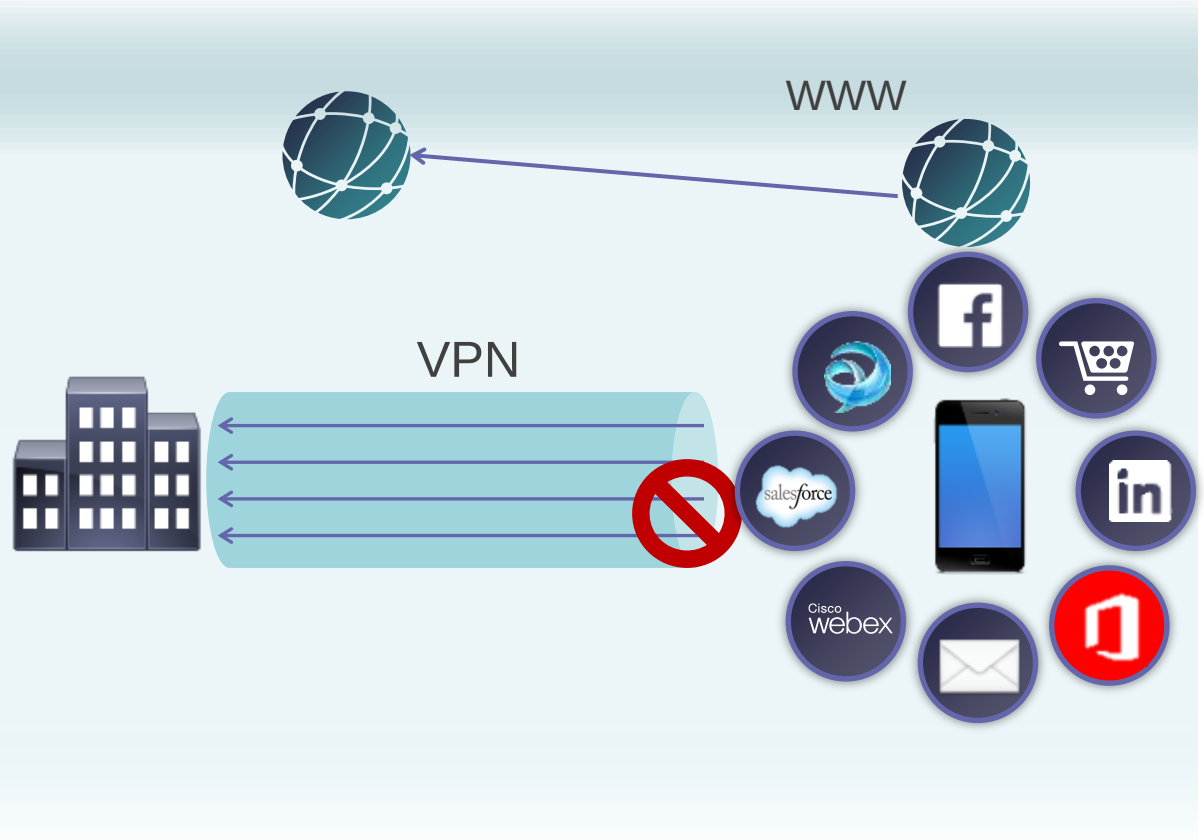
What's New in Cisco AnyConnect 4.0?

Connect Only Approved Applications over VPN

NEW

- Provide secure remote access for selected applications by user, role, device, etc. (per-app VPN)
- Reduce the potential for non-approved applications to compromise enterprise data
- Support a range of remote users and endpoints (employees, partners, contractors), streamlining IT operations

Selectively Tunnels Traffic Through VPN

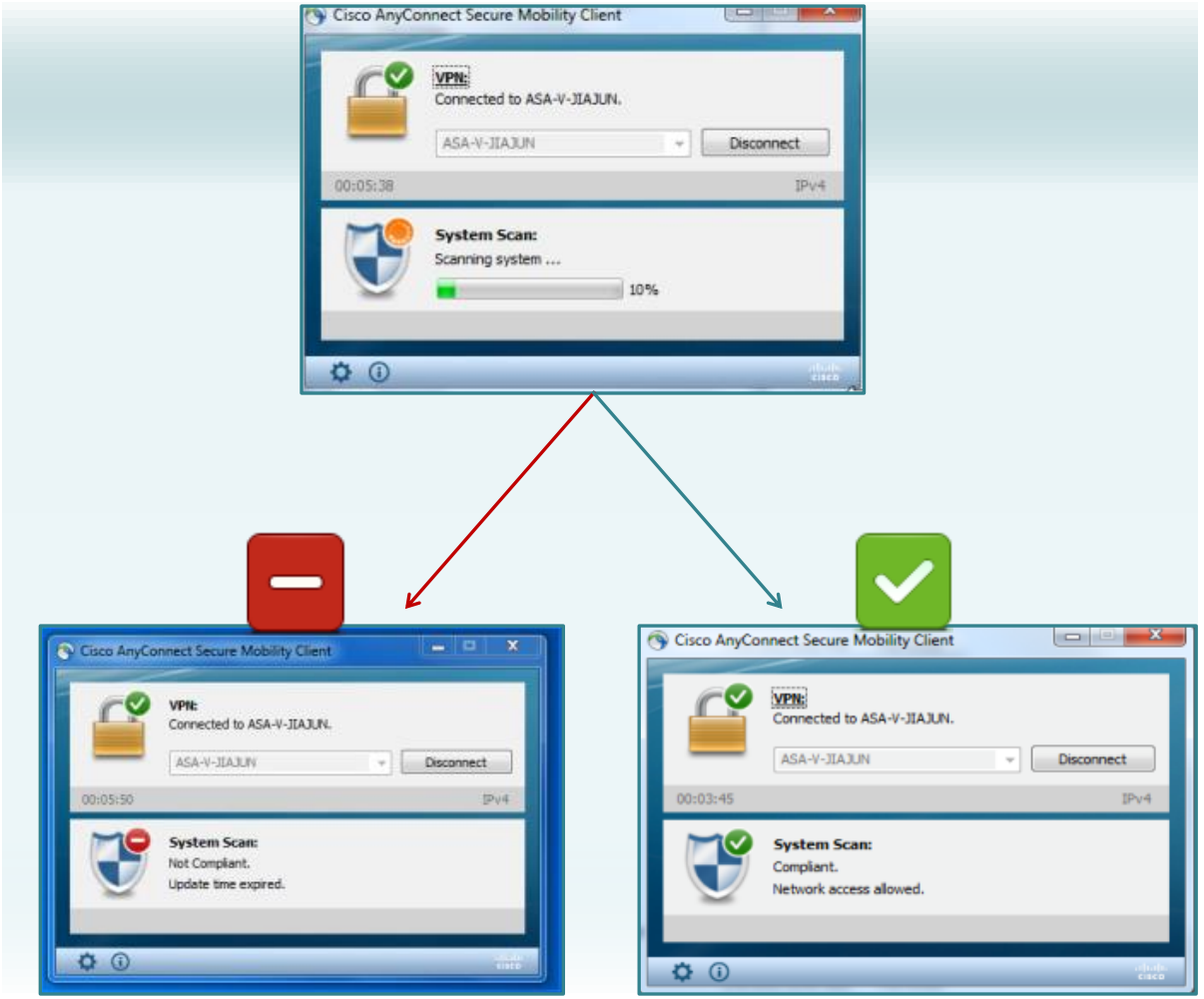


What's New in Cisco AnyConnect 4.0?

Posture Check and Secure VPN Access with Unified Agent and Cisco ISE 1.3

NEW

- Supports device posture and authorization across multiple access methods
- Simplifies management with only one agent to manage
- Prevents noncompliant devices from accessing the network

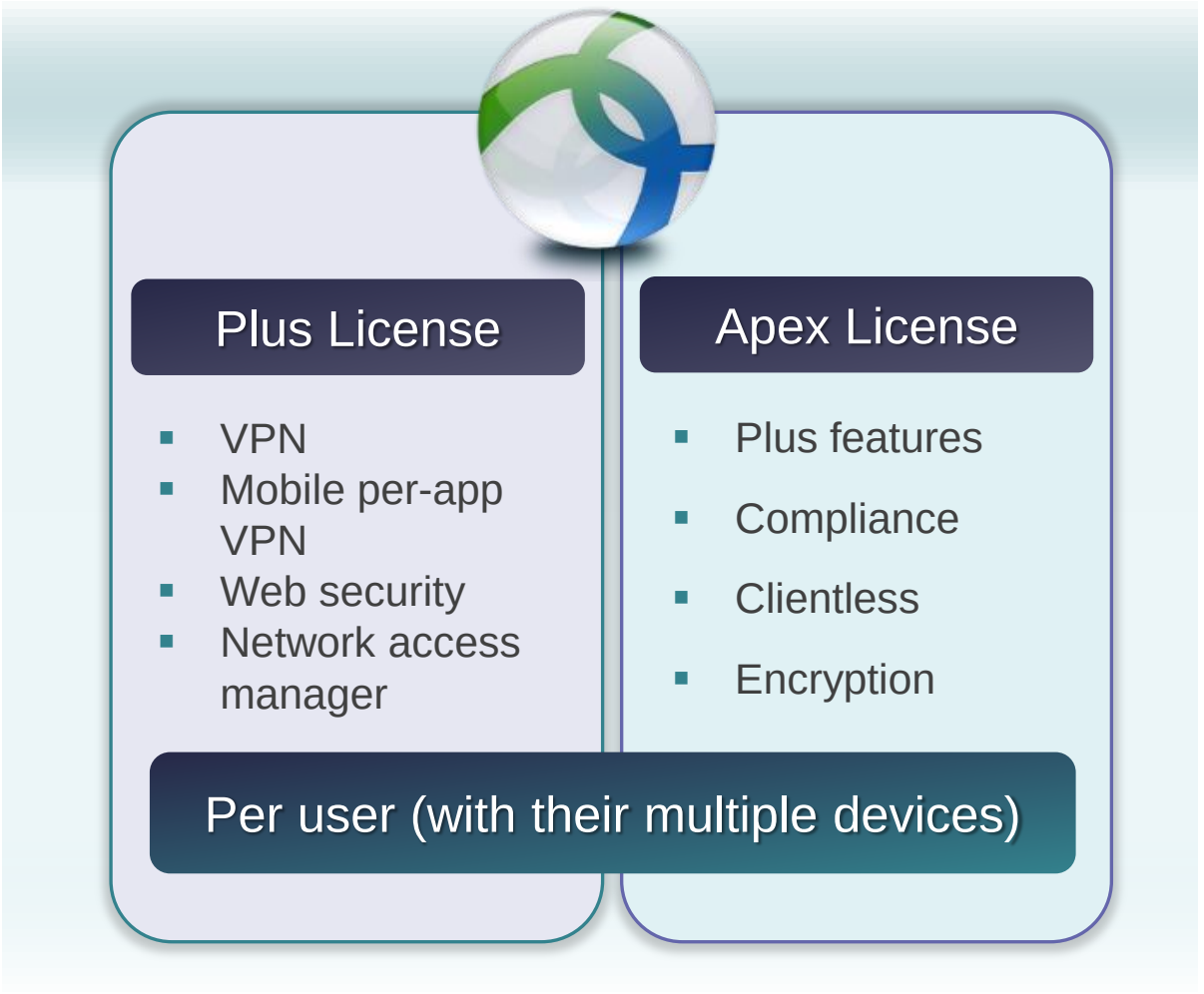


What's New in Cisco AnyConnect 4.0?

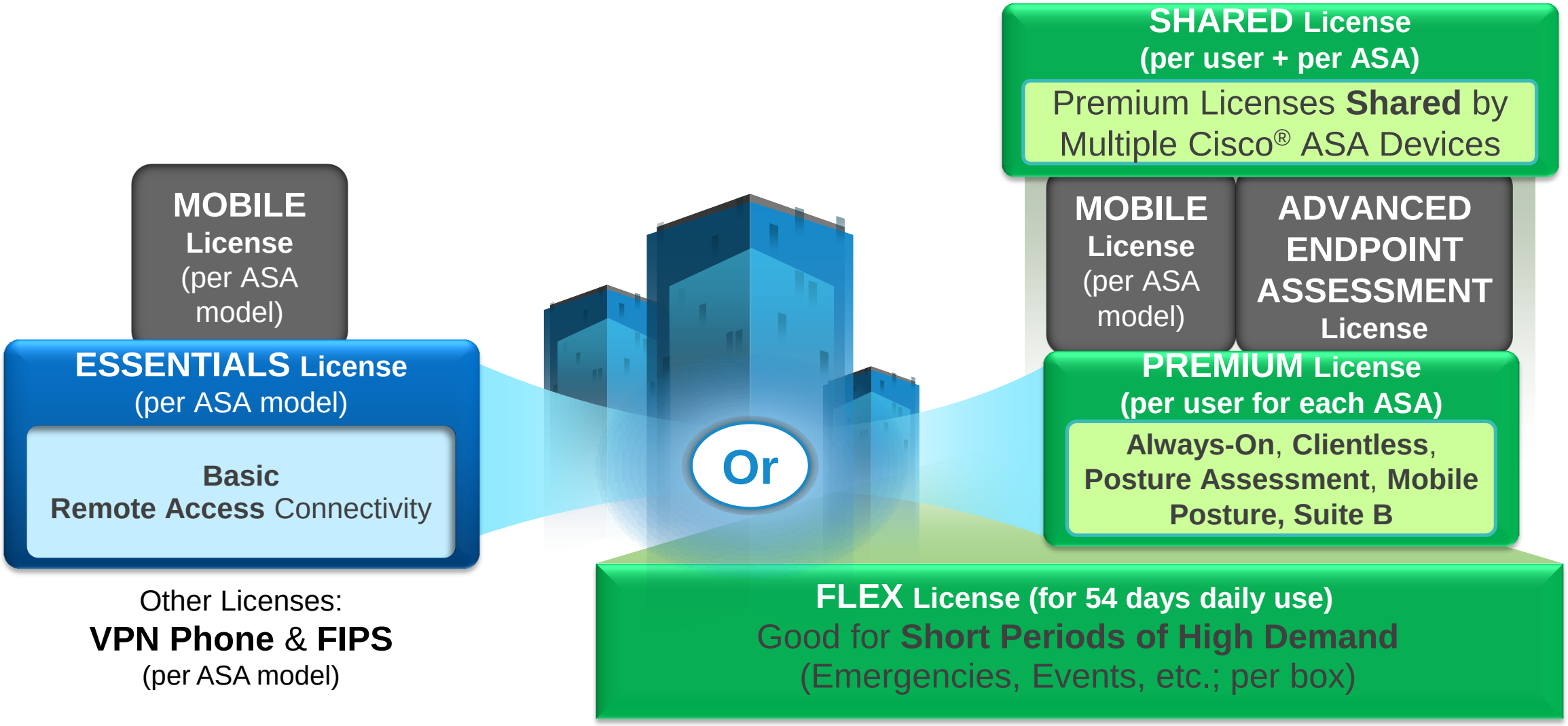
Port Licensing for Greater Flexibility

NEW

- New endpoint licensing portable across any hardware platforms, simplifying transfer
- New two-tiered licensing structure to allow customers to grow based on new enterprise mobility needs
- Migration
  - Essentials to Plus
  - Premium to Apex



AnyConnect Licensing - Today



Other Licenses:
VPN Phone & **FIPS**
(per ASA model)

New AC Features & Licensing

AC 3.X
(Tight with ASA only)

- Premium (Perpetual)
- Shared (Perpetual)
- Flex (Perpetual)
- AEA (Perpetual)
- Mobile (Perpetual)
- Essentials (Perpetual)
- Non-Lic (NAM, CWS, Mobile Opt)

AC 4.X
(Loose with ASA, ISE, ISR, ASR, CSR, CWS)

"APEX" ***New!***

- Advanced PC + **Mobile** Services
  - **Unified Endpoint Compliance /Remediation (Posture)**
  - Suite B
  - Clientless
  - Includes PLUS

"PLUS" ***New!***

- Basic PC + **Mobile** Services
  - Device VPN / **Per app VPN**
  - Always On
  - ASA, ISE, ASR, CSR
  - **FIPS**
  - CWS / Web Security
  - NAM

Deployment Logic

- **Users**
  - How many users will utilize AC services?
- **Services**
  - How many users need basic services?
  - How many users need advanced services?
- **Headend**
  - How many active sessions at any given time?
  - What headend platform/s?
  - How many locations?

PLUS

APEX

Migration Strategy

Existing AC licenses
(Core)

Premium
(Perpetual)

Shared
(Perpetual)

AC APEX Migration Licenses
($0 for 3 YR, Any User Count)

APEX (Term)

PLUS (Term)

AC PLUS Migration Licenses
(50% Discount on 5/3/1 Yr Licenses,
Any User Count) *

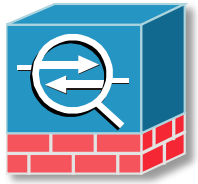
Essentials
(Perpetual)

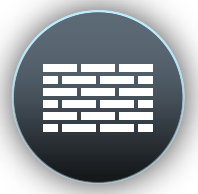
Non-Lic
(NAM, CWS, etc)

PLUS (Term)

New ASA (Existing TMP)

Old ASA





*** Yes – No Offer For Migration To Plus Perpetual**

AnyConnect Offers

PLUS (Perpetual)

- 25-250K per user pricing ($$$)
- “Right to Use” based on user/seat count vs concurrency
- Support (SASU) ordered separately
- Compliance -> Trust (Phase 1)
- Built in “Shared” functionality
- Covers PC and Mobile
- Includes “near” zero day OS support for all supported platforms

or

APEX (Term)

PLUS (Term)

- 25-250K per user pricing ($)
- “Right to Use” based on user/seat count vs concurrency
- 1, 3 and 5 Yr options (includes support)
- Compliance -> Trust (Phase 1)
- Built in “Shared, Flex” functionality
- Covers PC and Mobile
- Includes “near” zero day OS support for all supported platforms

Scenario #1a – Basic VPN Greenfield (Term)

New customer wants to cover 1000 users with 500 active endpoint connected at any one time. This is basic device-based VPN for PC as well as mobile devices, requires HA, and is centralized. Customer is interested in migrating to per app VPN on mobile platforms to help decrease bandwidth backhaul costs.

1 Order appropriate appliances and SMARTnet options

Product Number	List Price	Qty	Total
ASA5525-K9	$8,995	2	$18,990
(SMARTNET/SASU-SKUs)	-	-	-

2 Selects AC PLUS based on total number of users

Product Number	List Price	Qty	Total
L-AC-PLS-5Y-G	$-	1	$-
AC-PLS-5Y-1K	$2,500	1	$2,500

Scenario #1b – Basic VPN Greenfield (Perpetual)

New customer wants to cover 1000 users with 500 active endpoint connected at any one time. This is basic device-based VPN for PC as well as mobile devices, requires HA, and is centralized. Customer is interested in migrating to per app VPN on mobile platforms to help decrease bandwidth backhaul costs. Have CAPEX vs OPEX preference.

1 Order appropriate appliances and SMARTnet options

Product Number	List Price	Qty	Total
ASA5525-K9	$8,995	2	$18,990
(SMARTNET/SASU-SKUs)	-	-	-

2 Selects AC PLUS based on total number of users

Product Number	List Price	Qty	Total
L-AC-PLS-P-G	$-	1	$-
AC-PLS-P-1K	$6,250	1	$6,250

Scenario #2a – Advanced VPN Greenfield

New customer wants to cover 1000 users with 500 active endpoint connected at any one time. This is advanced device-based VPN for PC as well as mobile devices, requires HA, and is centralized. They want clientless for contractors and want to enforce PC compliance prior for employees.

1 Order appropriate appliances and SMARTnet options

Product Number	List Price	Qty	Total
ASA5525-K9	$8,995	2	$18,990
(SMARTNET/SASU-SKUs)	-	-	-

2 Selects AC PLUS based on total number of users

Product Number	List Price	Qty	Total
L-AC-APX-5Y-G	$-	1	$-
AC-APX-5Y-1K	$12,000	1	$12,000

Scenario #2b – Advanced + Basic VPN Greenfield

New customer wants to cover 750 users with 500 active endpoint connected at any one time. This is advanced device-based VPN for PC as well as mobile devices, requires HA, and is centralized. They want clientless for 250 contractors and want to enforce PC compliance for 250 employees but they want basic VPN access for 250 partners regardless of PC or mobile for partner portal access

1 Order appropriate appliances and SMARTnet options

Product Number	List Price	Qty	Total
ASA5525-K9	$8,995	2	$18,990
(SMARTNET/SASU-SKUs)	-	-	-

2 Selects AC PLUS and APEX based on total number of users

Product Number	List Price	Qty	Total
L-AC-PLS-5Y-G	$-	1	$-
AC-PLS-5Y-250	$625	1	$625
L-AC-APX-5Y-G	$-	1	$-
AC-APX-5Y-500	$9,000	1	$9,000

Scenario #3 – Basic VPN Migration

Existing customer has pair of 5540s with essentials and mobile. They have been providing basic VPN access to 5000 users (averaging 1000 concurrently sessions). This is all device-based VPN. Customer expects mobile device count to grow so want so add per app VPN services in addition to covering new future Windows OS and Apple OS X software versions. Feels that existing 5540s still has enough headroom (only expect 2000 concurrent worst case). Budget wise they want 3 year licenses.

1 Does not need any new appliances

2 Selects AC PLUS migration based on total number of users

Product Number	List Price	Qty	Total
L-AC-PLS-M-3Y-G	$-	1	$-
AC-PLS-M-3Y-5K	$4,600	1	$4,600

Scenario #4 – Adv VPN Migration

Existing customer has pair of 5540s with 1000 AC Premium licenses. They have been providing advanced VPN access to 3000 users with (averaging 1000 concurrently sessions). The are using Hostscan and Adv Endpoint Assessment and want to maintain that service but open service up to larger number of employees (5000 in total). Feels that existing 5540s still has enough headroom (only expect 2000 concurrent worst case).

1 Does not need any new appliances

2 Selects AC Apex migration based on total number of users

Product Number	List Price	Qty	Total
L-AC-APX-M-SG	$0	1	$0
L-AC-APX-M-5K	$0	1	$0

Web Security Appliance AsyncOS 8.5

New Features and Enhancements

- ISE Integration (Preview / pre-beta)
- Advanced Malware Protection (AMP) - Phase 2
- High Availability
- Time and Bandwidth Quotas
- Virtual SMA (Security Management Appliance)
- Enhanced Operations and Security Updates

Thank you.