Secure

Security

Why Cisco?

Today's threat landscape is nothing like that of 10 years ago. Simple attacks that caused containable damage have given way to modern, sophisticated, and well-funded cybercrime operations capable of disrupting and causing major loss to organizations and national infrastructure. These are difficult to detect, can remain in networks for long periods of time, and amass resources to launch attacks elsewhere.
Legacy protection methods that exclusively rely on detection and blocking are no longer adequate. It's time for a new security model that addresses the full attack continuum: before, during and after an attack.
To erect the new security model, focus on three strategic imperatives:

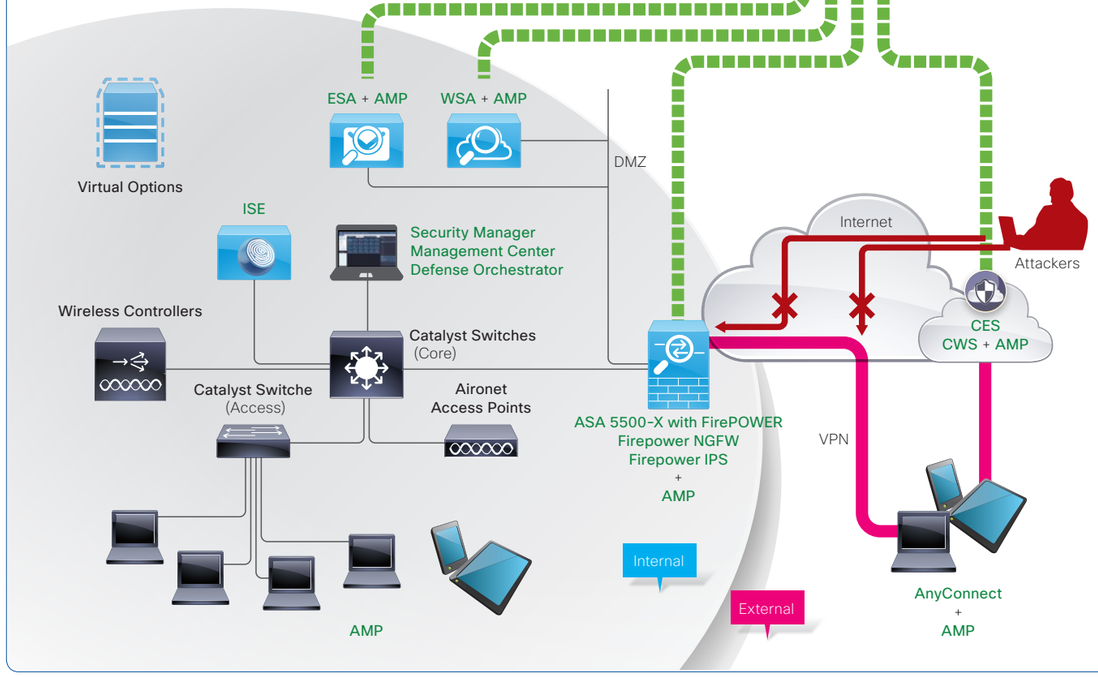
- **Visibility Driven**
  Get global intelligence and context for deeper insights and better decisions.
- **Threat Focused**
  Detect, understand, and stop threats across the entire attack continuum
- **Platform Based**
  Reduce fragmentation by using a platform-based approach to protect the network, devices, and the cloud.

Across-the-board protection (spanning the attack continuum) requires the integration of technologies with different areas of focus. The Cisco security portfolio, offers a comprehensive range of threat-centric cybersecurity solutions that fight advanced malware, targeted attacks, and APTs. These visibility-driven, threat-focused, and platform-based solutions offer the industry's broadest set of enforcement and remediation options at attack vectors where threats manifest.

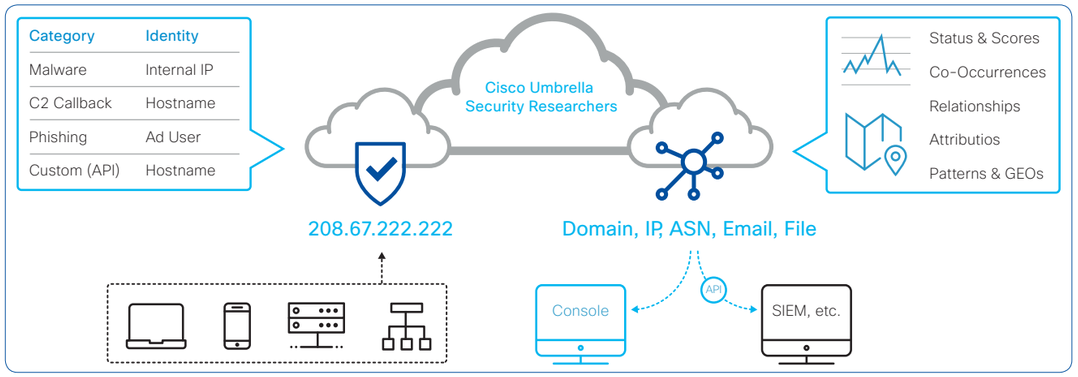
Visibility Driven	Threat Focused	Platform Based
Network-Integrated, Broad Sensor Base, Context and Automation	Continuous Advanced Threat Protection, Cloud-Based Security Intelligence	Agile and Open Platforms, Built for Scale, Consistent Control, Management

Network Endpoint Mobile Virtual Cloud

For details on Cisco Security, visit the following Web site:
http://www.cisco.com/go/security



Cisco Umbrella NEW



The Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. Our global infrastructure handles over 80 billion internet request a day, which our security engine analyzes to learn where attacks are being staged even before the first victim is hit.

■ Cisco Umbrella
- **First Line of Defense against Threats**
  Block malware, phishing, and command & control callbacks over any port or protocol—before threats reach you.
- **Visibility & Protection Everywhere**
  Gain the visibility needed to protect internet access across all devices on your network, all office locations, and roaming users.
- **Integrations to Amplify Existing Investments**
  Integrate with existing tools and feeds to extend protection and enrich your incident response data.

■ Cisco Umbrella Investigate
- **A Live Graph of Global & Historical Internet Activity**
  The most complete view of the relationships and evolution of internet domains, IPs, networks, and malware.
- **Pivot through Attackers' Infrastructures**
  Use our dynamic search engine or RESTful API to mine our diverse data sets and statistical models.
- **Enrich Your SIEM Data and Speed Up Workflows**
  Use our global context and predictive intelligence to prioritize incident response and stay ahead of attacks.

■ Cisco Umbrella Roaming License*1

SKU	Description
UMB-ROAM	Umbrella Roaming Per User License

■ Cisco Umbrella Branch Licenses for Cisco ISR 4000 Series*1

SKU	Description
UMB-BRAN-4321	Umbrella Branch License for Cisco ISR 4321
UMB-BRAN-4331	Umbrella Branch License for Cisco ISR 4331
UMB-BRAN-4351	Umbrella Branch License for Cisco ISR 4351
UMB-BRAN-4431	Umbrella Branch License for Cisco ISR 4431
UMB-BRAN-4451	Umbrella Branch License for Cisco ISR 4451

■ Cisco Umbrella Professional License*1

SKU	Description
UMB-PROFESSIONAL	Umbrella Professional Per User License

■ Cisco Umbrella Insights License*1

SKU	Description
UMB-INSIGHTS-K9	Umbrella Insights Per User License

■ Cisco Umbrella Platform License*1

SKU	Description
UMB-PLATFORM-K9	Umbrella Platform Per User License

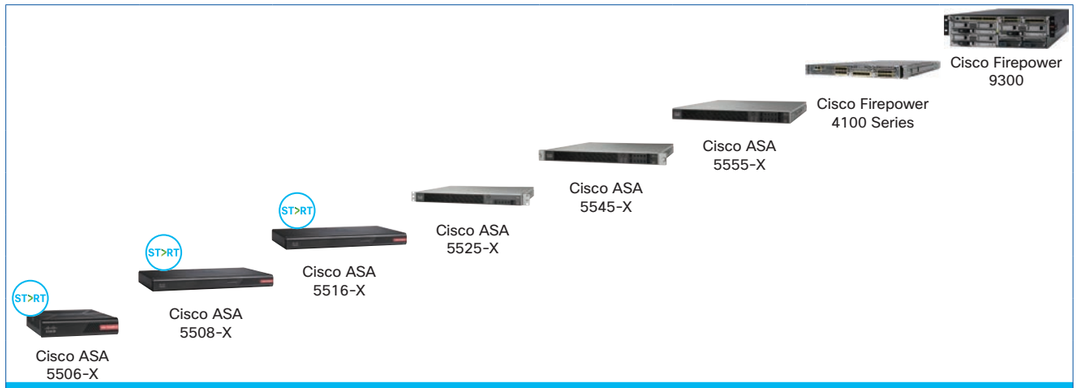
■ Cisco Umbrella Package Comparison

Package		Roaming	Branch	Professional	Insights	Platform
Best for		Cisco NGFW/ AnyConnect	Cisco ISR 4000 Series	Small Companies	Mid-sized Companies	Advanced Security Teams
Performance	100 % Cloud — No Hardware to Install or Software to Maintain	●	●	●	●	●
	100 % Uptime — Resolves 80 B+ Requests Daily with No Added Latency	●	●	●	●	●
	7 M+ Unique Malicious Destinations Enforced Concurrently across 25 Data Centers	●	●	●	●	●
Protection	Add a New Layer of Predictive Security for Any Device, Anywhere	●*2	●*3	●	●	●
	Prevent Malware, Phishing, and C2 Callbacks over Any Port	●	●	●	●	●
	Enforce Acceptable Use Policies Using 60 Content Categories	–	●	●	●	●
Enforcement	Block Malicious Domain Requests & IP Responses at the DNS-Layer	●	●	●	●	●
	Block Malicious URL Paths & Direct IP Connections at the IP-Layer	–	–	–	●	●
Visibility	Real-Time, Enterprise-Wide Activity Search & Scheduled Reports	●	●	●	●	●
	Identify Targeted Attacks by Comparing Local vs. Global Activity	–	–	–	●	●
	Identify Cloud & IoT Usage Risks by Reporting on 1800+ Services	–	–	–	●	●
Management	Custom Block/Allow Lists, Built-in Block Pages, and Bypass Options	●*4	●	●	●	●
	Enforcement & Visibility per Internal Network or AD User/Group	–	●*5	–	●	●
	Retain Logs Forever by Integrating with Your Amazon S3 Bucket	–	–	–	●	●
Platform Package Exclusive	API-based Integrations to Enforce & Manage 3rd-party Block Lists	–	–	–	–	●
	Investigate Console — Threat Intelligence on All Domains, IPs, & File Hashes	–	–	–	–	●

*1 UMBRELLA-SUB is required. *2 Off-network only. *3 On-network only. *4 Only has allow list and 1 built-in block page. *5 Only per internal network (no Active Directory).

Next-Generation Firewalls

Cisco ASA 5500-X with FirePOWER Services



The Cisco ASA 5500-X with FirePOWER Services is the industry's first fully integrated, threat-focused next-generation firewall with unified management. It includes **Application Visibility and Control (AVC)**, optional **Firepower Next-Generation IPS (NGIPS)**, **Cisco Advanced Malware Protection (AMP),** and **URL Filtering**. Cisco Firepower NGFW provides advanced threat protection before, during, and after attacks.

For details on Cisco ASA 5500-X with FirePOWER Services, visit the following Web site:

http://www.cisco.com/go/asa

- **Stop more threats**: Contain known and unknown malware with leading Cisco AMP and sandboxing. Get application firewalling (AVC) for 4,000 commercial applications, plus additional custom applications.
- **Gain more insight**: Gain superior visibility into your environment with Cisco Firepower NGIPS. Automated risk rankings and impact flags identify priorities for your team.
- **Detect earlier, act faster**: The Cisco Annual Security Report identifies a 100-day median time from infection to detection, across enterprises. Cisco reduces this time to less than a day.
- **Reduce complexity**: Get unified management and automated threat correlation across tightly integrated security functions, including application firewalling, NGIPS, and AMP.
- **Get more from your network**: Enhance security, and take advantage of your existing investments, with optional integration of other Cisco and third-party networking and security solutions.

■ Cisco ASA 5500-X with FirePOWER Services (1 of 2)

SKU	Description	Dimensions (Height x Width x Depth)	Maximum Weight
ASA5506-K9	Cisco ASA 5506-X with FirePOWER Services	4.37 x 19.99 x 23.44 cm	1.81 kg
ASA5506W-x-K9	Cisco ASA 5506W-X with FirePOWER Services Wireless Model	4.37 x 19.99 x 23.44 cm	1.81 kg
ASA5506H-SP-BUN-K9	Cisco ASA 5506H-X with FirePOWER Services Hardened Model	6.90 x 22.98 x 22.98 cm	3.18 kg
ASA5508-K9	Cisco ASA 5508-X with FirePOWER Services	4.37 x 43.69 x 28.67 cm	3.63 kg
ASA5516-K9	Cisco ASA 5516-X with FirePOWER Services	4.37 x 43.69 x 28.67 cm	3.63 kg

■ Cisco ASA 5500-X with FirePOWER Services (2 of 2)

SKU	Throughput				AVC Sessions		VPN Tunnels		Ports	Power Supply	Rack mount
	FW	FW AVC	FW AVC IPS	VPN	Concurrent Sessions	New Connections per Second	Site-to-Site	Remote Access	GE		
ASA5506-K9	750 Mbps	250 Mbps	125 Mbps	100 Mbps	20,000	5,000	10	50	8	1 AC	1 RU
ASA5506W-x-K9	750 Mbps	250 Mbps	125 Mbps	100 Mbps	20,000	5,000	10	50	8	1 AC	1 RU
ASA5506H-SP-BUN-K9	750 Mbps	250 Mbps	125 Mbps	100 Mbps	50,000	5,000	50	50	4	1 AC	1 RU
ASA5508-K9	1 Gbps	450 Mbps	250 Mbps	175 Mbps	100,000	10,000	100	100	8	1 AC	1 RU
ASA5516-K9	1.8 Gbps	850 Mbps	450 Mbps	250 Mbps	250,000	20,000	300	300	8	1 AC	1 RU

Cisco ASA Transition Guide

Legacy Models	FW + AVC	FW + AVC + IPS	Current Models	FW + AVC	FW + AVC + IPS
Cisco ASA 5505	-	-	**Cisco ASA 5506-X**	250 Mbps	125 Mbps
Cisco ASA 5510	-	-	**Cisco ASA 5508-X**	450 Mbps	250 Mbps
Cisco ASA 5512	300 Mbps	150 Mbps	**Cisco ASA 5516-X**	850 Mbps	450 Mbps
Cisco ASA 5515-X	500 Mbps	250 Mbps	**Cisco ASA 5516-X**	850 Mbps	450 Mbps

Cisco FirePOWER Services License

The **Cisco ASA 5500-X with FirePOWER Services** ship with a base license for Application Visibility and Control (AVC). Optional subscriptions for Next-Generation IPS (NGIPS), Cisco Advanced Malware Protection (AMP), and URL Filtering (URL) can be added to the base configuration for advanced functionality.

- **Application Visibility and Control (AVC)**
  Supports more than 4,000 application-layer and risk-based controls that can launch tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.

One-year, **3-year**, and **5-year** subscriptions for each FirePOWER Services are available.

- **Next-Generation IPS (NGIPS)**
  Provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications, and content to detect multivector threats and automate defense response. The NGIPS licenses can be added alone to the base Cisco FirePOWER Services licenses or bundled with AMP, or with AMP and URL licenses.
- **Cisco Advanced Malware Protection (AMP)**
  Delivers inline network protection against sophisticated malware and Cisco Threat Grid sandboxing. The AMP licenses can be added alone to the base Cisco FirePOWER Services licenses or bundled with NGIPS, or with NGIPS and URL licenses.
- **URL Filtering (URL)**
  Adds the capability to filter more than 280 million top-level domains by risk level and more than 82 categories. The URL licenses can be added alone to the base FirePOWER Services licenses or bundled with NGIPS, or with NGIPS and AMP licenses.

■ Cisco FirePOWER Services License Comparison

Licenses	Characters Included in SKU	Next-Generation IPS (NGIPS)	Advanced Malware Protection (AMP)	URL Filtering (URL)
NGIPS License	TA	●	-	-
AMP License	AMP	-	●	-
URL License	URL	-	-	●
NGIPS & AMP License	TAM	●	●	-
NGIPS & URL License	TAC	●	-	●
NGIPS & AMP & URL License	TAMC	●	●	●

■ Cisco FirePOWER Services NGIPS License*1

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-TA-1Y	L-ASA5506-TA-3Y	L-ASA5506-TA-5Y	ASA 5506
L-ASA5506-TA-1Y	L-ASA5506-TA-3Y	L-ASA5506-TA-5Y	ASA 5506W
L-ASA5506H-TA-1Y	L-ASA5506H-TA-3Y	L-ASA5506H-TA-5Y	ASA 5506H
L-ASA5508-TA-1Y	L-ASA5508-TA-3Y	L-ASA5508-TA-5Y	ASA 5508
L-ASA5516-TA-1Y	L-ASA5516-TA-3Y	L-ASA5516-TA-5Y	ASA 5516

■ Cisco FirePOWER Services NGIPS & AMP License*4

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-TAM-1Y	L-ASA5506-TAM-3Y	L-ASA5506-TAM-5Y	ASA 5506
L-ASA5506-TAM-1Y	L-ASA5506-TAM-3Y	L-ASA5506-TAM-5Y	ASA 5506W
L-ASA5506H-TAM-1Y	L-ASA5506H-TAM-3Y	L-ASA5506H-TAM-5Y	ASA 5506H
L-ASA5508-TAM-1Y	L-ASA5508-TAM-3Y	L-ASA5508-TAM-5Y	ASA 5508
L-ASA5516-TAM-1Y	L-ASA5516-TAM-3Y	L-ASA5516-TAM-5Y	ASA 5516

■ Cisco FirePOWER Services AMP License*2

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-AMP-1Y	L-ASA5506-AMP-3Y	L-ASA5506-AMP-5Y	ASA 5506
L-ASA5506-AMP-1Y	L-ASA5506-AMP-3Y	L-ASA5506-AMP-5Y	ASA 5506W
L-ASA5506H-AMP-1Y	L-ASA5506H-AMP-3Y	L-ASA5506H-AMP-5Y	ASA 5506H
L-ASA5508-AMP-1Y	L-ASA5508-AMP-3Y	L-ASA5508-AMP-5Y	ASA 5508
L-ASA5516-AMP-1Y	L-ASA5516-AMP-3Y	L-ASA5516-AMP-5Y	ASA 5516

■ Cisco FirePOWER Services NGIPS & URL License*5

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-TAC-1Y	L-ASA5506-TAC-3Y	L-ASA5506-TAC-5Y	ASA 5506
L-ASA5506-TAC-1Y	L-ASA5506-TAC-3Y	L-ASA5506-TAC-5Y	ASA 5506W
L-ASA5506H-TAC-1Y	L-ASA5506H-TAC-3Y	L-ASA5506H-TAC-5Y	ASA 5506H
L-ASA5508-TAC-1Y	L-ASA5508-TAC-3Y	L-ASA5508-TAC-5Y	ASA 5508
L-ASA5516-TAC-1Y	L-ASA5516-TAC-3Y	L-ASA5516-TAC-5Y	ASA 5516

■ Cisco FirePOWER Services URL License*3

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-URL-1Y	L-ASA5506-URL-3Y	L-ASA5506-URL-5Y	ASA 5506
L-ASA5506-URL-1Y	L-ASA5506-URL-3Y	L-ASA5506-URL-5Y	ASA 5506W
L-ASA5506H-URL-1Y	L-ASA5506H-URL-3Y	L-ASA5506H-URL-5Y	ASA 5506H
L-ASA5508-URL-1Y	L-ASA5508-URL-3Y	L-ASA5508-URL-5Y	ASA 5508
L-ASA5516-URL-1Y	L-ASA5516-URL-3Y	L-ASA5516-URL-5Y	ASA 5516

■ Cisco FirePOWER Services NGIPS & AMP & URL License*6

SKU			Compatible Models
1-Year	3-Year	5-Year	
L-ASA5506-TAMC-1Y	L-ASA5506-TAMC-3Y	L-ASA5506-TAMC-5Y	ASA 5506
L-ASA5506-TAMC-1Y	L-ASA5506-TAMC-3Y	L-ASA5506-TAMC-5Y	ASA 5506W
L-ASA5506H-TAMC-1Y	L-ASA5506H-TAMC-3Y	L-ASA5506H-TAMC-5Y	ASA 5506H
L-ASA5508-TAMC-1Y	L-ASA5508-TAMC-3Y	L-ASA5508-TAMC-5Y	ASA 5508
L-ASA5516-TAMC-1Y	L-ASA5516-TAMC-3Y	L-ASA5516-TAMC-5Y	ASA 5516

*1 L-ASAxxxx-TA= is required (The "xxxx" corresponds to the supported models). *2 L-ASAxxxx-AMP= is required (The "xxxx" corresponds to the supported models).
*3 L-ASAxxxx-URL= is required (The "xxxx" corresponds to the supported models). *4 L-ASAxxxx-TAM= is required (The "xxxx" corresponds to the supported models).
*5 L-ASAxxxx-TAC= is required (The "xxxx" corresponds to the supported models). *6 L-ASAxxxx-TAMC= is required (The "xxxx" corresponds to the supported models).

VPN and Endpoint Security Clients

Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility Client is a unified agent with remote access functionality, posture enforcement, web security features, and off-network security protection. It gives your IT department all the secure-access features necessary to provide a robust, user-friendly, and highly secure mobile experience.

The industry-leading Cisco AnyConnect Secure Mobility Client is a multifaceted endpoint software product. That means it not only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules. These modules provide services that include compliance through the VPN and Cisco Identity Services Engine (ISE) posture along with web security, network visibility, off-network protection, and the Cisco Network Access Manager.

Cisco AnyConnect Secure Mobility Client is available across a broad set of platforms, including Windows, Mac OS X, Linux, iOS, Android, Windows Phone, BlackBerry, and Google Chrome.

Cisco AnyConnect License Comparison

	Plus	Apex
Device or System VPN (Including Cisco Phone VPN)	●	●
Third-Party IPsec IKEv2 Remote Access VPN Clients (Non-AnyConnect Client)	●	●
Per-Application VPN	●	●
Cloud Web Security and Web Security Appliance	●	●
Cisco Umbrella Roaming*1	●	●
Network Access Manager	●	●
AMP for Endpoints Enabler*2	●	●
Network Visibility Module	-	●
Unified Endpoint Compliance and Remediation (Posture)*3	-	●
Suite B or Next-Generation Encryption (Including Third-Party IPsec IKEv2 Remote VPN Clients)	-	●
Clientless (Browser-based) VPN Connectivity	-	●
ASA Multicontext-mode Remote Access	-	●

Cisco AnyConnect Plus License (1 of 2)*4

SKU			User Range
1-Year*5	3-Year*5	5-Year*5	
L-AC-PLS-1Y-S1	L-AC-PLS-3Y-S1	L-AC-PLS-5Y-S1	25 to 99
L-AC-PLS-1Y-S2	L-AC-PLS-3Y-S2	L-AC-PLS-5Y-S2	100 to 249
L-AC-PLS-1Y-S3	L-AC-PLS-3Y-S3	L-AC-PLS-5Y-S3	250 to 499

Cisco AnyConnect Apex License*4

SKU			User Range
1-Year*7	3-Year*7	5-Year*7	
L-AC-APX-1Y-S1	L-AC-APX-3Y-S1	L-AC-APX-5Y-S1	25 to 99
L-AC-APX-1Y-S2	L-AC-APX-3Y-S2	L-AC-APX -5Y-S2	100 to 249
L-AC-APX-1Y-S3	L-AC-APX-3Y-S3	L-AC-APX -5Y-S3	250 to 499

Cisco AnyConnect Plus License (2 of 2)*4

SKU	Users
Perpetual*6	
AC-PLS-P-25-S	25
AC-PLS-P-50-S	50
AC-PLS-P-100-S	100
AC-PLS-P-250-S	250
AC-PLS-P-500-S	500

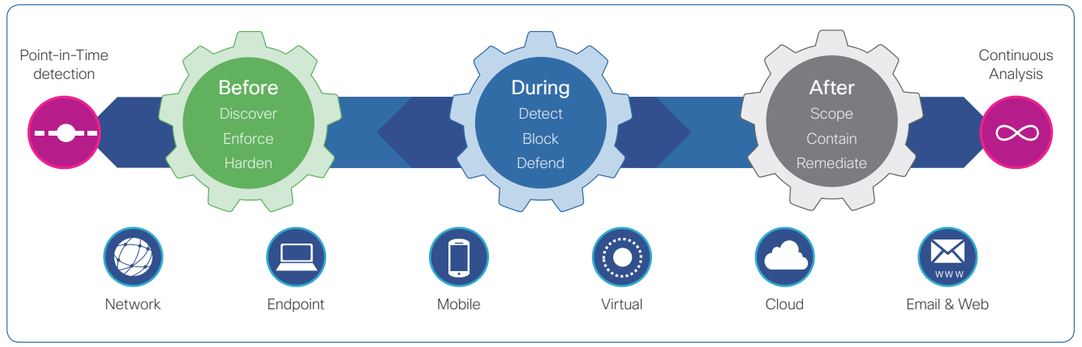
Cisco AnyConnect VPN Only License*4

SKU	Simultaneous Connections
Perpetual	
L-AC-VPNO-25=	25
L-AC-VPNO-50=	50
L-AC-VPNO-100=	100
L-AC-VPNO-250=	250
L-AC-VPNO-500=	500

*1 Cisco Umbrella Roaming License is required. *2 Cisco AMP for Endpoints License is required. *3 Cisco ISE Apex License is required.
*4 Refer to the Ordering Guide for a full list of orderable SKUs. *5 L-AC-PLS-LIC= is required. *6 L-AC-PLS-P-G is required. *7 L-AC-APX-LIC= is required.

Advanced Malware Protection (AMP)

Cisco Advanced Malware Protection (AMP) for Endpoints



Cisco Advanced Malware Protection (AMP)

The Cisco Advanced Malware Protection (AMP) is a security solution that addresses the full lifecycle of the advanced malware problem. Not only can it prevent breaches, but it also gives you the visibility and control to rapidly detect, contain, and remediate threats if they evade front-line defenses—all cost-effectively and without impacting operational efficiency. Cisco AMP protects your organization **before**, **during**, and **after** an attack.

- **Before** an attack, Cisco AMP uses global threat intelligence from the **Cisco Collective Security Intelligence** organization, **Talos Security Intelligence and Research Group**, and **Threat Grid**'s threat intelligence feeds to strengthen defenses and protect against known and emerging threats.
- **During** an attack, Cisco AMP uses that intelligence, coupled with known file signatures and **Threat Grid**'s malware analysis technology, to identify and block policy-violating file types, exploit attempts, and malicious files trying to infiltrate the network.
- **After** an attack, or after a file is initially inspected, the solution continues to monitor and analyze all file activity and traffic, regardless of file disposition, searching for any indications of malicious behavior. If a file with an unknown or previously deemed "good" disposition starts behaving badly, Cisco AMP alerts security teams with an indication of compromise. It then provides comprehensive visibility into where the malware originated, what systems were affected, and what the malware is doing. It also provides the controls to rapidly respond to the intrusion, contain the threat, and remediate it with a few clicks.

For details on Cisco AMP, visit the following Web site:
http://www.cisco.com/go/amp

Cisco Advanced Malware Protection (AMP) for Endpoints

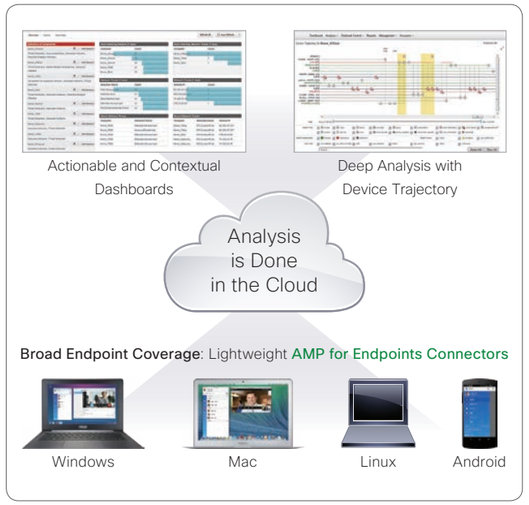
The Cisco AMP for Endpoints is a cloud-managed endpoint security solution that provides the visibility, context, and control to not only prevent breaches, but also rapidly detect, contain, and remediate threats if they evade front-line defenses and get inside, all cost-effectively and without affecting operational efficiency.

- **Prevent**: Strengthen defenses using the best global threat intelligence and block malware in real time.
- **Monitor and Detect**: Continuously monitor and record all file activity to quickly detect stealthy malware.
- **Respond**: Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, and Android mobile devices.

Cisco AMP for Endpoints is managed through an easy-to-use, web-based console. It is deployed through AMP's lightweight endpoint connector, with minimal performance impact on users. Analysis is done in the cloud, not on the endpoint.

The solution is offered as a subscription on endpoints, including coverage for Windows, Macs, Linux, and Android mobile devices.

If your organization has high privacy requirements that restrict using a public cloud, the Cisco AMP Private Cloud Virtual Appliance is an on-premises, air-gapped option. Each private cloud instance supports up to 10,000 connectors, and multiple Private Cloud Virtual Appliances can be added to the environment.



Cisco AMP for Endpoints Connector License*1

SKU			Connectors Range
1-Year	3-Year	5-Year	
FP-AMP-1Y-S1	FP-AMP-3Y-S1	FP-AMP-5Y-S1	50 to 99
FP-AMP-1Y-S2	FP-AMP-3Y-S2	FP-AMP-5Y-S2	100 to 499
FP-AMP-1Y-S3	FP-AMP-3Y-S3	FP-AMP-5Y-S3	500 to 999
FP-AMP-1Y-S4	FP-AMP-3Y-S4	FP-AMP-5Y-S4	1,000 to 4,999
FP-AMP-1Y-S5	FP-AMP-3Y-S5	FP-AMP-5Y-S5	5,000 to 9,999

Cisco AMP Virtual Private Cloud Appliance*2

SKU	Max Connectors
FP-AMP-CLOUD-SW	10,000

*1 FP-AMP-LIC= is required. Refer to the Ordering Guide for a full list of orderable SKUs. *2 FP-AMP-CLOUD-BUN and Cisco AMP for Endpoints Connector License are required.