Secure
Security

Featured Products

Cisco Firepower 2100 Series

Gain Business Resiliency through Superior Security with Threat-Focused Next-Generation Firewall

FPR2110-NGFW-K9

Dual Multicore CPU	2 Gbps FW + AVC Throughput	2 Gbps AVC + IPS Throughput	750 Mbps VPN Throughput	1,500 VPN Peers	Default AVC	Optional NGIPS	Optional AMP	Optional URL Filtering
12-port GE	4-port SFP	Firepower Device Manager						

Secure
Security

Cisco Advanced Malware Protection for Endpoints

Replace Your Legacy Anti-Virus with Next-Generation Endpoint Security

FP-AMP-LIC=

| Powered by Talos | 1.6 million Global Sensors | 1.5 million Samples per Day | 100 TB Data per Day | 13 Billion Web Requests | 24-Hour Operations | Windows | macOS | Linux Red Hat Enterprise | Linux CentOS | Android | iOS |

Secure
Security

Featured Products

Cisco Meraki MX Cloud Managed Security Appliances

Comprehensive Security in a Single Box
Secure a Site in Minutes, Right Out of the Box

MX84-HW

500 Mbps FW Throughput	320 Mbps Adv. Security Throughput	250 Mbps VPN Throughput	100 VPN Peers	1 TB Web Caching
Default AVC	Optional NGIPS	Optional AMP	Optional URL Filtering	
2-port GE-WAN	8-port GE-LAN	2-port SFP-LAN	USB for 4G	

MX65W-HW

250 Mbps FW Throughput	200 Mbps Adv. Security Throughput	100 Mbps VPN Throughput	50 VPN Peers	
Default AVC	Optional NGIPS	Optional AMP	Optional URL Filtering	
2-port GE-WAN	8-port GE-LAN	2-port GE-LAN PoE+	11ac Wave 2 AP	USB for 4G

Secure - Security
Cisco ASA 5500-X Series

WEB

| Overview | Positioning Map | Platform Spec | Licenses |

Superior Multilayered Protection

The Cisco ASA 5500-X Series is not only the world's most widely deployed, enterprise-class stateful firewall, but aloso the industry's first adaptive, threat-focused Next-Generation FireWall (NGFW). It provides comprehensive protection from known and advanced threats, including protection against targeted and persistent malware attacks.

With Cisco ASA, you consolidate multiple security layers in a single platform, eliminating the cost of buying and managing multiple solutions. This integrated approach combines best-in-class security technology with multilayer protection integrated in a single device that's less costly than piecemeal security solutions.

Highlights

● Site-to-site and remote access VPN and advanced clustering provide highly secure, high-performance access and high availability to help ensure business continuity.

● Granular Application Visibility and Control (AVC) supports more than 3,000 application-layer and risk-based controls that can launch tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.

● The industry-leading Cisco Firepower 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.

● Cisco Advanced Malware Protection (AMP) provides industry-leading breach detection effectiveness, sandboxing, a low total cost of ownership, and superior protection value that helps you discover, understand, and stop malware and emerging threats missed by other security layers.

● Reputation- and category-based URL Filtering offer comprehensive alerting and control over suspicious web traffic and enforce policies on hundreds of millions of URLs in more than 80 categories.

Secure – Security

Cisco ASA 5500-X Series

WEB

| Overview | **Positioning Map** | Platform Spec | Licenses |

ASA 5585-X

ASA 5555-X

ASA 5545-X

ASA 5525-X

ASA 5516-X

ASA 5508-X

ASA 5506-X

Throughput   → High

Secure - Security

Cisco ASA 5500-X Series

WEB

Overview	Positioning Map	**Platform Spec**	Licenses

Product SKU	Service (CSE) SKU	Throughput			AVC Sessions		VPN Peers	GE Ports	11n Wireless AP	Power Supply	Fanless	Rack Mount
		FW AVC	FW AVC IPS	VPN	Concurrent Sessions	New Connections per Second						
ASA5506-FTD-K9	CON-SMBS-ASAK506F	250 Mbps	125 Mbps	100 Mbps	20,000	3,000	50	8	-	External	●	–*1
ASA5506W-x-FTD-K9	CON-SMBS-ASAxxxxW	250 Mbps	125 Mbps	100 Mbps	20,000	3,000	50	8	●	External	●	–*1
ASA5506H-FTD-K9	CON-SMBS-ASAD506H	250 Mbps	125 Mbps	100 Mbps	20,000	3,000	50	4	-	External	●	–*2
ASA5508-FTD-K9	CON-SMBS-ASD5508F	450 Mbps	250 Mbps	175 Mbps	100,000	7,000	100	8	-	External	-	1 RU
ASA5516-FTD-K9	CON-SMBS-ASA5K16F	850 Mbps	450 Mbps	250 Mbps	250,000	8,000	300	8	-	External	-	1 RU

*1 Rack Mount Kit (ASA5506-RACK-MNT=) is required.   Optional Wall Mount Kit (ASA5506-WALL-MNT=) is available.

*2 Rack Mount Kit (ASA5506-RACK-MNT=) is required.   Optional Wall Mount Kit (ASA5506-WALL-MNT=) and DIN Rail Mount Kit (ASA5506H-DIN-MNT=) are available.

Secure - Security

Cisco ASA 5500-X Series

Overview	Positioning Map	Platform Spec	Licenses

Cisco Firepower Threat Defense Software Image & Licenses

The Cisco ASA 5500-X Series ships with the Cisco Firepower Threat Defense software image. It includes Application Visibility and Control (AVC), and optional Next-Generation IPS (NGIPS), Cisco Advanced Malware Protection (AMP) for Networks, and URL Filtering.

● Application Visibility and Control (AVC)

Supports more than 3,000 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 below 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 licenses, or bundled with AMP, or with AMP and URL licenses.

● Cisco Advanced Malware Protection (AMP) for Networks

Delivers inline network protection against sophisticated malware and Cisco Threat Grid sandboxing. The AMP licenses can be added alone to the base 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 licenses, or bundled with NGIPS, or with NGIPS and AMP licenses.

Cisco Firepower Threat Defense License Comparison

Licenses	Characters Included in Product SKU	Next-Generation IPS (NGIPS)	Advanced Malware Protection (AMP)	URL Filtering (URL)
NGIPS License	T	●	-	-
AMP License	AMP	-	●	-
URL License	URL	-	-	●
NGIPS & AMP License	TM	●	●	-
NGIPS & URL License	TC	●	-	●
NGIPS & AMP & URL License	TMC	●	●	●

Secure – Security

Cisco ASA 5500-X Series

| Overview | Positioning Map | Platform Spec | Licenses |

Cisco Firepower Threat Defense NGIPS Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-T-1Y	L-ASA5506T-T-3Y	L-ASA5506T-T-5Y	ASA 5506
L-ASA5506WT-T-1Y	L-ASA5506WT-T-3Y	L-ASA5506WT-T-5Y	ASA 5506W
L-ASA5506HT-T-1Y	L-ASA5506HT-T-3Y	L-ASA5506HT-T-5Y	ASA 5506H
L-ASA5508T-T-1Y	L-ASA5508T-T-3Y	L-ASA5508T-T-5Y	ASA 5508
L-ASA5516T-T-1Y	L-ASA5516T-T-3Y	L-ASA5516T-T-5Y	ASA 5516

*1　L-ASAxxxxT-T= is required (The "xxxx" corresponds to the supported models).

Cisco Firepower Threat Defense AMP Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-AMP-1Y	L-ASA5506T-AMP-3Y	L-ASA5506T-AMP-5Y	ASA 5506
L-ASA5506WT-AMP-1Y	L-ASA5506WT-AMP-3Y	L-ASA5506WT-AMP-5Y	ASA 5506W
L-ASA5506HT-AMP-1Y	L-ASA5506HT-AMP-3Y	L-ASA5506HT-AMP-5Y	ASA 5506H
L-ASA5508T-AMP-1Y	L-ASA5508T-AMP-3Y	L-ASA5508T-AMP-5Y	ASA 5508
L-ASA5516T-AMP-1Y	L-ASA5516T-AMP-3Y	L-ASA5516T-AMP-5Y	ASA 5516

*1　L-ASAxxxxT-AMP= is required (The "xxxx" corresponds to the supported models).

Cisco Firepower Threat Defense URL Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-URL-1Y	L-ASA5506T-URL-3Y	L-ASA5506T-URL-5Y	ASA 5506
L-ASA5506WT-URL-1Y	L-ASA5506WT-URL-3Y	L-ASA5506WT-URL-5Y	ASA 5506W
L-ASA5506HT-URL-1Y	L-ASA5506HT-URL-3Y	L-ASA5506HT-URL-5Y	ASA 5506H
L-ASA5508T-URL-1Y	L-ASA5508T-URL-3Y	L-ASA5508T-URL-5Y	ASA 5508
L-ASA5516T-URL-1Y	L-ASA5516T-URL-3Y	L-ASA5516T-URL-5Y	ASA 5516

*1　L-ASAxxxxT-URL= is required (The "xxxx" corresponds to the supported models).

Secure - Security

Cisco ASA 5500-X Series

WEB

Overview	Positioning Map	Platform Spec	Licenses

Cisco Firepower Threat Defense NGIPS & AMP Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-TM-1Y	L-ASA5506T-TM-3Y	L-ASA5506T-TM-5Y	ASA 5506
L-ASA5506WT-TM-1Y	L-ASA5506WT-TM-3Y	L-ASA5506WT-TM-5Y	ASA 5506W
L-ASA5506HT-TM-1Y	L-ASA5506HT-TM-3Y	L-ASA5506HT-TM-5Y	ASA 5506H
L-ASA5508T-TM-1Y	L-ASA5508T-TM-3Y	L-ASA5508T-TM-5Y	ASA 5508
L-ASA5516T-TM-1Y	L-ASA5516T-TM-3Y	L-ASA5516T-TM-5Y	ASA 5516

*1   L-ASAxxxxT-TM= is required (The "xxxx" corresponds to the supported models).

Cisco Firepower Threat Defense NGIPS & URL Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-TC-1Y	L-ASA5506T-TC-3Y	L-ASA5506T-TC-5Y	ASA 5506
L-ASA5506WT-TC-1Y	L-ASA5506WT-TC-3Y	L-ASA5506WT-TC-5Y	ASA 5506W
L-ASA5506HT-TC-1Y	L-ASA5506HT-TC-3Y	L-ASA5506HT-TC-5Y	ASA 5506H
L-ASA5508T-TC-1Y	L-ASA5508T-TC-3Y	L-ASA5508T-TC-5Y	ASA 5508
L-ASA5516T-TC-1Y	L-ASA5516T-TC-3Y	L-ASA5516T-TC-5Y	ASA 5516

*1   L-ASAxxxxT-TC= is required (The "xxxx" corresponds to the supported models).

Cisco Firepower Threat Defense NGIPS & AMP & URL Licenses for Cisco ASA 5500-X Series

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-ASA5506T-TMC-1Y	L-ASA5506T-TMC-3Y	L-ASA5506T-TMC-5Y	ASA 5506
L-ASA5506WT-TMC-1Y	L-ASA5506WT-TMC-3Y	L-ASA5506WT-TMC-5Y	ASA 5506W
L-ASA5506HT-TMC-1Y	L-ASA5506HT-TMC-3Y	L-ASA5506HT-TMC-5Y	ASA 5506H
L-ASA5508T-TMC-1Y	L-ASA5508T-TMC-3Y	L-ASA5508T-TMC-5Y	ASA 5508
L-ASA5516T-TMC-1Y	L-ASA5516T-TMC-3Y	L-ASA5516T-TMC-5Y	ASA 5516

*1   L-ASAxxxxT-TMC= is required (The "xxxx" corresponds to the supported models).

Secure - Security

Cisco Firepower 2100 Series

WEB

| **Overview** | **Positioning Map** | **Platform Spec** | **Licenses** |

▌ Business Resiliency through Superior Threat Defense

The Cisco Firepower 2100 Series is the industry's first fully integrated, threat-focused Next-Generation FireWall (NGFW) with unified management. It delivers business resiliency through superior security with sustained performance—provides sustained network performance when threat inspection features are activated to keep your business running securely. And It is now simpler to manage for improved IT efficiency and a lower total cost of ownership.

The Firepower 2100 NGFWs sustain its throughput performance as threat services are added. They do this by uniquely incorporating an innovative dual multi-core CPU architecture that optimizes firewall, cryptographic, and threat inspection functions simultaneously. They won't become a network bottleneck or lose effectiveness like competitors when threat inspection is turned on. Now, achieving security doesn't come at the expense of network performance.

▌ Highlights

● **Stop more threats**: Contain known and unknown malware with leading Cisco AMP and sandboxing.

● **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.
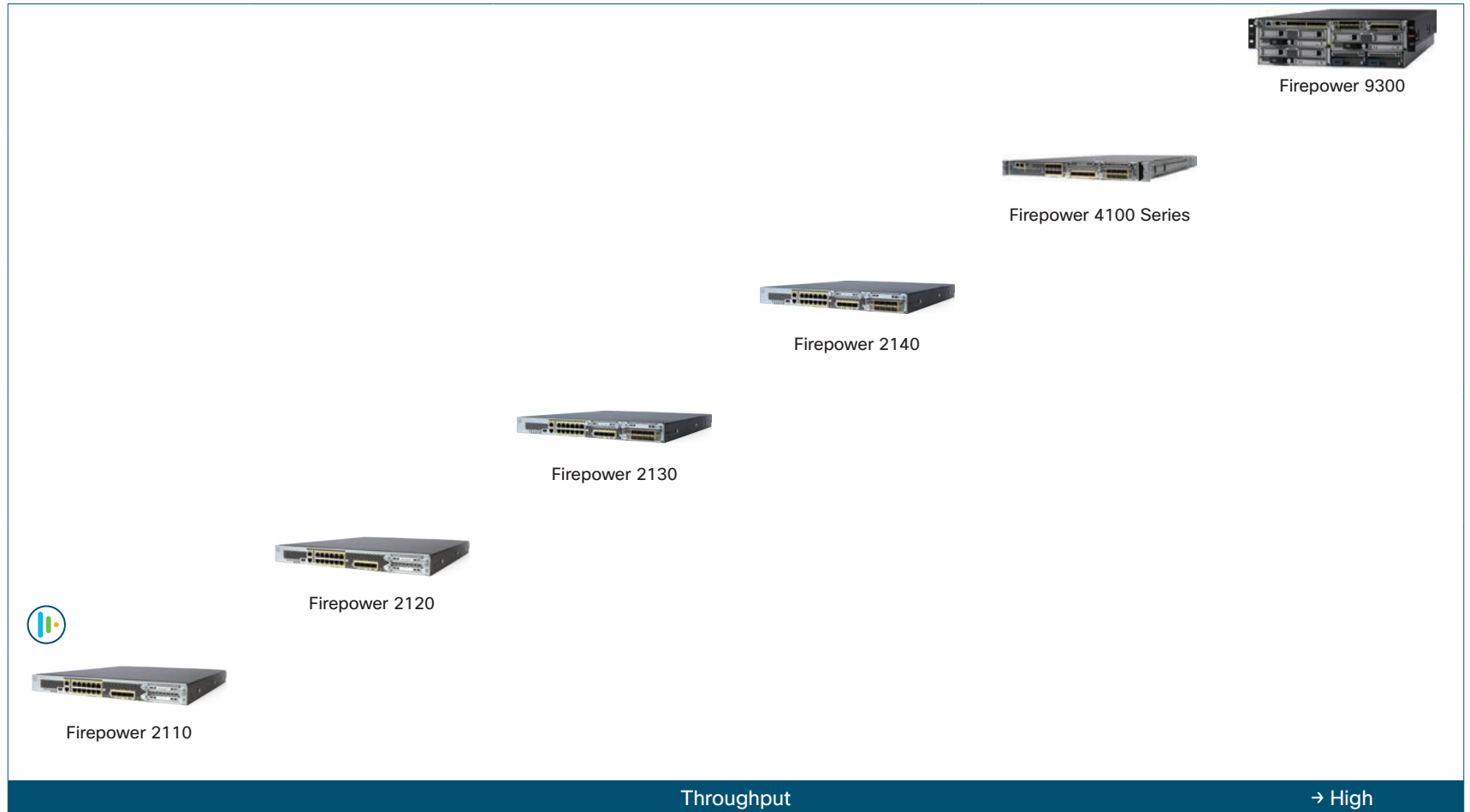
Secure - Security
Cisco Firepower 2100 Series

| Overview | **Positioning Map** | Platform Spec | Licenses |

Firepower 9300

Firepower 4100 Series

Firepower 2140

Firepower 2130

Firepower 2120

Firepower 2110

Throughput   → High

Secure – Security

Cisco Firepower 2100 Series

WEB

| Overview | Positioning Map | **Platform Spec** | Licenses |

Product SKU	Service (CSE) SKU	Throughput			AVC Sessions		VPN Peers	Ports		Power Supply	Rack Mount
		FW AVC	FW AVC IPS	VPN	Concurrent Sessions	New Connections per Second		GE	SFP		
FPR2110-NGFW-K9	–	2 Gbps	2 Gbps	250 Mbps	1,000,000	12,000	1,500	12	4	Internal	1 RU

Cisco Firepower 2100 Series

WEB

Overview	Positioning Map	Platform Spec	Licenses

Cisco Firepower Threat Defense NGIPS Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-T-1Y	L-FPR2110T-T-3Y	L-FPR2110T-T-5Y	Firepower 2110

*1　L-FPR2110T-T= is required.

Cisco Firepower Threat Defense AMP Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-AMP-1Y	L-FPR2110T-AMP-3Y	L-FPR2110T-AMP-5Y	Firepower 2110

*1　L-FPR2110T-AMP= is required.

Cisco Firepower Threat Defense URL Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-URL-1Y	L-FPR2110T-URL-3Y	L-FPR2110T-URL-5Y	Firepower 2110

*1　L-FPR2110T-URL= is required.

Cisco Firepower Threat Defense NGIPS & AMP Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-TM-1Y	L-FPR2110T-TM-3Y	L-FPR2110T-TM-5Y	Firepower 2110

*1　L-FPR2110T-TM= is required.

Cisco Firepower Threat Defense NGIPS & URL Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-TC-1Y	L-FPR2110T-TC-3Y	L-FPR2110T-TC-5Y	Firepower 2110

*1　L-FPR2110T-TC= is required.

Cisco Firepower Threat Defense NGIPS & AMP & URL Licenses for Cisco Firepower 2110

Product SKU*1			Compatible Models
1-Year	3-Years	5-Years	
L-FPR2110T-TMC-1Y	L-FPR2110T-TMC-3Y	L-FPR2110T-TMC-5Y	Firepower 2110

*1　L-FPR2110T-TMC= is required.

Secure - Security

Cisco AnyConnect Secure Mobility Client

WEB

Overview	Features	Licenses

▍ Easy to Use, Highly Secure, Much More than a VPN

The industry-leading Cisco AnyConnect Secure Mobility Client is a modular endpoint software product. 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 such as compliance through the VPN with Cisco ASA or through wired, wireless, and VPN with Cisco Identity Services Engine (ISE), web security along side Cisco Cloud Web Security (CWS), network visibility into endpoint flows within Cisco Stealthwatch, or off-network roaming protection with Cisco Umbrella.

Cisco AnyConnect clients are available across a broad set of platforms, including Windows, macOS, Linux, iOS, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.

Basic VPN	Advanced VPN	Endpoint Compliance	Inspection Services	Enterprise Access	Threat Protection	Network Visibility	CCNS Plugin

AnyConnect Features

Integration with Other Cisco Solutions

ASA	ISR/RV	ASR/CSR	ISE	CWS/WSA	Catalyst/WC	NetFlow Collectors	AMP	Umbrella

Secure - Security

Cisco AnyConnect Secure Mobility Client

WEB

| Overview | Features | Licenses |

Feature	Description
Unified Endpoint Compliance	The Cisco AnyConnect ISE Posture Module in Cisco ISE deployments provides unified endpoint posture checks and automated remediation across wired, wireless, and VPN environments. This module serves as the main source of endpoint posture checking for OS levels, latest antivirus/spyware/malware updates, application and hardware inventory and other endpoint checks to determine compliance state and strengthen endpoint security. For VPN only environments, the Cisco ASA provides endpoint posture using Cisco AnyConect Hostscan Module.
Highly Secure Network Access	The Cisco AnyConnect Network Access Manager provides superior connectivity features. Administrators can control which networks or resources for endpoints to connect. It provides an IEEE 802.1X supplicant that can be provisioned as part of authentication, authorization, and accounting (AAA) capabilities along with some unique encryption technologies such as MACsec IEEE 802.1AE.
Web Security	A built-in Cisco AnyConnect module implements web security either through the on-premise Cisco Web Security Appliance (WSA) or the cloud-based Cisco Cloud Web Security (CWS) offering. Combining web security with VPN access, administrators can provide comprehensive, highly secure mobility to all end users, which is vital for bring-your-own-device (BYOD) deployments. Enterprises have a choice of deployments to defend the network against web malware and to control and safeguard web usage.
Network Visibility	The Cisco AnyConnect Network Visibility Module on Windows, macOS, Linux, and Samsung Knox-enabled devices gives administrators the ability to monitor endpoint application usage to uncover potential behavior anomalies and to make more informed network design decisions. Usage data can be shared with NetFlow analysis tools such as Cisco Stealthwatch.
Off-Network Protection (DNS-Layer Security)	Cisco Umbrella Roaming is a cloud-delivered security service that protects devices when they are off the corporate network. Whether users turn off the VPN or forget to turn it on, Umbrella Roaming enforces security at the DNS layer to protect against malware, phishing, and command-and-control callbacks over any port or protocol.
Mobile Device Support	Administrators need to support end-user productivity by providing personal mobile devices with remote access to the company network. Cisco AnyConnect services can be deployed on the most popular devices used by today's diverse workforce. Highly secure remote access can either be device-based or through select per-application VPN, which eliminates unapproved applications from accessing confidential business resources further reducing malware intrusion risks and bandwidth costs for remote access.
Servers and Platforms	Cisco AnyConnect services are used in conjunction with numerous Cisco head server platforms, including but not limited to the Cisco ASA (physical and virtual), Cisco Firepower Next-Generation Firewalls (physical and virtual/ASA and FTD operating systems), Cisco Identity Services Engine (ISE), Cisco Aggregation Services Routers (ASR), Cisco Cloud Web Security (CWS), and Cisco IOS software on Cisco ISR. Headend termination devices and cloud services, along with the associated service costs and support contracts, are purchased separately.

Secure - Security

Cisco AnyConnect Secure Mobility Client

WEB

Overview   **Features**   **Licenses**

Cisco AnyConnect Licenses

The Cisco AnyConnect offers simplified licensing to meet the needs of the broad enterprise IT community as it adapts to growing end-user mobility demands. The current AnyConnect 4.x collapses the formerly complex AnyConnect licensing model into two simple tiers: the first is AnyConnect Plus and the second is AnyConnect Apex.

● **Cisco AnyConnect Plus License**

Includes basic VPN services such as device and per-application VPN (including third-party IKEv2 remote access VPN headend support), trusted network detection, basic device context collection, and Federal Information Processing Standards (FIPS) compliance. AnyConnect Plus also includes other non-VPN services such as the AnyConnect Network Access Manager 802.1X supplicant, the Cisco Cloud Web Security (CWS) module, and the Cisco Umbrella Roaming module. Existing AnyConnect customers should think of AnyConnect Plus as similar to the previous AnyConnect Essentials.

● **Cisco AnyConnect Apex License**

Includes more advanced services such as endpoint posture checks (Hostscan through ASA VPN, or ISE Posture through the Cisco Identity Services Engine), network visibility, next-generation VPN encryption (including Suite B), and clientless remote access VPN as well as all the capabilities of AnyConnect Plus. Existing AnyConnect customers should think of AnyConnect Apex as similar to previous AnyConnect Premium and Premium Shared Licenses.

AnyConnect Plus and Apex licenses offer a set of features and deployment flexibility to meet a wide range of your enterprise's requirements. For enterprises that want only AnyConnect for remote access use cases, there is also the **Cisco AnyConnect VPN Only License**.

Cisco AnyConnect Plus & Apex 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	-	●
SAML authentication[*4]	-	●

*1   Cisco Umbrella Roaming License is required.
*2   Cisco AMP for Endpoints License is required.
*3   Cisco ISE Apex License is required.
*4   Cisco ASA 9.7.1 or later is required.

Secure – Security
Cisco AnyConnect Secure Mobility Client

WEB

Overview	Features	Licenses

Cisco AnyConnect Plus Licenses

Product SKU[1] [2]			User Range
1-Year	3-Years	5-Years	
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

[1]   Refer to the Ordering Guide for a full list of SKUs supporting over 500 users.
[2]   L-AC-PLS-LIC= is required.

Product SKU[1] [2]	Users
Perpetual	
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

[1]   Refer to the Ordering Guide for a full list of SKUs supporting over 500 users.
[2]   L-AC-PLS-P-G is required.

Cisco AnyConnect Apex Licenses

Product SKU[1] [2]			User Range
1-Year	3-Years	5-Years	
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

[1]   Refer to the Ordering Guide for a full list of SKUs supporting over 500 users.
[2]   L-AC-APX-LIC= is required.

Cisco AnyConnect VPN Only Licenses

Product SKU[1] [2]	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]   Refer to the Ordering Guide for a full list of SKUs supporting over 500 users.

Secure - Security

Cisco Advanced Malware Protection for Endpoints

WEB

Overview   **Licenses**   **AMP Everwhere**

▌ Cloud-Managed Next-Generation Endpoint Security

The **Cisco Advanced Malware Protection (AMP) for Endpoints** is a cloud-managed endpoint security solution that provides the visibility, context, and control to 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.
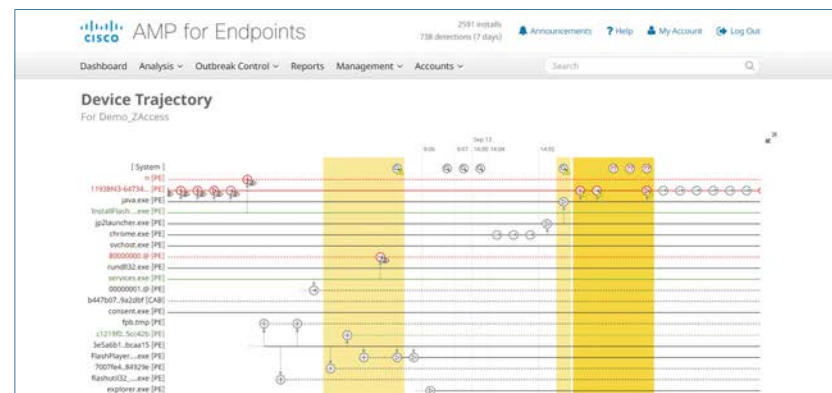
● **Prevent**: Strengthen defenses using the best global threat intelligence and block malware in real time
● **Detect**: Continuously monitor and record all file activity to quickly detect stealthy malware
● **Respond**: Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, servers and mobile devices (Android and iOS)

▌ Threat Intelligence and Dynamic Malware Analysis

The Cisco AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the **Cisco Talos Security Intelligence Group**, and **Cisco Threat Grid** intelligence feeds.
Organizations benefit from:

● 1.5 million incoming malware samples per day
● 1.6 million global sensors
● 100 terabytes of data per day
● 13 billion web requests
● Team of engineers, technicians, and researchers
● 24-hour operations

Cisco AMP for Endpoints is managed through an easy-to-use, web-based console. It is deployed through AMP's lightweight endpoint connector, with no 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, servers and mobile devices (Android and iOS).
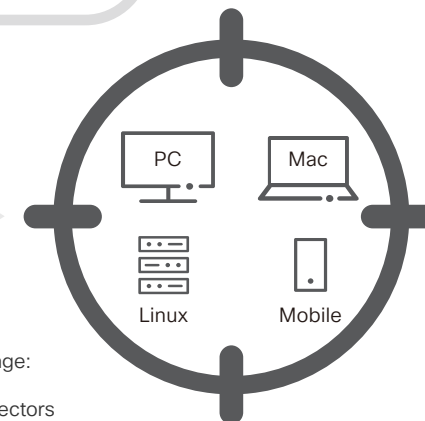

Managed through an easy-to-use, web-based console

Analysis is Done in the Cloud

Powered by Talos

Visibility

Context

Control

PC   Mac

Linux   Mobile

Broad Endpoint Coverage:
Lightweight
AMP for Endpoints Connectors

Secure - Security

Cisco Advanced Malware Protection for Endpoints

WEB

Overview	Licenses	AMP Everwhere

Cisco AMP for Endpoints Connector Licenses

Product SKU[1] [2]			Connector Range
1-Year	3-Years	5-Years	
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

*1   Refer to the Ordering Guide for a full list of SKUs supporting over 500 users.
*2   FP-AMP-LIC= is required.

Cisco AMP Virtual Private Cloud Appliance

Product SKU[1]	Max Connectors
FP-AMP-CLOUD-SW	10,000

*1   FP-AMP-CLOUD-BUN and Cisco AMP for Endpoints Connector License are required.

TIP Software Requirements

Connector	Supported OS
Cisco AMP Windows Connector	● Microsoft Windows 7 ● Microsoft Windows 8 and 8.1 ● Microsoft Windows 10 ● Microsoft Windows Server 2008 ● Microsoft Windows Server 2012
Cisco AMP Mac Connector	● Mac OS X 10.7 and later
Cisco AMP Linux Connector	● Linux Red Hat Enterprise 6.5, 6.6, 6.7, 6.8, 7.2, and 7.3 ● Linux CentOS 6.4, 6.5, 6.6, 6.7, 6.8, 7.2 and 7.3
Cisco AMP Mobile	● Android version 2.1 and later ● MDM supervised iOS version 11

Secure - Security

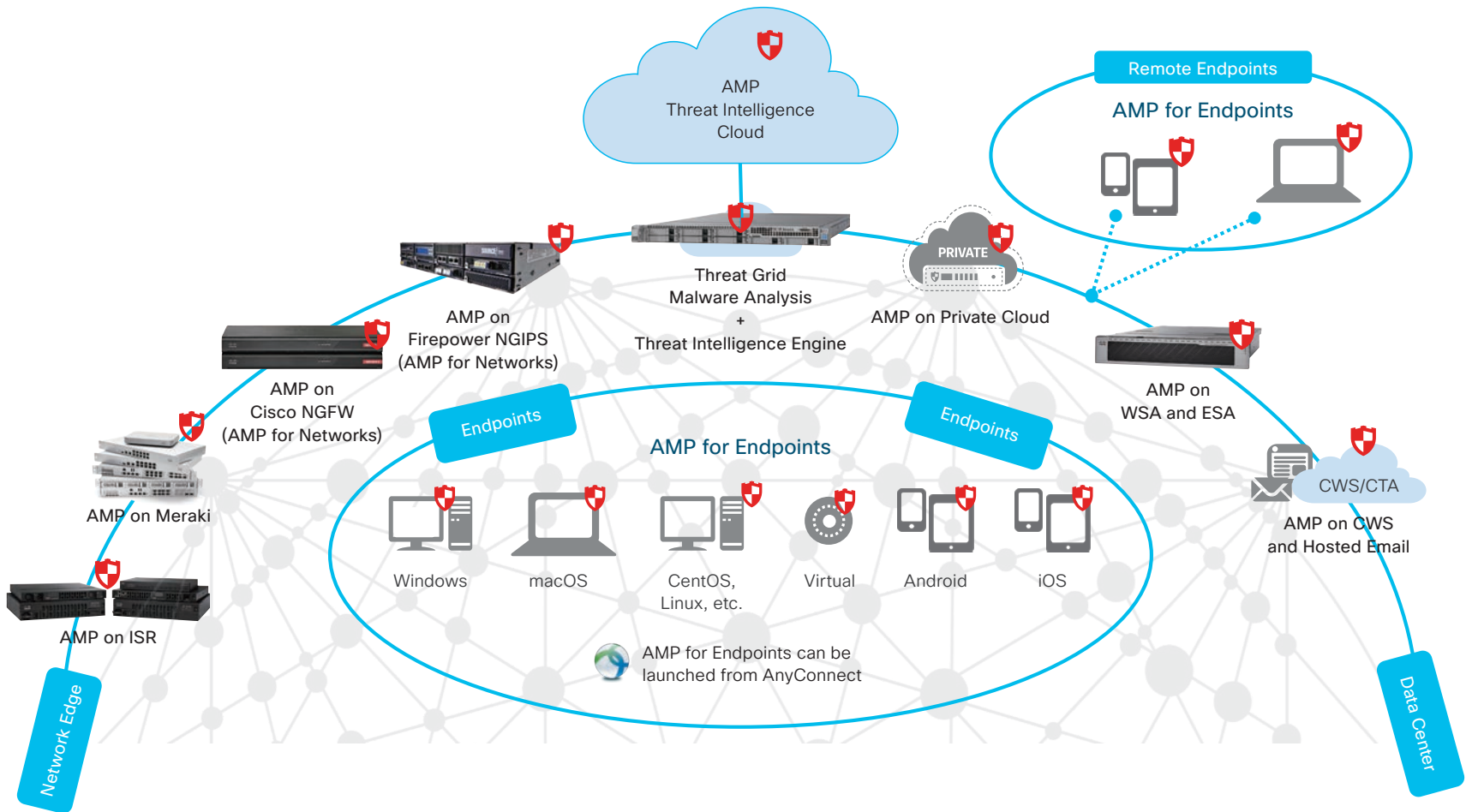# Cisco Advanced Malware Protection for Endpoints

WEB

| Overview | Licenses | **AMP Everwhere** |

Find the Best AMP Deployment for You

The **Cisco Advanced Malware Protection (AMP)** is subscription-based, managed through a web-based management console, and deployed on a variety of platforms.

AMP
Threat Intelligence
Cloud

Remote Endpoints

AMP for Endpoints

AMP on
Firepower NGIPS
(AMP for Networks)

Threat Grid
Malware Analysis
+
Threat Intelligence Engine

PRIVATE

AMP on Private Cloud

AMP on
Cisco NGFW
(AMP for Networks)

AMP on
WSA and ESA

AMP on Meraki

Endpoints

AMP for Endpoints

Endpoints

CWS/CTA

AMP on CWS
and Hosted Email

Windows   macOS   CentOS,   Virtual   Android   iOS
                     Linux, etc.

AMP on ISR

AMP for Endpoints can be
launched from AnyConnect

Network Edge

Data Center

Secure - Security

Cisco Umbrella

WEB

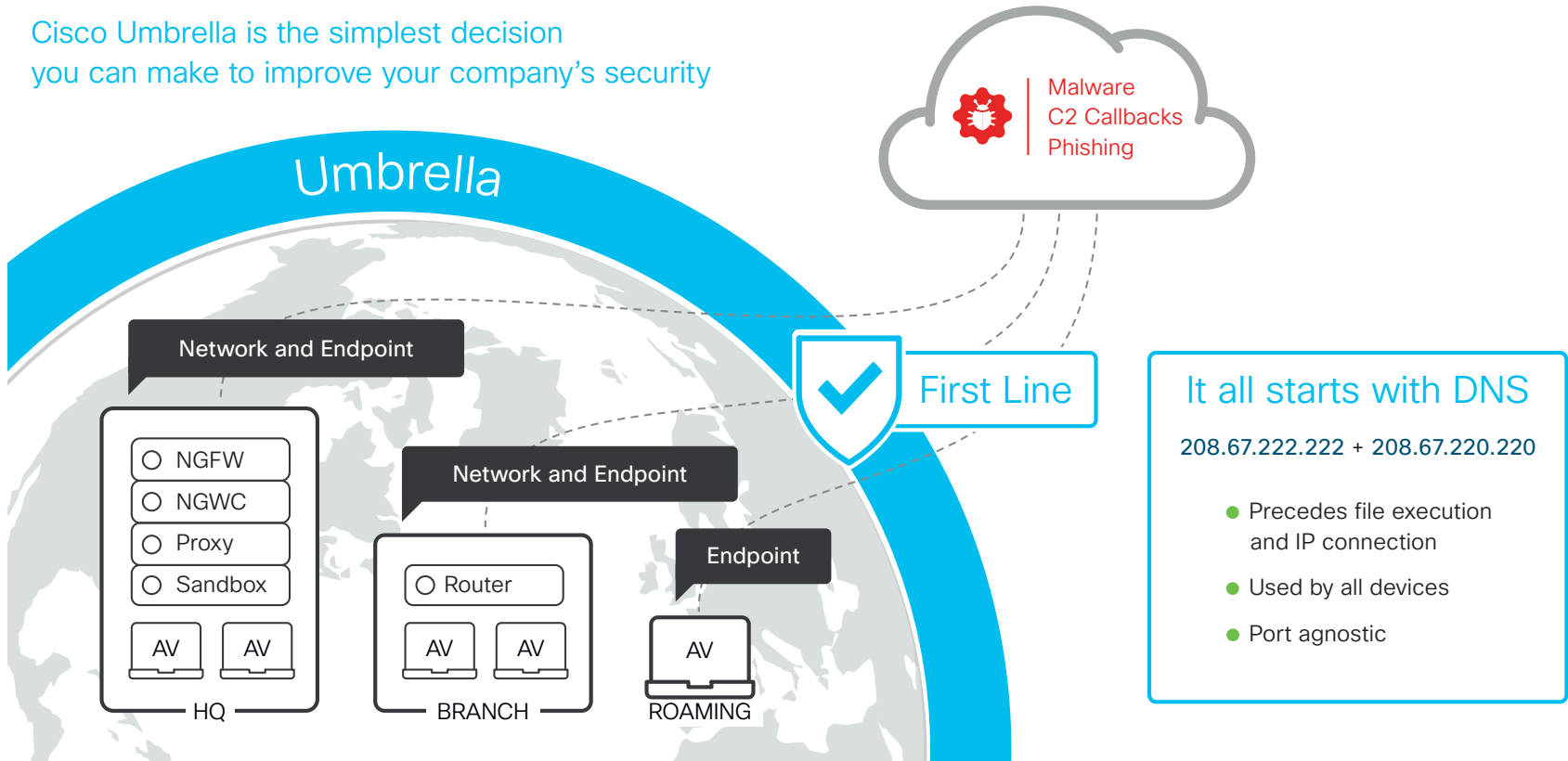| **Overview** | **Features** | **Licenses** | **Promotions** |

▌The Fastest and Easiest Way to Protect All of Your Users in Minutes

The Cisco Umbrella is the industry's first Secure Internet Gateway that provides the first line of defense against threats on the internet wherever users go. Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network or endpoints. As a cloud-delivered, open platform, Umbrella integrates easily with your existing security stack and delivers live threat intelligence about current and emerging threats.

Because it is delivered from the cloud, there is no hardware to install or software to manually update. You can provision all on-network devices — including BYOD and IoT — in minutes and use your existing Cisco footprint — AnyConnect, Wireless Controller, Integrated Services Router (ISR), and so on — to quickly provision thousands of network egresses and roaming laptops. Additionally, with the Cisco Security Connector app, you can use the Umbrella extension to protect supervised iOS 11 devices.

Cisco Umbrella is the simplest decision
you can make to improve your company's security

Umbrella

Malware
C2 Callbacks
Phishing

Network and Endpoint

NGFW
NGWC
Proxy
Sandbox

AV AV

HQ

Network and Endpoint

Router

AV AV

BRANCH

Endpoint

AV

ROAMING

First Line

It all starts with DNS

208.67.222.222 + 208.67.220.220

- Precedes file execution and IP connection
- Used by all devices
- Port agnostic

Secure – Security
Cisco Umbrella

WEB

Overview	**Features**	Licenses	Promotions

Package		Roaming	Branch	WLAN	Professional	Insights	Platform
Best for		AnyConnect NGFW	ISR 4000	Wireless Controllers	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	●*1	●*3	●*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	●*2	●	●	●	●	●
	Enforcement & Visibility per Internal Network or AD User/Group	–	●*4	●*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 Off-network only. *2 Only has allow list and 1 built-in block page. *3 On-network only.
*4 Only per internal network (no Active Directory). *5 Per SSID, access point, AP group, and user group (no Active Directory).

Secure - Security
Cisco Umbrella

Overview	Features	Licenses	Promotions

Cisco Umbrella Roaming License

Product SKU*1	Description
UMB-ROAM	Umbrella Roaming per User License

*1   UMBRELLA-SUB is required.

Cisco Umbrella Branch Licenses

Product SKU	Description
UMB-BRAN-4221	Umbrella Branch License for Cisco ISR 4321
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

*1   UMBRELLA-SUB is required.

Cisco Umbrella WLAN License

Product SKU*1	Description
UMB-WLAN	Umbrella WLAN per Access Point License

*1   UMBRELLA-SUB is required.

Cisco Umbrella Professional License

Product SKU*1	Description
UMB-PROFESSIONAL	Umbrella Professional per User License

*1   UMBRELLA-SUB is required.

Cisco Umbrella Insights License

Product SKU*1	Description
UMB-INSIGHTS-K9	Umbrella Insights per User License

*1   UMBRELLA-SUB is required.

Cisco Umbrella Platform License

Product SKU*1	Description
UMB-PLATFORM-K9	Umbrella Platform per User License

*1   UMBRELLA-SUB is required.

Secure - Security
Cisco Umbrella

WEB

| Overview | Features | Licenses | **Promotions** |

Promotion Prices & Trial

OpenDNS Home	OpenDNS Home VIP	Umbrella 14 Day Trial	Umbrella Professional
FREE	**US$ 19.95/year**	**FREE**	**US$ 38/year**
Our classic, free service with customizable filtering and identity theft protection	OpenDNS Home package plus one year of usage stats and optional white-list mode	Get start in 30 seconds No credit card or phone call required	Per user (10 to 90 users) Cisco Promotion Price

Free Umbrella 14-Day Trial (https://signup.opendns.com/freetrial)

If you want to add an additional layer of DNS security to your router or firewall, try our free trial—you can set it up yourself in less than five minutes, no credit card or phone call required.

Umbrella Professional: Best for Small Companies (https://umbrella.cisco.com/products/small-teams)

This is Cisco's direct sale promotion price via on-line credit card settlement. Cisco authorized distributors are also offering even more attractive promotion pricing for various umbrella packages. Actual purchase price will be determined between purchaser & reseller of your choice.

Secure - Security

Cisco Meraki MX Cloud Managed Security Appliances

WEB

| **Overview** | **Positioning Map** | **Platform Spec** | **Licenses & Accessories** |

█ 100 % Centralized Cloud Management for Security, Networking, and Application Control

The Cisco Meraki MX Cloud Managed Security Appliances are ideal for organizations considering a Unified Threat Managment (UTM) solution, for distributed sites, campuses or datacenter VPN concentration. Since the MX is 100 % cloud managed, installation and remote management is simple. The MX has a comprehensive suite of network services, eliminating the need for multiple appliances.

These services include SD-WAN capabilities, application-based firewalling, content filtering, web search filtering, SNORT based intrusion detection and prevention, Cisco Advanced Malware Protection (AMP), web caching, 4G cellular failover and more. Auto VPN and SD-WAN features are available on our hardware and virtual appliances, configurable in Amazon Web Services.
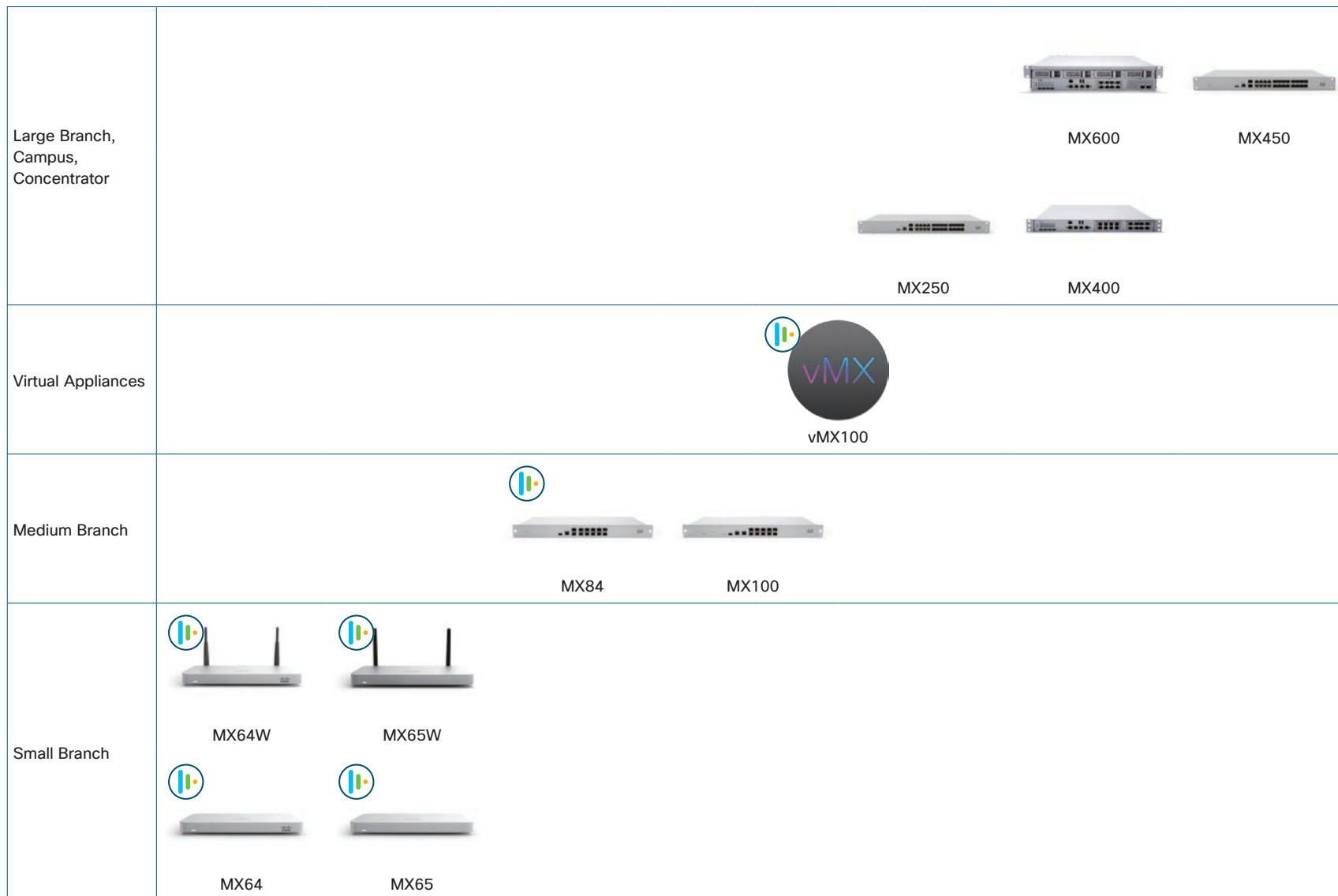

█ Highlights

● **Identity-Based Firewall**: Automatically assigns firewall and traffic shaping rules, VLAN tags, and bandwidth limits to enforce the right policies for each class of users

● **Intrusion Prevention**: Protects critical network resources from the latest security threats and vulnerabilities

● **Auto VPN**: Securely connects branch locations using mesh or hub-and-spoke topologies. Provides simple VPN access into Amazon Web Services

● **Content Filtering**: Block undesirable web content across 70+ categories, and leverage cloud lookups to filter billions of URLs

● **Advanced Malware Protection**: Protect your network against malware using the latest threat intelligence, and identify previously unknown malicious files with retrospective detection

● **High Availability & Failover**: Provides device and connection integrity through multiple uplinks, warm spare failover, and self-healing VPN

● **Application Visibility & Control**: Identify which applications are being used, and then prioritize critical apps while limiting recreational apps

● **Centralized Management**: Seamlessly manage campus-wide Wi-Fi deployments and distributed multi-site networks from a single pane-of-glass

Cisco Meraki MX Cloud Managed Security Appliances

Overview   **Positioning Map**   Platform Spec   Licenses & Accessories

Large Branch, Campus, Concentrator	MX600 MX450 MX250 MX400	
Virtual Appliances	vMX100	
Medium Branch	MX84 MX100	
Small Branch	MX64W MX65W MX64 MX65	

Throughput   → High

Secure - Security

Cisco Meraki MX Cloud Managed Security Appliances

WEB

| Overview | Positioning Map | Platform Spec | Licenses & Accessories |

Product SKU	Recommended Clients	Throughput			Concurrent VPN Tunnels	Web Caching	WAN Ports	WAN/LAN Ports	LAN Ports			Wireless		Power Supply	Rack Mount
		Stateful Firewall	Advanced Security	VPN			GE	GE	GE	GE PoE+	SFP	11ac AP	4G LTE		
MX64-HW	50	250 Mbps	200 Mbps	100 Mbps	50	–	1	1	4	–	–	–	–*2	External	–*2
MX64W-HW	50	250 Mbps	200 Mbps	100 Mbps	50	–	1	1	4	–	–	●	–*2	External	–*2
MX65-HW	50	250 Mbps	200 Mbps	100 Mbps	50	–	2	–	8	2	–	–	–*2	External	–*2
MX65W-HW	50	250 Mbps	200 Mbps	100 Mbps	50	–	2	–	8	2	–	●	–*2	External	–*2
MX84-HW	200	500 Mbps	320 Mbps	250 Mbps	100	1 TB	2	–	8	–	2	–	–*2	Internal	1 RU
vMX100	–	–	–	500 Mbps	–	–	–	–	–	–	–	–	–	–	–

*1   Cellular Modem is required.

*2   Desktop or Wall mountable with included mount hardware.

Secure - Security

Cisco Meraki MX Cloud Managed Security Appliances

WEB

| Overview | Positioning Map | Platform Spec | **Licenses & Accessories** |

Cisco Meraki Enterprise Licenses for Cisco Meraki MX Series

Product SKU			Compatible Models
1-Year	3-Years	5-Years	
LIC-MX64-ENT-1YR	LIC-MX64-ENT-3YR	LIC-MX64-ENT-5YR	MX64
LIC-MX64W-ENT-1YR	LIC-MX64W-ENT-3YR	LIC-MX64W-ENT-5YR	MX64W
LIC-MX65-ENT-1YR	LIC-MX65-ENT-3YR	LIC-MX65-ENT-5YR	MX65
LIC-MX65W-ENT-1YR	LIC-MX65W-ENT-3YR	LIC-MX65W-ENT-5YR	MX65W
LIC-MX84-ENT-1YR	LIC-MX84-ENT-3YR	LIC-MX84-ENT-5YR	MX84

Cisco Meraki Advanced Security Licenses for Cisco Meraki MX Series

Product SKU			Compatible Models
1-Year	3-Years	5-Years	
LIC-MX64-SEC-1YR	LIC-MX64-SEC-3YR	LIC-MX64-SEC-5YR	MX64
LIC-MX64W-SEC-1YR	LIC-MX64W-SEC-3YR	LIC-MX64W-SEC-5YR	MX64W
LIC-MX65-SEC-1YR	LIC-MX65-SEC-3YR	LIC-MX65-SEC-5YR	MX65
LIC-MX65W-SEC-1YR	LIC-MX65W-SEC-3YR	LIC-MX65W-SEC-5YR	MX65W
LIC-MX84-SEC-1YR	LIC-MX84-SEC-3YR	LIC-MX84-SEC-5YR	MX84

Cisco Meraki Advanced Security Licenses for Cisco Meraki vMX100

Product SKU			Compatible Models
1-Year	3-Years	5-Years	
LIC-VMX100-1YR	LIC-VMX100-3YR	LIC-VMX100-5YR	vMX100

Cisco Meraki License Comparison

	Enterprise	Advanced Security
Stateful Firewall	●	●
Site to Site VPN	●	●
Client VPN	●	●
Branch Routing	●	●
Link Bonding and Failover	●	●
Application Control	●	●
Web Caching	●	●
Content Filtering	-	●
Geo-based IP Firewall	-	●
Google SafeSearch and YouTube for Schools	-	●
Intrusion Detection & Prevention (IDS/IPS)	-	●
Advanced Malware Protection (AMP)	-	●
Cisco Threat Grid[*1]	-	●

*1   Cisco Threat Grid License is required.

Cisco Meraki 1000BASE Small Form-Factor Pluggable (SFP) Modules

SKU	Description	Max Distance	Compatible Series					
			MX64	MX64W	MX65	MX65W	MX84	vMX100
MA-SFP-1GB-TX	1000BASE-T SFP Module	100 m	-	-	-	-	●	-
MA-SFP-1GB-SX	1000BASE-SX SFP Module	550 m	-	-	-	-	●	-
MA-SFP-1GB-LX10	1000BASE-LX10 Module	10 km	-	-	-	-	●	-

Secure - Security

Cisco Meraki Z Cloud Managed Teleworker Gateway

WEB

Overview   **Platform Spec**   **Licenses & Accessories**

Offering Fast, Reliable Connectivity for the Modern Teleworker

The Cisco Meraki Z Cloud Managed Teleworker Gateway is an enterprise class firewall, VPN gateway and router. Each model offers five gigabit ethernet ports and wireless for connectivity. Each model is designed to securely extend the power of Meraki cloud managed networking to employees, IT staff, and executives working from home.

Using Meraki's proven and highly scalable Auto VPN technology, administrators can deploy network services including VoIP and remote endpoints with automatic, zero-touch provisioning. All models feature a high-performance stateful firewall, support for VLANs, inter-VLAN routing, and isolation to segregate corporate data from recreational traffic.

Highlights

- Self-configuring, plug-and-play deployment
- Auto VPN for intelligent site-to-site VPN connectivity
- Layer 7 application traffic shaping and prioritization
- Layer 3 firewall to separate corporate data from personal traffic
- IEEE 802.1x port authentication for wired devices (Meraki Z3)
- USB port for 3G/4G connectivity
- GE downlinks for printers, phones and other wired devices
- PoE output for VoIP phones and other powered devices (Meraki Z3)

- Built-in IEEE 802.11n/ac-compatible wireless access point (Meraki Z3)
- Built-in IEEE 802.11n-compatible wireless access point (Meraki Z1)
- Up to 4 SSIDs with integrated enterprise security and personal/guest access
- Sleek, low profile design
- Optional desk stand (Meraki Z3)

Secure - Security

Cisco Meraki Z Cloud Managed Teleworker Gateway

WEB

Overview   **Platform Spec**   **Licenses & Accessories**

| Product SKU	Recommended Clients	Throughput		WAN Ports	LAN Ports		Wireless			Power Supply	Rack Mount
		Stateful Firewall	VPN	GE	GE	GE PoE+	11n AP	11ac AP	4G LTE		
Z1-HW	5	50 Mbps	10 Mbps	1	4	–	●	–	●	External	–*1
Z3-HW ▬NEW▬	5	100 Mbps	50 Mbps	1	3	1	●	●	●	External	–*2

*1   Desktop or Wall mountable with included mount hardware.

*1   Desktop or Wall mountable with included mount hardware. Vertical Desk Stand (MA-STND-1) is available.
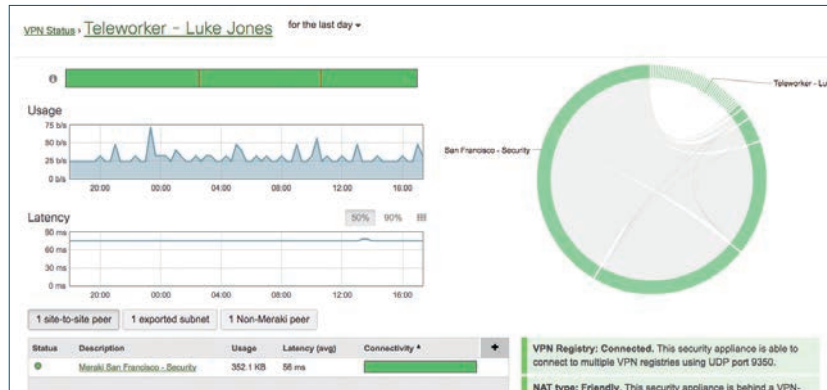
Auto Configuring Site-to-Site VPN

Multi-Site Management via the Meraki Cloud
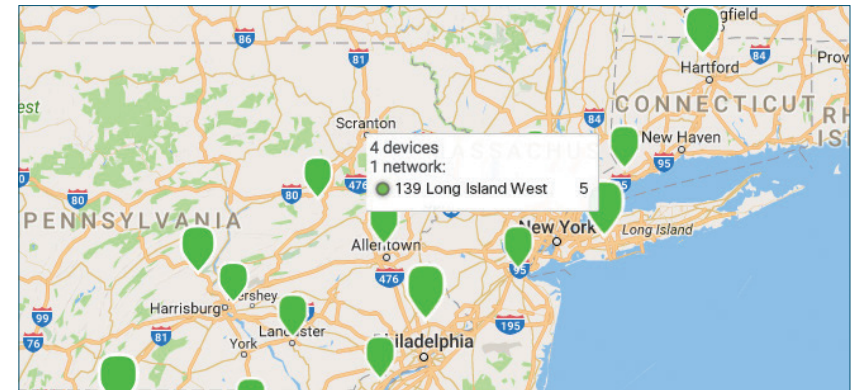
Secure - Security

Cisco Meraki Z Cloud Managed Teleworker Gateway

WEB

Overview	Platform Spec	Licenses & Accessories

Cisco Meraki Enterprise Licenses for Cisco Meraki Z Series

Product SKU					Compatible Models
1-Year	3-Years	5-Years	7-Years	10-Years	
LIC-Z1-ENT-1YR	LIC-Z1-ENT-3YR	LIC-Z1-ENT-5YR	LIC-Z1-ENT-7YR	LIC-Z1-ENT-10YR	Z1
LIC-Z3-ENT-1YR	LIC-Z3-ENT-3YR	LIC-Z3-ENT-5YR	LIC-Z3-ENT-7YR	LIC-Z3-ENT-10YR	Z3

Cisco Meraki Vertical Desk Stand for Cisco Meraki Z3

Product SKU	Description
MA-STND-1	Vertical Desk Stand

Secure - Security
Cisco Meraki MV Cloud Managed Security Cameras

WEB

Overview	**Platform Spec**	**Licenses & Accessories**

▌ Bringing Meraki Magic to the Video Security World

The Cisco Meraki MV Cloud Managed Security Cameras are exceptionally simple to deploy and configure. Their integration into the Meraki dashboard, ease of deployment, and use of cloud-augmented edge storage, eliminate the cost and complexity required by traditional security camera solutions.

Like all Meraki products, MV cameras provide zero-touch deployment. Using just serial numbers, an administrator can add devices to the Meraki dashboard and begin configuration before the hardware even arrives on site. In the Meraki dashboard, users can easily stream video and create video walls for monitoring key areas across multiple locations without ever configuring an IP or installing a plugin.

▌ Highlights

- **Centralized Cloud Management**: The Meraki dashboard provides secure monitoring and management of all your cameras from anywhere in the world
- **Edge Storage**: 128 or 256 GB of high write endurance solid state storage on each camera eliminates the need for an NVR
- **Optimized Retention**: Use motion-based retention and scheduled recording to customize video storage plans for every deployment
- **Advanced Analytics**: Industry-leading analytics and machine learning capabilities onboard each MV12

- **Motion Search**: Dynamically and retroactively select areas of interest in a video stream to find that missing laptop, then export clips directly from the dashboard
- **Encrypted By Default**: Video is encrypted at rest and during transport by default, with automated TLS certificate provisioning
- **Granular Access Controls**: Easily define who can see which video streams, view historical footage, and export video, all from the dashboard
- **Firmware Always Up-to-Date**: Feature releases, firmware updates, and bug fixes are always pushed automatically and at no additional cost with active license

Secure - Security

Cisco Meraki MV Cloud Managed Security Cameras

WEB

| Overview | **Platform Spec** | Licenses & Accessories |

Model	Indoor				Outdoor
Product SKU	MV12N-HW NEW	MV12W-HW NEW	MV12WE-HW NEW	MV21-HW	MV71-HW
Camera	1/3", 4 MP (2,688 × 1,520) progressive CMOS image sensor			1/3.2", 5 MP (2,560 x 1,920) progressive CMOS image sensor	
	3.8 mm focal length f/1.8 minimum aperture	2.8 mm focal length f/1.8 minimum aperture		3 - 10 mm vari-focal lens f/1.3 - 2.5 variable aperture	
	Field of view 73° horizontal 44° vertical 86° diagonal	Field of view 114° horizontal 61° vertical 132° diagonal		Variable field of view 28 - 82° (horizontal) 21 - 61° (vertical) 37 - 107° (diagonal)	
	1/32,000 to 1/30 sec. shutter speed			1/5 to 1/32,000 sec. shutter speed	
	Minimum illumination 0.18 Lux (standard recording) and 0.01 Lux (night mode)			Minimum illumination 0.27 Lux (F1.3, color) and 0.001 Lux (F1.3, B&W)	
	S/N Ratio 52.9 dB			S/N Ratio exceeding 62 dB - Dynamic Range 69 dB	
	Built-in IR illuminators, effective up to 15 m (49 ft)			Built-in IR illuminators, effective up to 30 m (98 feet)	
Video	1080p HD video recording (1,920 × 1,080) with H.264 encoding			720p HD video recording (1,280 x 720) with H.264 encoding	
Storage	256 GB high endurance SSD		128 GB high endurance SSD	128 GB high endurance SSD	
Interface	1 x GE, Dual band IEEE 802.11 a/b/g/n/ac, Bluetooth 4.X (BR/EDR/BLE)			1 x FE	
Power	Power consumption 12.95 W maximum via IEEE 802.3af PoE			Power consumption 10.94 W maximum via IEEE 802.3af PoE	
Dimensions	106 mm x 74 mm (diameter × height)			166 mm x 116.5 mm (diameter × height)	173.3 mm x 115 mm (diameter × height)
Weight	286 g			1,028 g (including mounting plate)	1,482 g (including mounting plate)
Lens Adjustment Range	Fixed			65° Tilt, 350° Rotation, 350° Pan	
Weather-Proof IP66	–			–	●
Vandal-Proof IK10	–			–	●

Cisco Meraki MV Cloud Managed Security Cameras

WEB

Overview	Platform Spec	**Licenses & Accessories**

Cisco Meraki Enterprise Licenses for Cisco Meraki MV Series

Product SKU					Compatible Models
1-Year	3-Years	5-Years	7-Years	10-Years	
LIC-MV-1YR	LIC-MV-3YR	LIC-MV-5YR	LIC-MV-7YR	LIC-MV-10YR	All MV

Cisco Meraki Power Injector for Cisco Meraki MV Series

Product SKU	Description	Compatible Models
MA-INJ-4-xx	PoE Injector (802.3at)	All MV

Cisco Meraki Mount Kits for Cisco Meraki MV Series

Product SKU	Description	Compatible Models				
		MV12N	MV12W	MV12WE	MV21	MV71
MA-MNT-MV-1	Wall Mount Arm	-	-	-	●	●
MA-MNT-MV-2	Pole Mount	-	-	-	-	●
MA-MNT-MV-3	L-Shape Wall Mount Bracket	-	-	-	●	●