Featured Products

Cisco Meraki MX67/68 Cloud Managed Security Appliances

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

MX67-HW

450 Mbps FW Throughput	300 Mbps Adv. Security Throughput	200 Mbps VPN Throughput	50 VPN Peers	
Default AVC	Optional NGIPS	Optional AMP	Optional URL Filtering	
1-port GE-WAN	1-port GE-WAN/LAN	4-port GE-LAN	11ac Wave 2 AP	USB for 4G

MX68CW-HW-WW

450 Mbps FW Throughput	300 Mbps Adv. Security Throughput	200 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	300 Mbps Internal LTE Modem	USB for 4G

Featured Products

Cisco Meraki MV22/32/72 Cloud Managed Smart Cameras

NEW

Bring Powerful, Advanced Analytics to the Typical Security Camera World,
With an Industry-Leading Processor and an Innovative Architecture

MV22-HW

4 MP Image Sensor	3 ~ 9 mm Varifocal Lens	IR Illumination Up to 30 m	Full HD Recording	H.264	256 GB SSD
1-port GE	PoE Input	11ac Wave 2			

MV32-HW

8.4 MP Image Sensor	1.19 mm Focal Lens	360° 4.2MP Recording	H.264	256 GB SSD
1-port GE	PoE Input	11ac Wave 2		

Featured Products

Cisco Meraki Z Cloud Managed Teleworker Gateway

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

Z3C-HW-WW

100 Mbps FW Throughput	50 Mbps VPN Throughput

1-port GE-WAN	3-port GE-LAN	1-port GE-LAN PoE	11ac Wave 2 AP	100 Mbps Internal LTE Modem	USB for 4G	Optional Desk Stand

Featured Products

Cisco Firepower 2100 Series

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

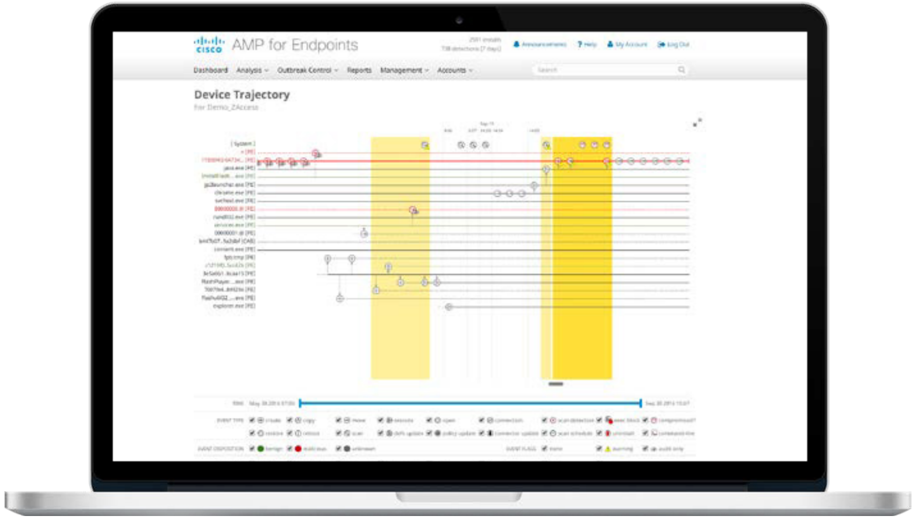
FPR2110-NGFW-K9

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						

Featured Products

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

Cisco ASA 5500-X Series

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

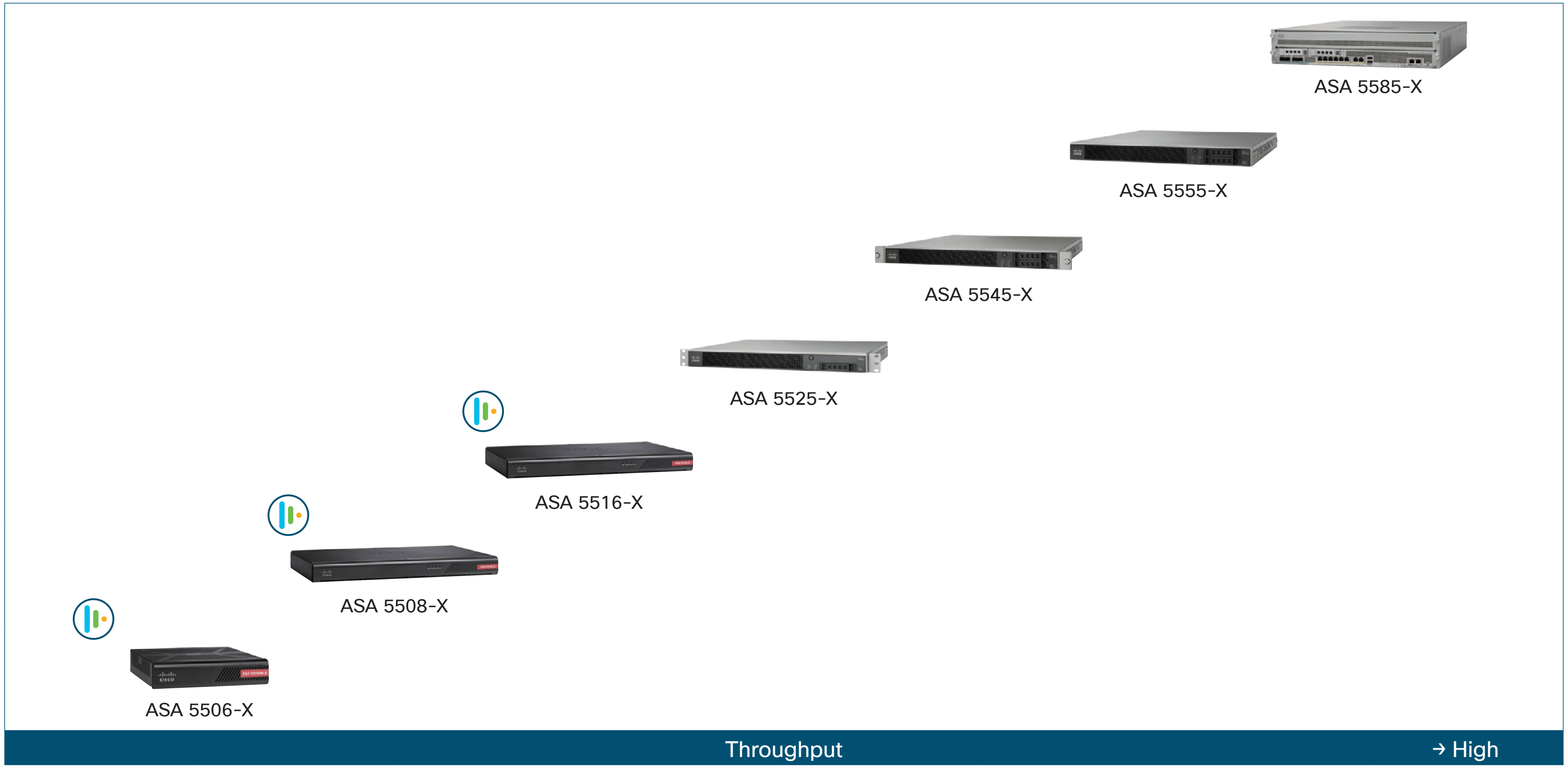
- Site-to-site and remote access VPN and advanced clustering provide highly secure, high-performance access and high availability to help ensure business continuity.
- Granular Application Visibility and Control (AVC) supports more than 3,000 application-layer and risk-based controls that can launch 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.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco ASA 5500-X Series

Overview | Positioning Map | Platform Spec | Licenses | Bundles



Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco ASA 5500-X Series

Overview | Positioning Map | Platform Spec | Licenses | Bundles

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
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.

Cisco ASA 5500-X Series

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	●	●	●

Cisco ASA 5500-X Series

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	-	ASA 5506
L-ASA5506HT-T-1Y	L-ASA5506HT-T-3Y	-	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 in CCW. See Ordering Guide for details.
(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	-	ASA 5506
L-ASA5506HT-AMP-1Y	L-ASA5506HT-AMP-3Y	-	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 in CCW. See Ordering Guide for details.
(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	-	ASA 5506
L-ASA5506HT-URL-1Y	L-ASA5506HT-URL-3Y	-	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 in CCW. See Ordering Guide for details.
(The "xxxx" corresponds to the supported models.)

Cisco ASA 5500-X Series

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	-	ASA 5506
L-ASA5506HT-TM-1Y	L-ASA5506HT-TM-3Y	-	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 in CCW. See Ordering Guide for details.
(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	-	ASA 5506
L-ASA5506HT-TC-1Y	L-ASA5506HT-TC-3Y	-	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 in CCW. See Ordering Guide for details.
(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	-	ASA 5506
L-ASA5506HT-TMC-1Y	L-ASA5506HT-TMC-3Y	-	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 in CCW. See Ordering Guide for details.
(The "xxxx" corresponds to the supported models.)

Cisco ASA 5500-X Series

Cisco ASA 5500-X Series Bundles

1. Select the bundle SKU for the desired appliance model.
2. Next select the matching software licensing subscription SKU.

	ASA5506-FTD-BUN	ASA5506H-FTD-BUN	ASA5508-FTD-BUN	ASA5516-FTD-BUN
ASA 5500-X Series with Firepower Threat Defense	ASA5506-FTD-K9	ASA5506W-x-FTD-K9	ASA5508-FTD-K9	ASA5516-FTD-K9
Firepower Threat Defense NGIPS License	L-ASA5506T-T=	L-ASA5506WT-T=	L-ASA5508T-T=	L-ASA5516T-T=
Firepower Threat Defense AMP License	L-ASA5506T-AMP=	L-ASA5506WT-AMP=	L-ASA5508T-AMP=	L-ASA5516T-AMP=
Firepower Threat Defense URL License	L-ASA5506T-URL=	L-ASA5506WT-URL=	L-ASA5508T-URL=	L-ASA5516T-URL=
Firepower Threat Defense NGIPS & AMP License	L-ASA5506T-TM=	L-ASA5506WT-TM=	L-ASA5508T-TM=	L-ASA5516T-TM=
Firepower Threat Defense NGIPS & URL License	L-ASA5506T-TC=	L-ASA5506WT-TC=	L-ASA5508T-TC=	L-ASA5516T-TC=
Firepower Threat Defense NGIPS & AMP & URL License	L-ASA5506T-TMC=	L-ASA5506WT-TMC=	L-ASA5508T-TMC=	L-ASA5516T-TMC=

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

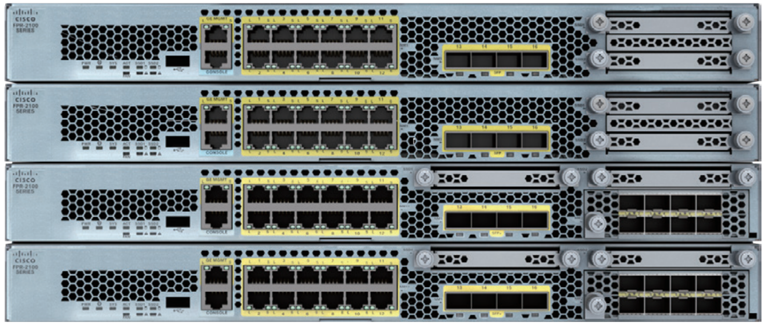
Cisco Firepower 2100 Series

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

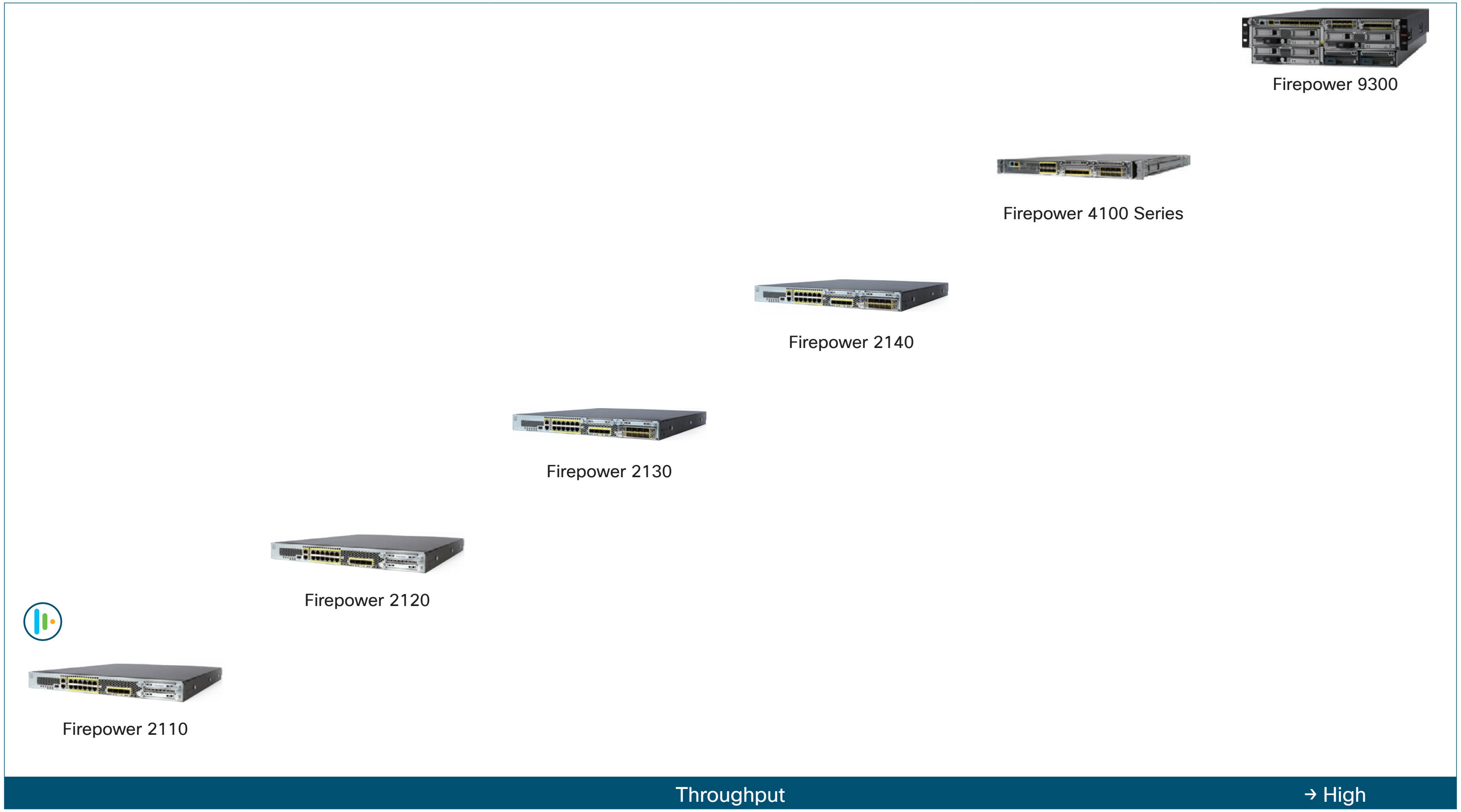
- Stop more threats: Contain known and unknown malware with leading Cisco AMP and sandboxing.
- Gain more insight: Gain superior visibility into your environment with Cisco Firepower NGIPS. Automated risk rankings and impact flags identify priorities for your team.
- Detect earlier, act faster: The Cisco 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.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco Firepower 2100 Series

Overview | Positioning Map | Platform Spec | Licenses



Secure - Security

Cisco Firepower 2100 Series

WEB

Cisco Firepower 2110 Firepower Threat Defense (FTD) Software Image

Product SKU*1	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

*1 FPR2110-BUN is recommended in CCW.

Cisco Firepower 2110 Adaptive Security Appliance (ASA) Software Image

Product SKU*1	Service (CSE) SKU	Throughput			FW Sessions		VPN Peers	Ports		Power Supply	Rack Mount
		FW	FW AVC IPS	VPN	Concurrent Sessions	New Connections per Second		GE	SFP		
FPR2110-ASA-K9	-	3 Gbps	-	500 Mbps	1,000,000	18,000	1,500	12	4	Internal	1 RU

*1 FPR2110-BUN is recommended in CCW.

Getting Started
What’s New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco Firepower 2100 Series

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

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 FTD

[*1] L-FPR2110T-T= is required, FPR2110-BUN is recommended, in CCW. See Ordering Guide for details.

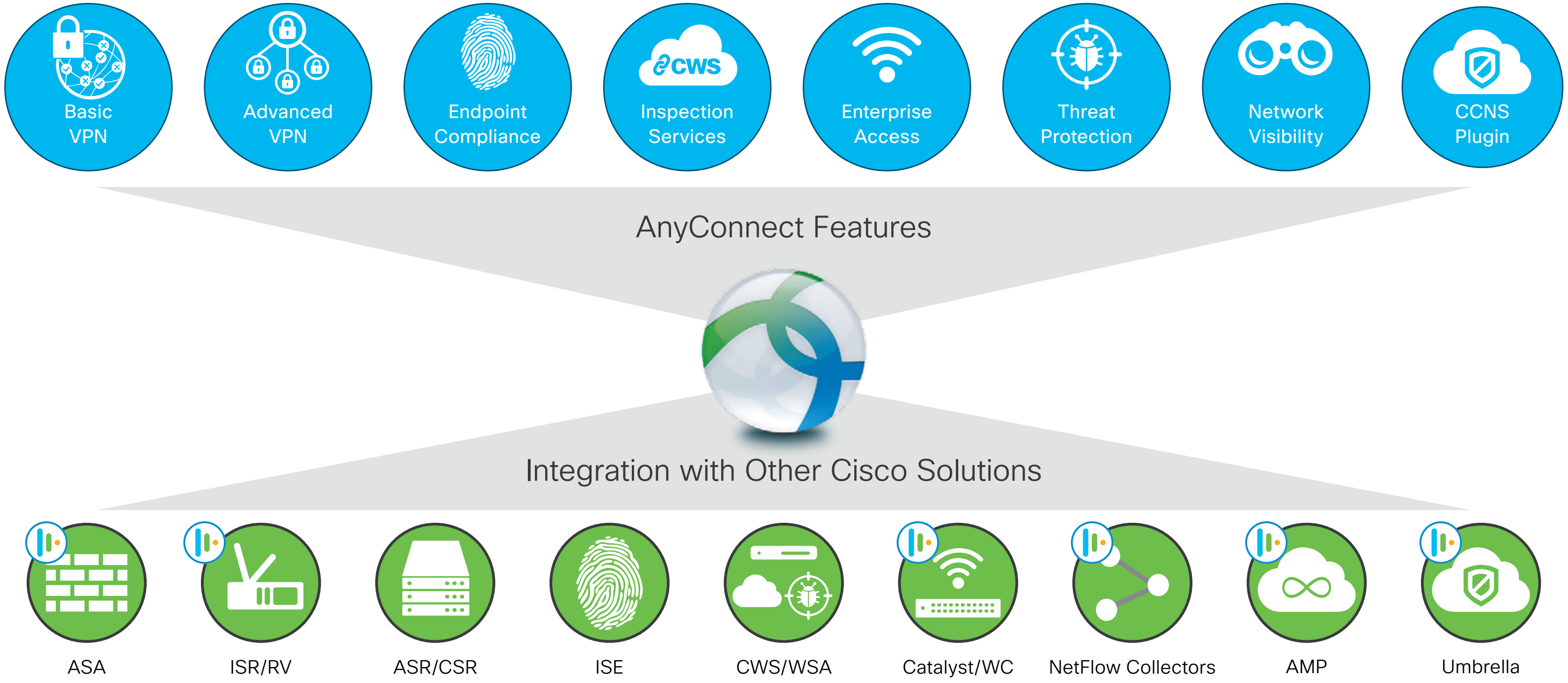
Cisco AnyConnect Secure Mobility Client

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.



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

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

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 See Ordering Guide for a full list of SKUs supporting over 500 users.
*2 L-AC-PLS-LIC= is required in CCW. See Ordering Guide for details.

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 See Ordering Guide for a full list of SKUs supporting over 500 users.
*2 L-AC-PLS-P-G is required in CCW. See Ordering Guide for details.

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 See Ordering Guide for a full list of SKUs supporting over 500 users.
*2 L-AC-APX-LIC= is required in CCW. See Ordering Guide for details.

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 See Ordering Guide for a full list of SKUs supporting over 500 users.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

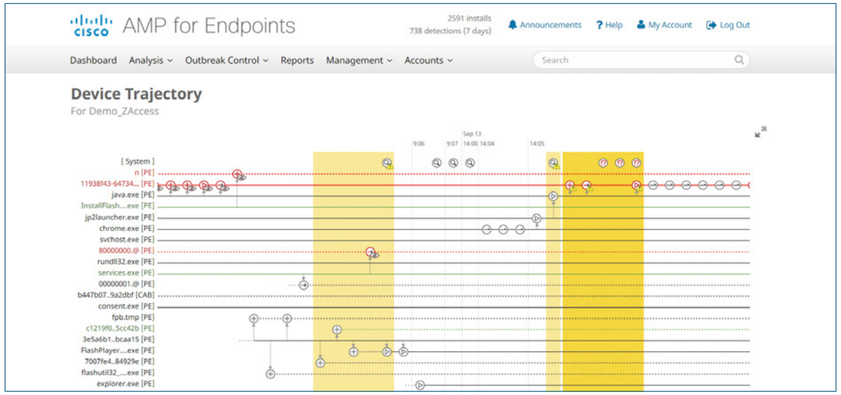
Cisco Advanced Malware Protection for Endpoints

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)



AMP for Endpoints

2591 installs
738 detections (7 days)

Device Trajectory
For Demo_ZAccess

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

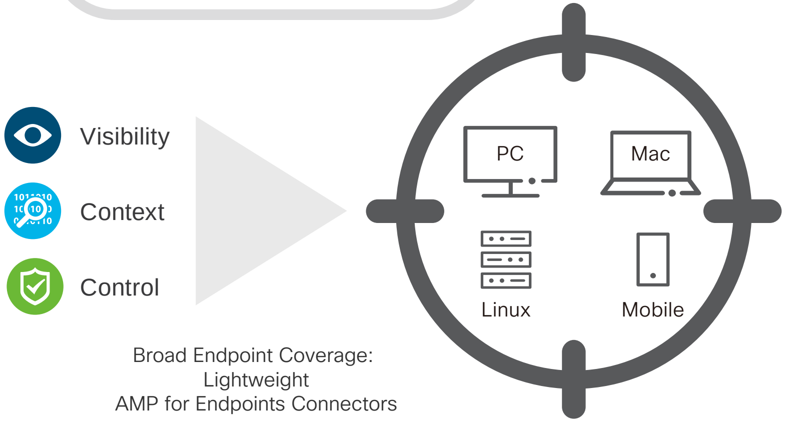
Threat Intelligence and Dynamic Malware Analysis

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).

Analysis is Done in the Cloud
Powered by Talos



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 ~ 99
FP-AMP-1Y-S2	FP-AMP-3Y-S2	FP-AMP-5Y-S2	100 ~ 499

*1 See Ordering Guide for a full list of SKUs supporting over 500 users.
*2 FP-AMP-LIC= is required in CCW. See Ordering Guide for details.

Cisco AMP Virtual Private Cloud Appliance

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

*1 FP-AMP-CLOUD-BUN is recommended in CCW. See Ordering Guide for details.

Cisco AMP Virtual Private Cloud Appliance Licenses

Product SKU[*1] [*2]		
1-Year	3-Years	5-Years
FP-AMPCLOUD-1Y	FP-AMPCLOUD-3Y	FP-AMPCLOUD-5Y

*1 FP-AMP-CLOUD= is required, FP-AMP-CLOUD-BUN is recommended, in CCW.
See Ordering Guide for details.

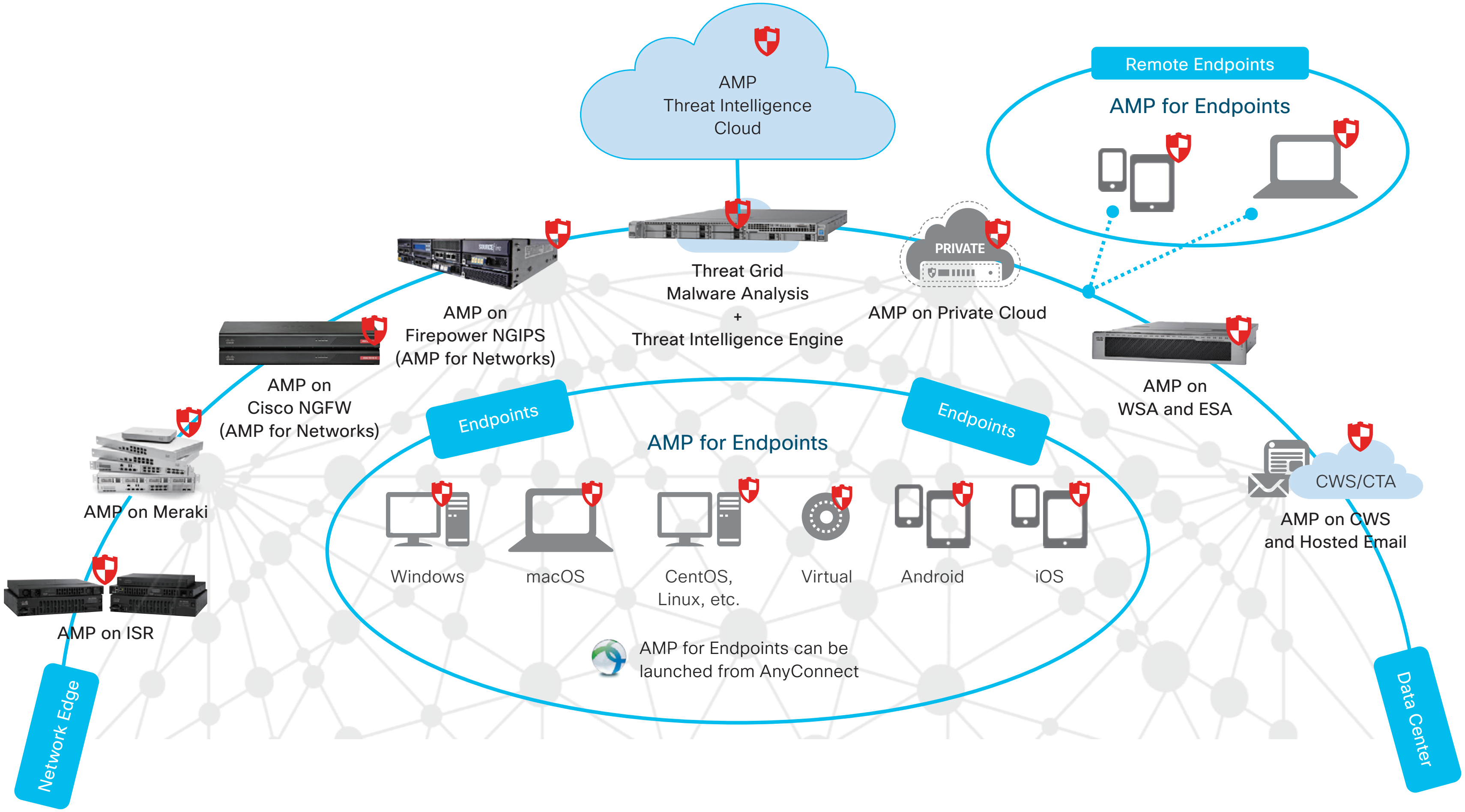
TIP Software Requirements

Connector	Supported OS
Cisco AMP Windows Connector	● Windows 7 ● Windows 8 and 8.1 ● Windows 10 ● Windows Server 2008 R2 ● Windows Server 2012 and 2012 R2 ● Windows Server 2016
Cisco AMP Mac Connector	● OSX 10.11 ● MacOS 10.12 and 10.13
Cisco AMP Linux Connector	● Linux Red Hat Enterprise 6.x and 7.x ● Linux CentOS 6.x and 7.x
Cisco AMP Mobile	● Android 2.1 (Éclair) ~ 6.0 (Marshmallow) ● iOS 11 ~

Cisco Advanced Malware Protection for Endpoints

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.



Secure - Security

Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

WEB

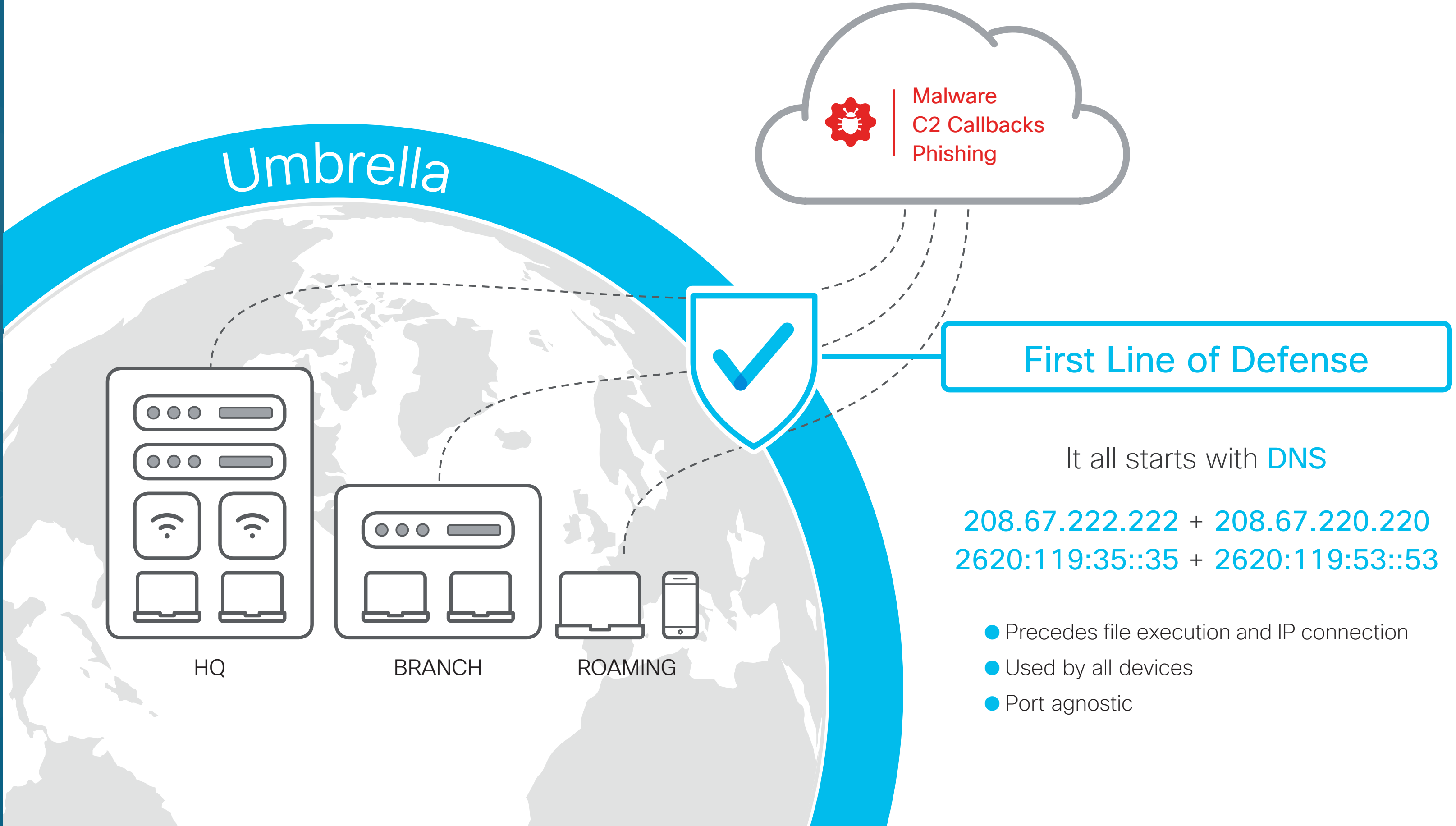
Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

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

The **Cisco Umbrella** is the industry's first **Secure Internet Gateway (SIG)** 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.

By analyzing and learning from internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established — without adding any latency for users.

With Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration.



It all starts with DNS

208.67.222.222 + 208.67.220.220
2620:119:35::35 + 2620:119:53::53

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

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

Package		Roaming	Branch	WLAN	Professional	Insights	Platform
Best for		AnyConnect NGFW	RV 340 ISR 1K/4K	Wireless AP/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 80+ 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 (App Discovery)	-	-	-	●*6	●	●
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).
*6 Umbrella App Discovery for Professional License is required.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

WEB

Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

Cisco Umbrella Roaming License

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

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

Cisco Umbrella Branch Licenses

Product SKU	Description
UMB-BRAN-RV NEW	Umbrella Branch License for Cisco RV 340 Series
UMB-BRAN-1100	Umbrella Branch License for Cisco ISR 1100 Series
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 in CCW. See Ordering Guide for details.

Cisco Umbrella WLAN License

Product SKU*1	Description
UMB-WLAN	Umbrella WLAN per Access Point License (5 ~ APs)

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

Cisco Umbrella Professional Licenses

Product SKU*1	Description
UMB-PROFESSIONAL	Umbrella Professional per User License (10 ~ Users)
UMB-APP-DISC	Umbrella App Discovery for Professional License

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

Cisco Umbrella Insights License

Product SKU*1	Description
UMB-INSIGHTS-K9	Umbrella Insights per User License (10 ~ Users)

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

Cisco Umbrella Platform License

Product SKU*1	Description
UMB-PLATFORM-K9	Umbrella Platform per User License (100 ~ Users)

*1 UMBRELLA-SUB is required in CCW. See Ordering Guide for details.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco Umbrella

Cisco Meraki and Umbrella Together At Last Promotion

Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

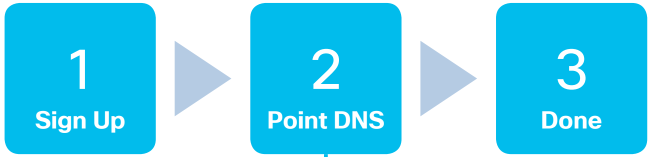
Enterprise-wide Deployment in Minutes

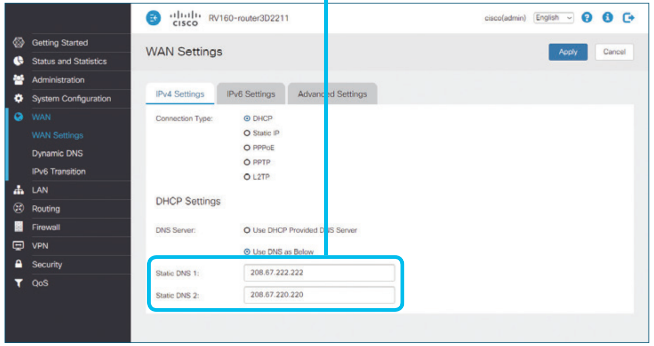
Cisco Umbrella is the fastest and easiest way to protect all of your users in minutes. Because it is delivered from the cloud, there is no hardware to install or software to manually update.

You can provision all on-network devices — including BYOD and IoT — in minutes and use your existing Cisco footprint — RV 340, ISR 1100/4000, Mobility Express, Wireless Controller 3540, and Meraki MR — 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 11.3 or higher devices.

How Easy Is It to Deploy Umbrella?





WAN Settings

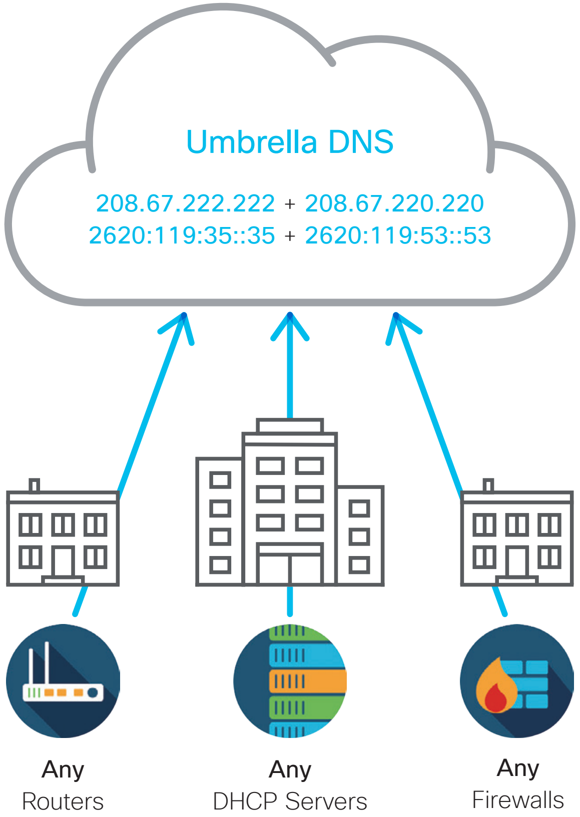
Connection Type: ● DHCP ○ Static IP ○ PPPoE ○ PPTP ○ L2TP

DHCP Settings

DNS Server: ○ Use DHCP Provided DNS Server ● Use DNS as Below

Static DNS 1: 208.67.222.222

Static DNS 2: 208.67.220.220



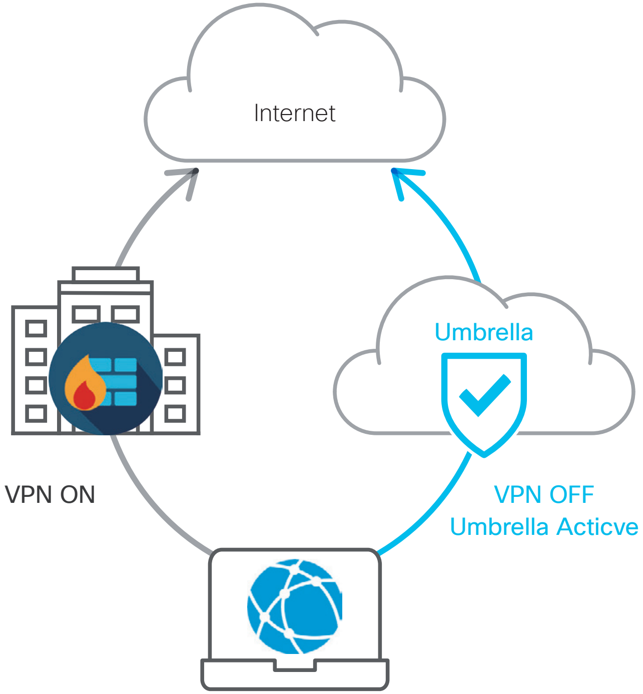
Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

Off-Network Security without VPN

Cisco Umbrella protects employees when they are off the VPN by blocking malicious domain requests and IP responses as DNS queries are resolved. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. Malware will not infect laptops and command & control (C2) callbacks or phishing will not exfiltrate data over any port. Plus, you gain real-time visibility of infected laptops with C2 activity.



Roaming Devices
Windows/macOS (Umbrella Roaming Client)
Chromebook (Umbrella Chromebook Client)
iOS (Security Connector)

The Way Your Employees Work Has Changed

82 % of your workers admit to not always using the VPN*1
Employees are using more cloud apps for work and leveraging their work laptops for personal use–the reality is that not every connection goes through the VPN. Your network extends beyond the perimeter, and your security must too.

49 % of your workforce is mobile and under defended*2
Zero-day malware spikes at night and on weekends when we're roaming and attackers know we're vulnerable. In fact, 22 % of malicious email links are clicked when roaming.*3 While security may never stop 100 % of the threats, it must work 100 % of the time.

*1 cs.co/IDG-survey *2 cs.co/sans-survey *3 cs.co/proofpoint-report

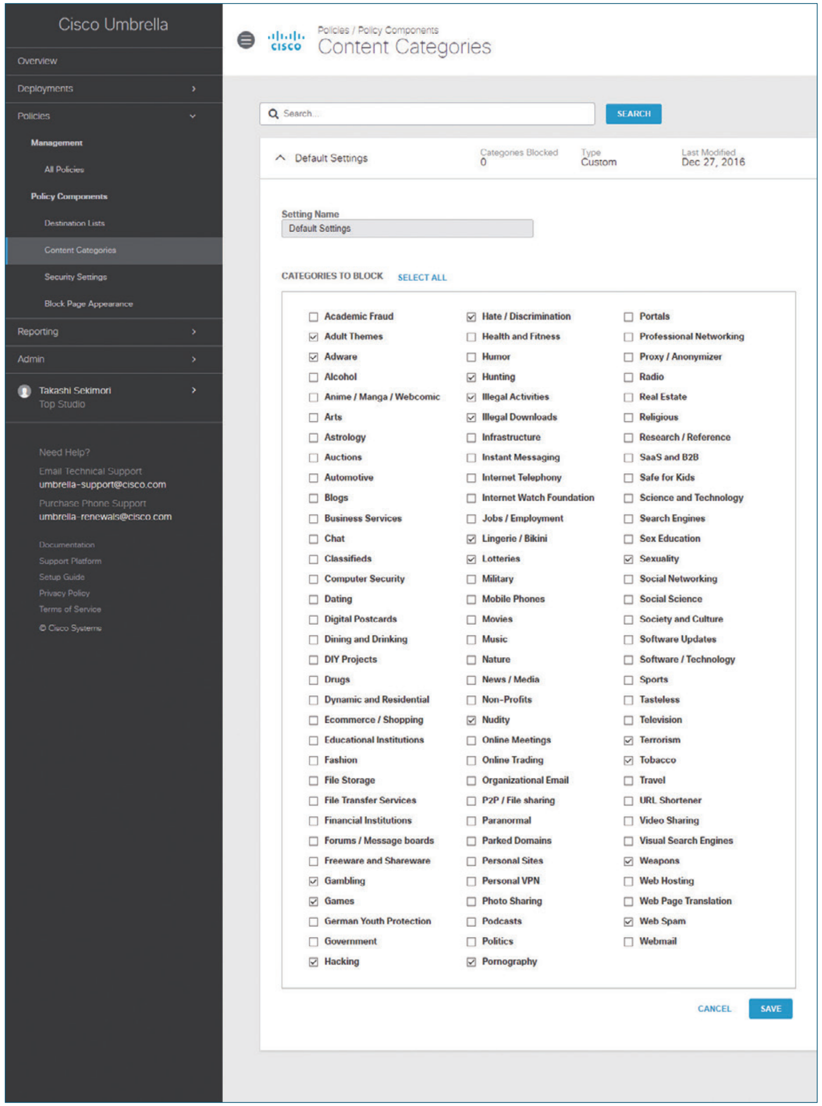
Secure - Security

Cisco Umbrella

Manage Fexible, Location-aware Policies

Cisco Umbrella's 80+ content categories cover millions of domains (and billions of web pages) to give you control over which sites can be accessed by users on your network and by roaming users. The easy-to-use, cloud-delivered administration console enables you to quickly set up, manage, and test different acceptable use policies per network, group, user, device, or IP address, giving you greater control of your organization's internet usage. You even have the flexibility to set up different policies depending on whether users are on or off the corporate network.

Umbrella enables you to customize our category-based filtering to meet each network's specific needs, particularly to help you meet compliance requirements. Quickly create exceptions to allow or block specific domains, regardless of whether it is in a category that is allowed or blocked. Our 80+ content categories empower you to enforce acceptable web use to comply with internal policies or external regulations such as CIPA. We are also a member of the Internet Watch Foundation (IWF), enabling you to block their list of child sexual abuse sites.



Content Categories

Default Settings — Categories Blocked: 0 — Type: Custom — Last Modified: Dec 27, 2016

Setting Name: Default Settings

CATEGORIES TO BLOCK

- ☐ Academic Fraud
- ☑ Adult Themes
- ☑ Adware
- ☐ Alcohol
- ☐ Anime / Manga / Webcomic
- ☐ Arts
- ☐ Astrology
- ☐ Auctions
- ☐ Automotive
- ☐ Blogs
- ☐ Business Services
- ☐ Chat
- ☐ Classifieds
- ☐ Computer Security
- ☐ Dating
- ☐ Digital Postcards
- ☐ Dining and Drinking
- ☐ DIY Projects
- ☐ Drugs
- ☐ Dynamic and Residential
- ☐ Ecommerce / Shopping
- ☐ Educational Institutions
- ☐ Fashion
- ☐ File Storage
- ☐ File Transfer Services
- ☐ Financial Institutions
- ☐ Forums / Message boards
- ☐ Freeware and Shareware
- ☑ Gambling
- ☑ Games
- ☐ German Youth Protection
- ☐ Government
- ☑ Hacking
- ☑ Hate / Discrimination
- ☐ Health and Fitness
- ☐ Humor
- ☑ Hunting
- ☑ Illegal Activities
- ☑ Illegal Downloads
- ☐ Infrastructure
- ☐ Instant Messaging
- ☐ Internet Telephony
- ☐ Internet Watch Foundation
- ☐ Jobs / Employment
- ☑ Lingerie / Bikini
- ☑ Lotteries
- ☐ Military
- ☐ Mobile Phones
- ☐ Movies
- ☐ Music
- ☐ Nature
- ☐ News / Media
- ☐ Non-Profits
- ☑ Nudity
- ☐ Online Meetings
- ☐ Online Trading
- ☐ Organizational Email
- ☐ P2P / File sharing
- ☐ Paranormal
- ☐ Parked Domains
- ☐ Personal Sites
- ☐ Personal VPN
- ☐ Photo Sharing
- ☐ Podcasts
- ☐ Politics
- ☑ Pornography
- ☐ Portals
- ☐ Professional Networking
- ☐ Proxy / Anonymizer
- ☐ Radio
- ☐ Real Estate
- ☐ Religious
- ☐ Research / Reference
- ☐ SaaS and B2B
- ☐ Safe for Kids
- ☐ Science and Technology
- ☐ Search Engines
- ☐ Sex Education
- ☑ Sexuality
- ☐ Social Networking
- ☐ Social Science
- ☐ Society and Culture
- ☐ Software Updates
- ☐ Software / Technology
- ☐ Sports
- ☐ Tasteless
- ☐ Television
- ☑ Terrorism
- ☑ Tobacco
- ☐ Travel
- ☐ URL Shortener
- ☐ Video Sharing
- ☐ Visual Search Engines
- ☑ Weapons
- ☐ Web Hosting
- ☐ Web Page Translation
- ☑ Web Spam
- ☐ Webmail

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Cisco Umbrella

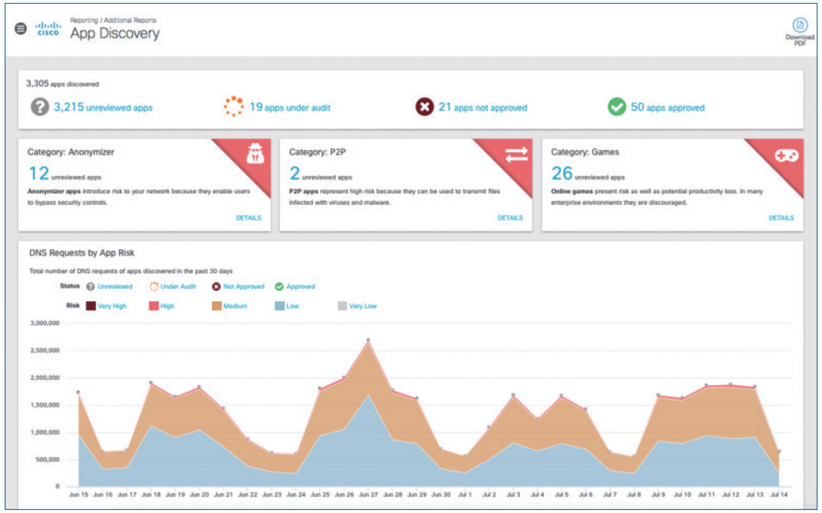
Cisco Meraki and Umbrella
Together At Last Promotion

Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

Expose Shadow IT and Manage Cloud Adoption

Cloud usage is continuing to expand as end users and departments become more comfortable acquiring cloud services. The typical organization is only aware of a small fraction of its overall cloud activity. The lack of a coordinated cloud enablement strategy leads to a broad set of productivity, expense, security, and support issues.

The App Discovery report of Cisco Umbrella provides full visibility and risk information to manage cloud adoption in a secure and organized fashion. Once decisions are made about specific apps, you can block access to applications that are not approved to reduce the risk of sensitive data loss, account compromise and malware infection.



Reporting / Additional Reports
App Discovery

3,305 apps discovered

3,215 unreviewed apps | 19 apps under audit | 21 apps not approved | 50 apps approved

Category: Anonymizer
12 unreviewed apps
Anonymizer apps introduce risk to your network because they enable users to bypass security controls.
DETAILS

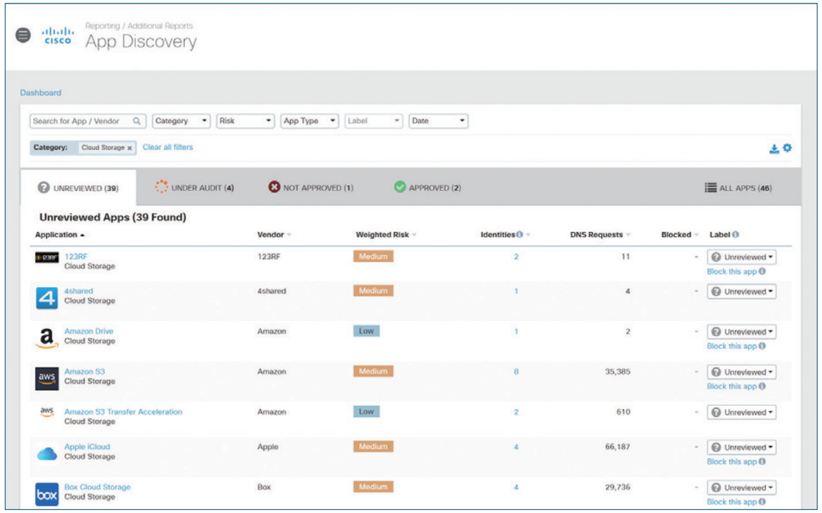
Category: P2P
2 unreviewed apps
P2P apps represent high risk because they can be used to transmit files infected with viruses and malware.
DETAILS

Category: Games
26 unreviewed apps
Online games present risk as well as potential productivity loss. In many enterprise environments they are discouraged.
DETAILS

DNS Requests by App Risk

Total number of DNS requests of apps discovered in the past 30 days

The App Discovery dashboard provides an overview of the number of app requests by date and risk level to show patterns and changes over time. The most recent set of discovered and unreviewed apps are highlighted for easy access and a chart showing the number of apps in each major category is provided with a breakdown by risk level. These summary charts allow point and click access to more detailed information on the category or individual application to simplify common administrator tasks.



Reporting / Additional Reports
App Discovery

Category: Cloud Storage

UNREVIEWED (39) | UNDER AUDIT (4) | NOT APPROVED (1) | APPROVED (2) | ALL APPS (46)

Unreviewed Apps (39 Found)

Application	Vendor	Weighted Risk	Identities	DNS Requests	Blocked	Label
123RF Cloud Storage	123RF	Medium	2	11	-	Unreviewed Block this app
4shared Cloud Storage	4shared	Medium	1	4	-	Unreviewed
Amazon Drive Cloud Storage	Amazon	Low	1	2	-	Unreviewed Block this app
Amazon S3 Cloud Storage	Amazon	Medium	8	35,385	-	Unreviewed Block this app
Amazon S3 Transfer Acceleration Cloud Storage	Amazon	Low	2	610	-	Unreviewed
Apple iCloud Cloud Storage	Apple	Medium	4	66,187	-	Unreviewed Block this app
Box Cloud Storage Cloud Storage	Box	Medium	4	29,736	-	Unreviewed Block this app

The Apps Grid report provides key details on all applications that have been discovered including the app and vendor name, category, weighted risk level, number of users, number of requests and current status. This report can be segmented and filtered into groups for deeper analysis by category, risk level or number of users to provide views that assist with the organization and management of cloud adoption.

Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

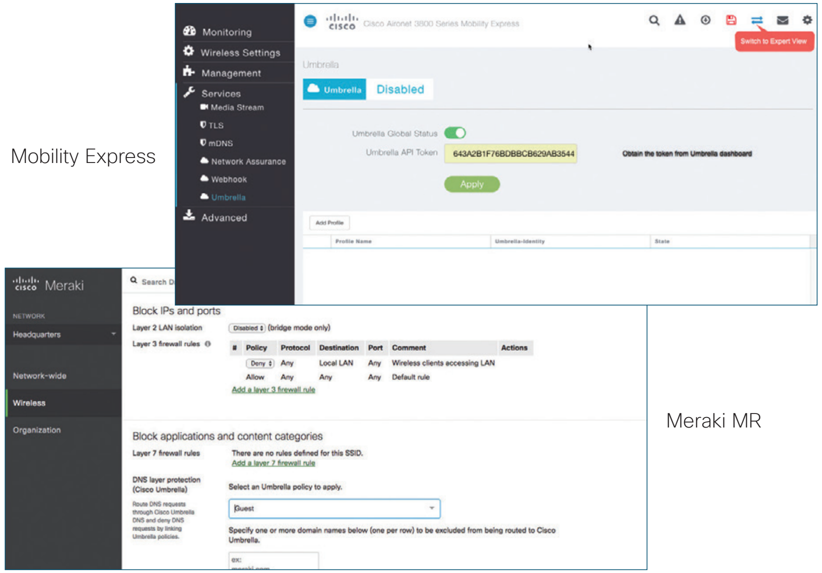
Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

Simple and Effective Protection for Corporate and Guest Wi-Fi

The Cisco Umbrella Wireless LAN (WLAN) package provides the first line of defense against threats for Wi-Fi connections. It offers the simplest, fastest way to protect every user on your Wi-Fi network.

Umbrella WLAN protects employees and guests who are accessing the internet from wireless access points. By enforcing security at the DNSlayer, connections to unsafe sites are never established and malicious files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port and protocol. Umbrella WLAN also brings a simple-to-use content filtering solution to your Wi-Fi network. It stops guests and corporate users from accessing inappropriate content, based on company policy. This keeps users happy with safe internet access, while also protecting your business.

Umbrella WLAN is the simplest way to protect any device accessing your wireless network — there's no action required from end users for protection. Whether it's a corporate device, employee-owned, or customer-owned device, Umbrella WLAN adds an easy, but very effective layer of protection. Umbrella WLAN works across a broad portfolio of wireless controllers and access points. Built-in integrations with the Cisco WAP125/WAP581, Cisco Aironet Access Points with Mobility Express, Cisco Wireless Controllers, and Cisco Meraki MR Cloud Managed Access Points provides additional ease of use and granularity.



Cisco Aironet 3800 Series Mobility Express

Umbrella

Umbrella Disabled

Umbrella Global Status: on

Umbrella API Token: 643A2B1F76BDBBCB629AB3544 — Obtain the token from Umbrella dashboard

Apply

Add Profile

Profile Name	Umbrella-Identity	State

Meraki

Block IPs and ports

Layer 2 LAN isolation: Disabled (bridge mode only)

Layer 3 firewall rules

#	Policy	Protocol	Destination	Port	Comment	Actions
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

Add a layer 3 firewall rule

Block applications and content categories

Layer 7 firewall rules: There are no rules defined for this SSID. Add a layer 7 firewall rule

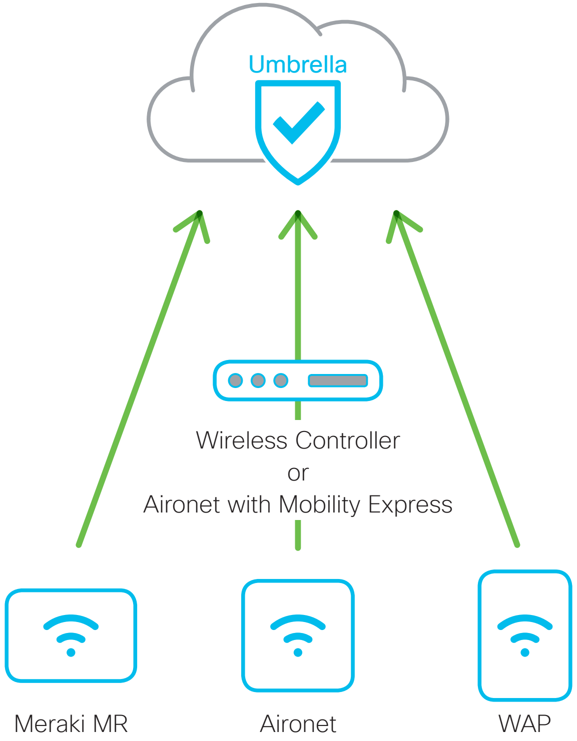
DNS layer protection (Cisco Umbrella): Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

Select an Umbrella policy to apply. Guest

Specify one or more domain names below (one per row) to be excluded from being routed to Cisco Umbrella.

ex: meraki.com

You can deploy Umbrella in minutes across your access points.
Simply input the API key and secret from Umbrella into the AP's GUI.



Secure - Security

Cisco Umbrella

Cisco Meraki and Umbrella Together At Last Promotion

WEB

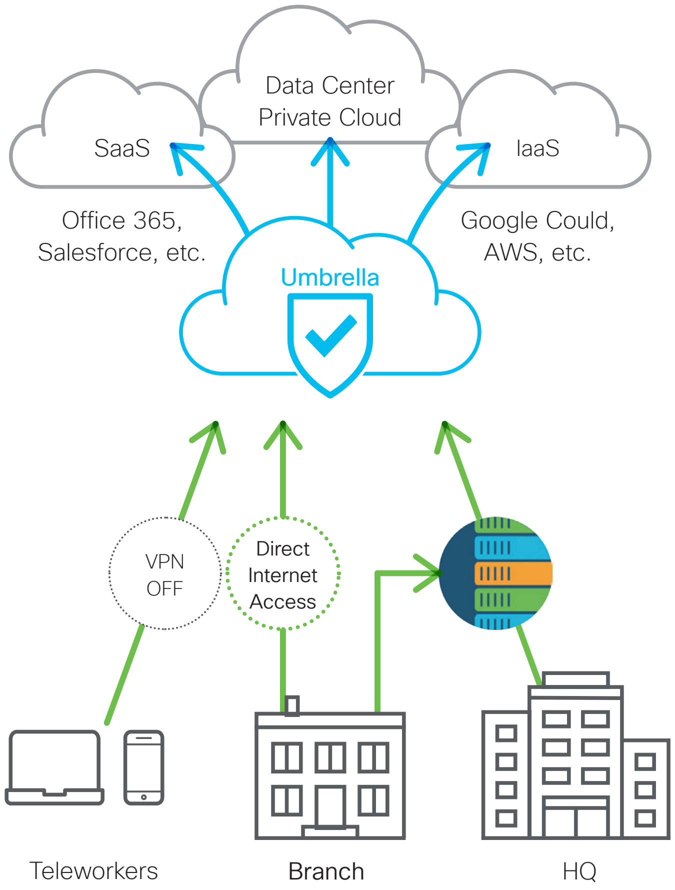
Overview | Features | Licenses | Why Umbrella? | 14-Day Trial

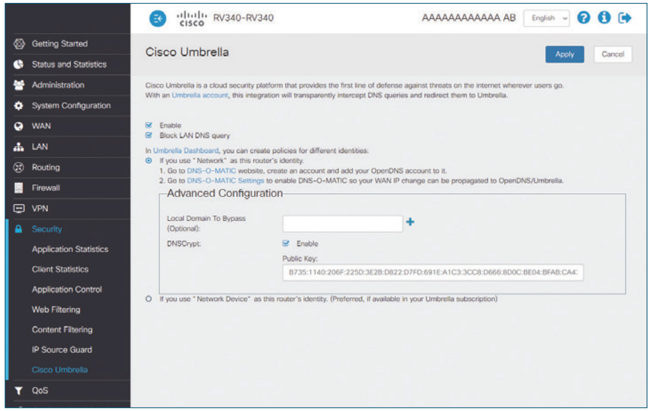
The Simplest and Fastest Way to Secure DIA from Branch

The traditional WAN was built to give branch offices and roaming users access to IT resources within private data centers. But today, as networks become more decentralized and users connect directly to SaaS applications, backhauling traffic to apply security policies just isn't efficient. And that's not the only problem. Backhauling internet-bound traffic is expensive, and it adds latency. So users get frustrated – and thwarted – in their attempt to get work done. That's why so many branch offices are migrating to direct internet access (DIA).

The **Cisco Umbrella Branch** package is a cloud-delivered security service for the **Cisco RV 340 Series** and **Cisco ISR 1100/4000 Series** routers. It provides the first layer of defense against threats at branch offices. And it offers the simplest, fastest way to protect every device on your branch network. You gain visibility and enforcement at the DNS-layer, so you can block requests to malicious domains and IPs before a connection is ever made.

Umbrella Branch protects employees and guests in distributed branch offices — like those in retail, finance, hospitality, and education. By enforcing security at the DNS-layer, connections are never established and files are never downloaded. This prevents malware from infecting devices and stops attacks from exfiltrating data over any port.





Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. With an Umbrella account, this integration will transparently intercept DNS queries and redirect them to Umbrella.

☑ Enable
☑ Block LAN DNS query

In Umbrella Dashboard, you can create policies for different identities:

● If you use " Network" as this router's identity.
1. Go to DNS-O-MATIC website, create an account and add your OpenDNS account to it.
2. Go to DNS-O-MATIC Settings to enable DNS-O-MATIC so your WAN IP change can be propagated to OpenDNS/Umbrella.

Advanced Configuration

Local Domain To Bypass (Optional):
DNSCrypt: ☑ Enable
Public Key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA4:

○ If you use " Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

RV 340

You can deploy Umbrella in minutes on your RV 340 series router.
Simply input the API key and secret from Umbrella into the router's GUI.

Secure - Security

Cisco Umbrella

Cisco Meraki and Umbrella
Together At Last Promotion

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

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.

WEB signup.umbrella.com

Umbrella Professional: Best for Small Companies

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.

WEB umbrella.cisco.com/products/small-teams

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

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

The **Cisco Meraki MX Security & SD-WAN Appliances** are ideal for organizations considering a Unified Threat Managment (UTM) solution for distributed sites, campuses or datacenter VPN concentration. Since the Cisco Meraki MX is 100 % cloud managed, installation and remote management are simple. Cisco Meraki 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, Cisco Snort-based intrusion detection and prevention (IPS/IPS), 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 or Microsoft Azure.

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 and Microsoft Azure.
- Content Filtering: Block undesirable web content across 80+ 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

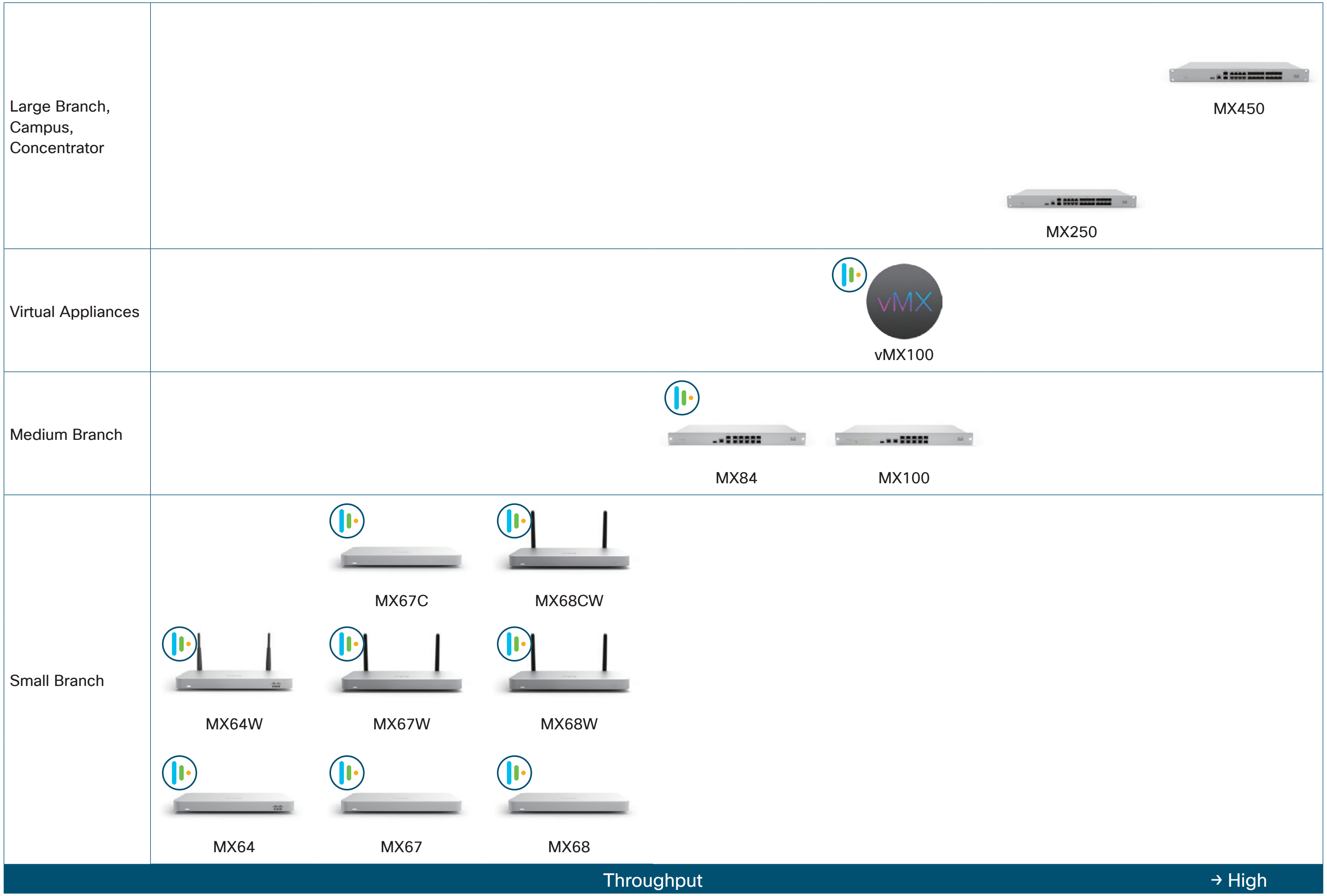
Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

WEB

Overview | Positioning Map | Platform Spec | Licenses & Accessories | Why Meraki MX?



Large Branch, Campus, Concentrator	MX250 MX450
Virtual Appliances	vMX100
Medium Branch	MX84 MX100
Small Branch	MX67C MX68CW MX64W MX67W MX68W MX64 MX67 MX68

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

Product SKU	Recom-mended Clients	Throughput			Concurrent VPN Tunnels	Web Caching	WAN Ports		WAN/ LAN Ports	LAN Ports			WLAN	Power Supply	Rack Mount
		Stateful Firewall	Advanced Security	VPN			GE	4G LTE	GE	GE	GE PoE+	SFP	11ac AP		
MX64-HW	50	250 Mbps	200 Mbps	100 Mbps	50	-	1	-[*1]	1	4	-	-	-	External	-[*2]
MX64W-HW	50	250 Mbps	200 Mbps	100 Mbps	50	-	1	-[*1]	1	4	-	-	●	External	-[*2]
MX67-HW	50	450 Mbps	300 Mbps	200 Mbps	50	-	1	-[*1]	1	4	-	-	-	External	-[*2]
MX67W-HW	50	450 Mbps	300 Mbps	200 Mbps	50	-	1	-[*1]	1	4	-	-	●	External	-[*2]
MX67C-HW-WW	50	450 Mbps	300 Mbps	200 Mbps	50	-	1	●	1	4	-	-	-	External	-[*2]
MX68-HW	50	450 Mbps	300 Mbps	200 Mbps	50	-	2	-[*1]	-	8	2	-	-	External	-[*2]
MX68W-HW	50	450 Mbps	300 Mbps	200 Mbps	50	-	2	-[*1]	-	8	2	-	●	External	-[*2]
MX68CW-HW-WW	50	450 Mbps	300 Mbps	200 Mbps	50	-	2	●	-	8	2	-	●	External	-[*2]
MX84-HW	200	500 Mbps	320 Mbps	250 Mbps	100	1 TB	2	-[*1]	-	8	-	2	-	Internal	1 RU
vMX100	-	-	-	500 Mbps	-	-	-	-	-	-	-	-	-	-	-

[*1] Cellular Modem is required.

[*2] Desktop or Wall mountable with included mount hardware.

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

Cisco Meraki Licensing for Cisco Meraki MX Series

The Cisco Meraki MX Cloud Managed Security Appliances have licenses on a per-model basis, so every Meraki MX model has a corresponding license. Please note that these licenses are non-transferrable between appliance models. For example, an MX64 will not be covered by an MX84 license; it will require an MX64 license.

The Cisco Meraki MX has multiple license editions: Enterprise and Advanced Security. Please note that the Meraki MX licensing edition is uniform across the Organization. For example, you can have all 25 appliances using Enterprise edition or Advanced Security edition, but you cannot have 20 appliances using one edition and 5 using the other edition. If you wish to use Enterprise edition for some appliances and Advanced Security edition for other appliances, you need to create two Organizations, one for your appliances with the Enterprise edition, and another for the appliances with the Advanced Security edition.

Cisco Meraki License Comparison

	Enterprise	Advanced Security
Next-Generation Firewalls (NGFW)	●	●
VLAN to VLAN Routing	●	●
Link Bonding and Failover	●	●
3G/4G Failover via USB Modem	●	●
Traffic Shaping and Prioritization	●	●
Auto VPN Self-Configuring Site-to-Site VPN	●	●
Client VPN	●	●
MPLS to VPN Failover	●	●
Splash Pages	●	●
Configuration Templates	●	●
HTTP Content Caching (Web Caching)	●	●
Group Policies	●	●
Client Connectivity Alerts	●	●
Active/Passive High Availability*1	●	●
SD-WAN	●	●
Geography-based Firewall Rules	-	●
Cisco Snort IDS/IPS	-	●
Content Filtering (with Google SafeSearch)	-	●
Anti-Virus and Anti-Phishing	-	●
Youtube for Schools	-	●
Web Search Filtering	-	●
Cisco Advanced Malware Protection (AMP)	-	●
Cisco Threat Grid*2	-	●

*1 No license required for Meraki MX deployed as Warm Spares.
*2 Cisco Threat Grid License is required.

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

Overview | Positioning Map | Platform Spec | Licenses & Accessories | Why Meraki MX?

Cisco Meraki Enterprise Licenses for Cisco Meraki MX Series

Product SKU					Compatible Models
1-Year	3-Years	5-Years	7-Years	10-Years	
LIC-MX64-ENT-1YR	LIC-MX64-ENT-3YR	LIC-MX64-ENT-5YR	LIC-MX64-ENT-7YR	LIC-MX64-ENT-10YR	MX64
LIC-MX64W-ENT-1YR	LIC-MX64W-ENT-3YR	LIC-MX64W-ENT-5YR	LIC-MX64W-ENT-7YR	LIC-MX64W-ENT-10YR	MX64W
LIC-MX67-ENT-1YR	LIC-MX67-ENT-3YR	LIC-MX67-ENT-5YR	LIC-MX67-ENT-7YR	LIC-MX67-ENT-10YR	MX67
LIC-MX67W-ENT-1YR	LIC-MX67W-ENT-3YR	LIC-MX67W-ENT-5YR	LIC-MX67W-ENT-7YR	LIC-MX67W-ENT-10YR	MX67W
LIC-MX67C-ENT-1YR	LIC-MX67C-ENT-3YR	LIC-MX67C-ENT-5YR	LIC-MX67C-ENT-7YR	LIC-MX67C-ENT-10YR	MX67C
LIC-MX68-ENT-1YR	LIC-MX68-ENT-3YR	LIC-MX68-ENT-5YR	LIC-MX68-ENT-7YR	LIC-MX68-ENT-10YR	MX68
LIC-MX68W-ENT-1YR	LIC-MX68W-ENT-3YR	LIC-MX68W-ENT-5YR	LIC-MX68W-ENT-7YR	LIC-MX68W-ENT-10YR	MX68W
LIC-MX68CW-ENT-1YR	LIC-MX68CW-ENT-3YR	LIC-MX68CW-ENT-5YR	LIC-MX68CW-ENT-7YR	LIC-MX68CW-ENT-10YR	MX68CW
LIC-MX84-ENT-1YR	LIC-MX84-ENT-3YR	LIC-MX84-ENT-5YR	LIC-MX84-ENT-7YR	LIC-MX84-ENT-10YR	MX84
LIC-VMX100-1YR	LIC-VMX100-3YR	LIC-VMX100-5YR	-	-	vMX100

Cisco Meraki Advanced Security Licenses for Cisco Meraki MX Series

Product SKU					Compatible Models
1-Year	3-Years	5-Years	7-Years	10-Years	
LIC-MX64-SEC-1YR	LIC-MX64-SEC-3YR	LIC-MX64-SEC-5YR	LIC-MX64-SEC-7YR	LIC-MX64-SEC-10YR	MX64
LIC-MX64W-SEC-1YR	LIC-MX64W-SEC-3YR	LIC-MX64W-SEC-5YR	LIC-MX64W-SEC-7YR	LIC-MX64W-SEC-10YR	MX64W
LIC-MX67-SEC-1YR	LIC-MX67-SEC-3YR	LIC-MX67-SEC-5YR	LIC-MX67-SEC-7YR	LIC-MX67-SEC-10YR	MX67
LIC-MX67W-SEC-1YR	LIC-MX67W-SEC-3YR	LIC-MX67W-SEC-5YR	LIC-MX67W-SEC-7YR	LIC-MX67W-SEC-10YR	MX67W
LIC-MX67C-SEC-1YR	LIC-MX67C-SEC-3YR	LIC-MX67C-SEC-5YR	LIC-MX67C-SEC-7YR	LIC-MX67C-SEC-10YR	MX67C
LIC-MX68-SEC-1YR	LIC-MX68-SEC-3YR	LIC-MX68-SEC-5YR	LIC-MX68-SEC-7YR	LIC-MX68-SEC-10YR	MX68
LIC-MX68W-SEC-1YR	LIC-MX68W-SEC-3YR	LIC-MX68W-SEC-5YR	LIC-MX68W-SEC-7YR	LIC-MX68W-SEC-10YR	MX68W
LIC-MX68CW-SEC-1YR	LIC-MX68CW-SEC-3YR	LIC-MX68CW-SEC-5YR	LIC-MX68CW-SEC-7YR	LIC-MX68CW-SEC-10YR	MX68CW
LIC-MX84-SEC-1YR	LIC-MX84-SEC-3YR	LIC-MX84-SEC-5YR	LIC-MX84-SEC-7YR	LIC-MX84-SEC-10YR	MX84

Secure - Security

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

Cisco Meraki Insight Licenses for Cisco Meraki MX Series

Product SKU			Supported Throughput	Compatible Models
1-Year	3-Years	5-Years		
LIC-MI-S-1YR	LIC-MI-S-3YR	LIC-MI-S-5YR	450 Mbps	MX6x
LIC-MI-M-1YR	LIC-MI-M-3YR	LIC-MI-M-5YR	750 Mbps	MX84

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

SKU	Description	Max Distance	Compatible Models
MA-SFP-1GB-TX	1000BASE-T SFP Module	100 m	MX84
MA-SFP-1GB-SX	1000BASE-SX SFP Module	550 m	MX84
MA-SFP-1GB-LX10	1000BASE-LX10 Module	10 km	MX84

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

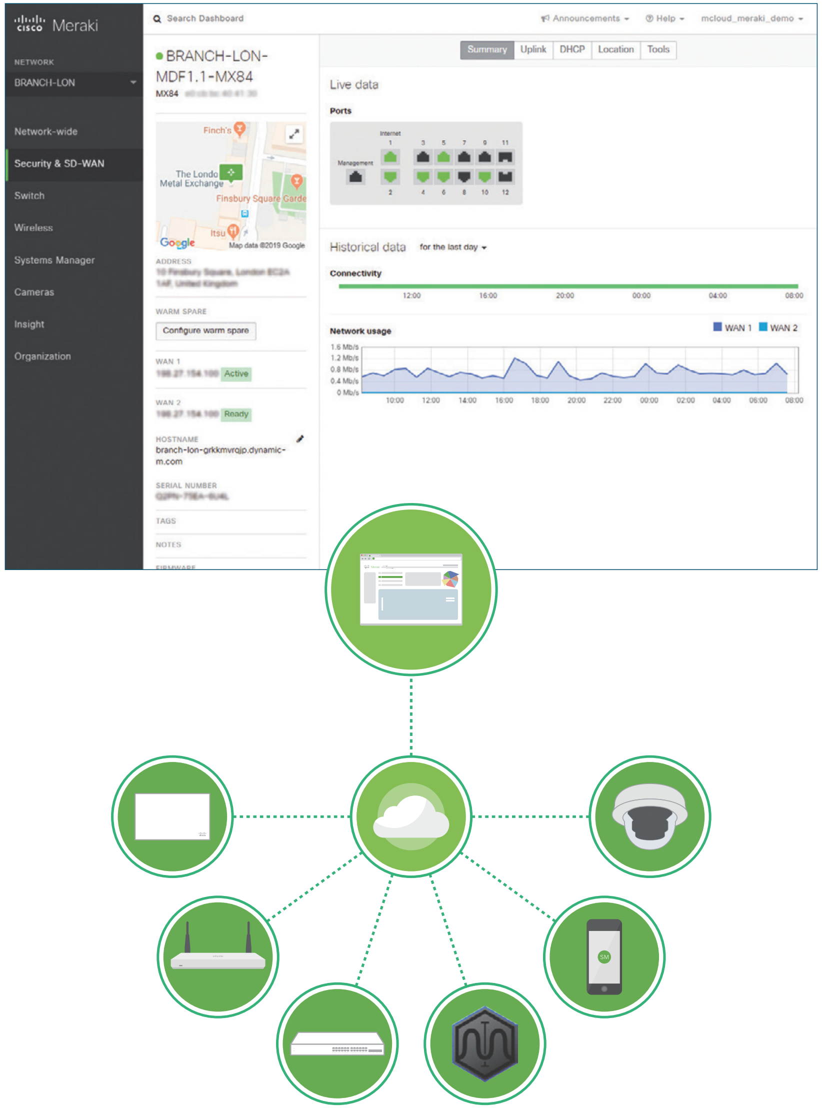
Cloud Management Architecture

Cisco Meraki's architecture provides feature rich network management without on-site management appliances or Wi-Fi controllers.

Every Meraki device —including access points, switches, security appliances, and cameras— connects over the Internet to Meraki's datacenters, which run Meraki's cloud management platform.

These connections, secured via SSL, utilize a patented protocol that provides real time visibility and control, yet uses minimal bandwidth overhead (typically 1 kbps or less.)

In place of traditional command-line based network configuration, Meraki provides a rich web based dashboard, providing visibility and control over up to tens of thousands of Meraki devices, anywhere in the world. Tools, designed to scale to large and distributed networks, make policy changes, firmware updates, deploying new branches, etc. simple and expedient, regardless of size or location. Meraki's real time protocols combine the immediacy of on-premise management applications with the simplicity and centralized control of a cloud application.



Meraki

Search Dashboard | Announcements | Help | mcloud_meraki_demo

NETWORK
BRANCH-LON

Network-wide
Security & SD-WAN
Switch
Wireless
Systems Manager
Cameras
Insight
Organization

BRANCH-LON-MDF1.1-MX84
MX84 [redacted]

ADDRESS
[redacted]

WARM SPARE
Configure warm spare

WAN 1
[redacted] Active

WAN 2
[redacted] Ready

HOSTNAME
branch-lon-grkkmvrqjp.dynamic-m.com

SERIAL NUMBER
[redacted]

TAGS

NOTES

FIRMWARE

Summary | Uplink | DHCP | Location | Tools

Live data

Ports

Historical data for the last day

Connectivity

Network usage

Secure - Security

Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

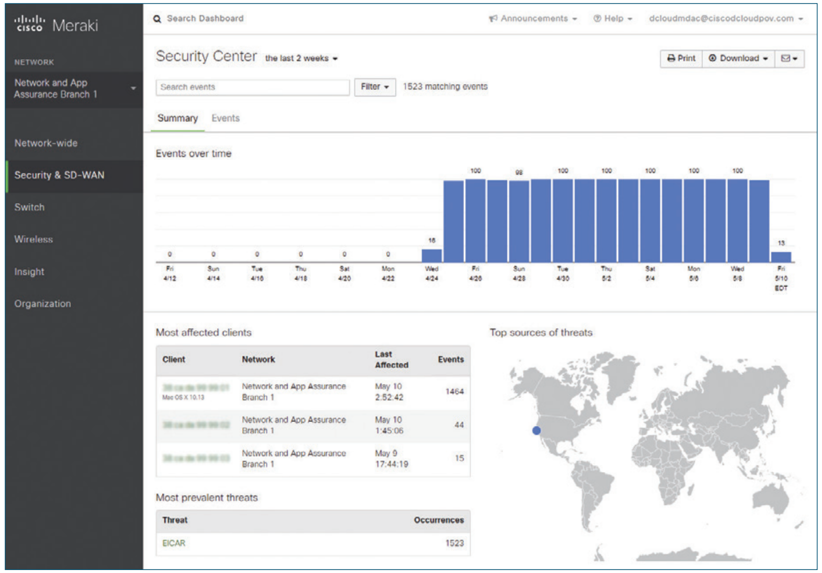
Ironclad Security

The Cisco Meraki MX platform has an extensive suite of security features including IDS/IPS, content filtering, web search filtering, antimalware, geo-IP based firewalling, IPsec VPN connectivity, and Cisco Advanced Malware Protection (AMP), while providing the performance required for modern, bandwidth-intensive networks.

Layer 7 fingerprinting technology lets administrators identify unwanted content and applications and prevent recreational apps like BitTorrent from wasting precious bandwidth.

The integrated Cisco Snort engine delivers superior intrusion prevention coverage, a key requirement for PCI 3.2 compliance. Cisco Meraki MX also uses the Webroot BrightCloud URL categorization database for CIPA/IWF compliant content-filtering, Cisco AMP engine for anti-malware, AMP Threat Grid Cloud, and MaxMind for geo-IP based security rules.

Best of all, these industry-leading Layer 7 security engines and signatures are always kept up-to-date via the cloud, simplifying network security management and providing peace of mind to IT administrators.



Security Center the last 2 weeks

Search events

1523 matching events

Events over time

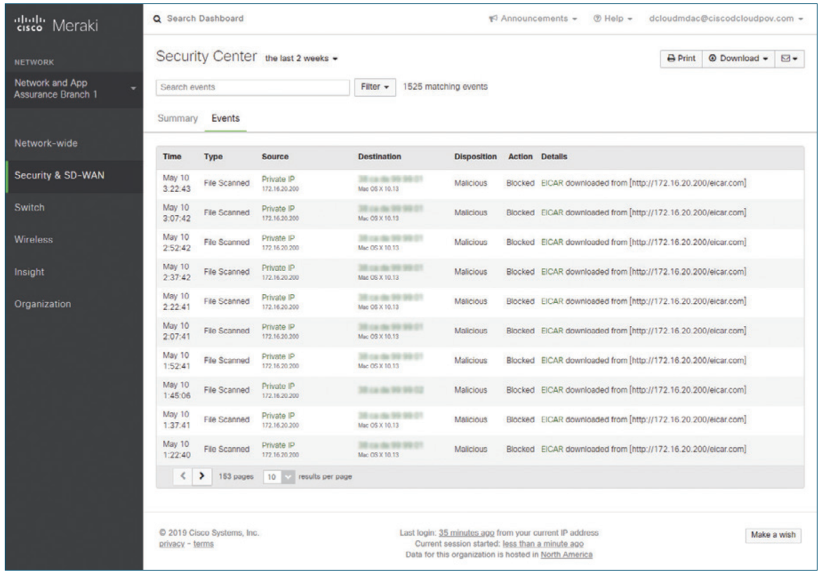
Most affected clients

Client	Network	Last Affected	Events
[redacted] Mac OS X 10.13	Network and App Assurance Branch 1	May 10 2:52:42	1464
[redacted]	Network and App Assurance Branch 1	May 10 1:45:06	44
[redacted]	Network and App Assurance Branch 1	May 9 17:44:19	15

Top sources of threats

Most prevalent threats

Threat	Occurrences
EICAR	1523



Security Center the last 2 weeks

Search events

1525 matching events

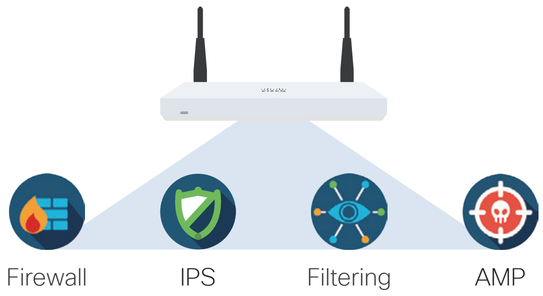
Time	Type	Source	Destination	Disposition	Action	Details
May 10 3:22:43	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 3:07:42	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 2:52:42	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 2:37:42	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 2:22:41	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 2:07:41	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 1:52:41	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 1:45:06	File Scanned	Private IP 172.16.20.200	[redacted]	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 1:37:41	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]
May 10 1:22:40	File Scanned	Private IP 172.16.20.200	[redacted] Mac OS X 10.13	Malicious	Blocked	EICAR downloaded from [http://172.16.20.200/eicar.com]

< > 153 pages 10 results per page

© 2019 Cisco Systems, Inc.
privacy - terms

Last login: 35 minutes ago from your current IP address
Current session started: less than a minute ago
Data for this organization is hosted in North America

All-in-One Security



Cisco Meraki MX Cloud Managed Security & SD-WAN Appliances

Software-Defined WAN (SD-WAN)

Cisco SD-WAN (powered by Meraki) is ideal for lean IT environments in which full stack management of WAN, LAN, and security is valued, along with simple management, orchestration, and automation, or where Meraki is the predominant architecture.

Cisco Meraki MX is equipped with SD-WAN capabilities that enable administrators to use available bandwidth more efficiently and ensure the highest possible level of performance for critical applications without sacrificing security or data privacy.

The following features can lower your operational costs and improve resource usage:

- Dual-Active VPN Uplinks

  In addition to supporting dual WAN uplinks and automatic VPN failover, the Meraki MX also has the ability to build multiple VPN tunnels that are active simultaneously on both uplinks, whether they are Internet or MPLS connections. Traffic can then be load-balanced across these tunnels to make optimal use of available bandwidth.

- Policy-based Routing (PbR)

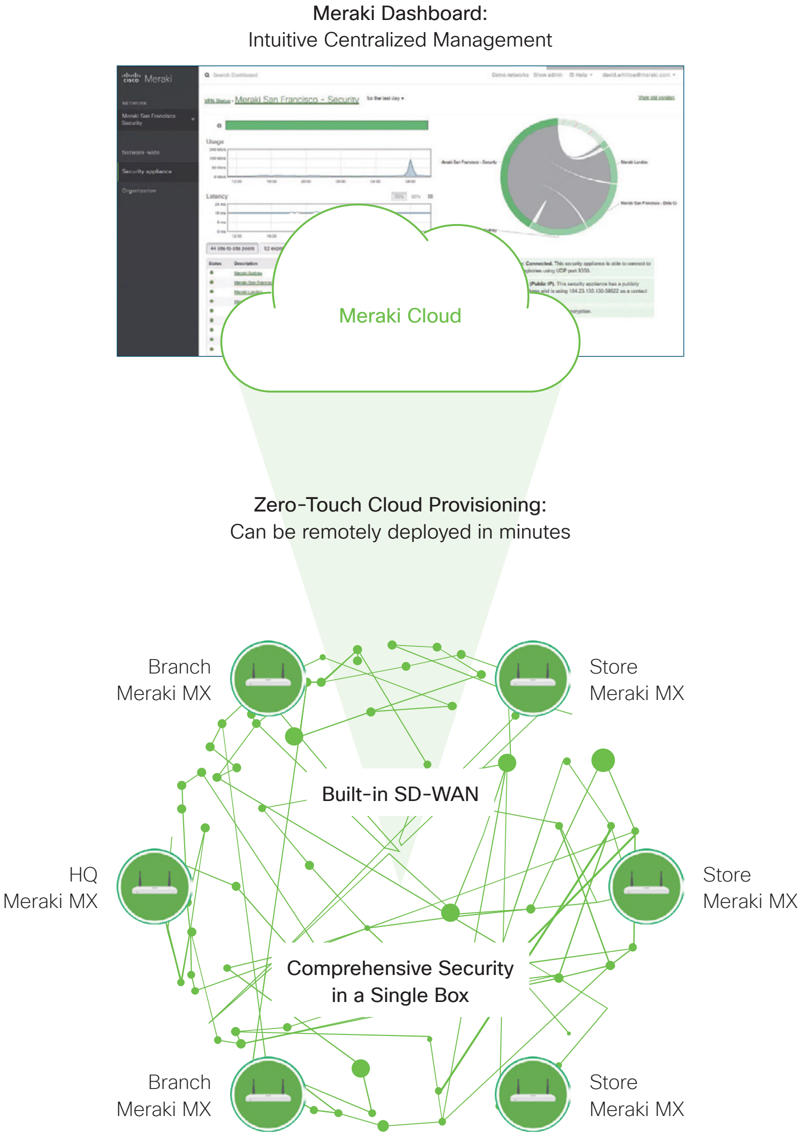
  PbR functionality allows administrators to assign traffic to a particular VPN path based on criteria such as traffic protocol, source, destination, or application.

- Dynamic Path Selection

  Dynamic path selection allows administrators to set performance thresholds for different types of traffic, in order to ensure that critical applications and data transfers always use the best path based on the loss, latency, and jitter over the available VPN tunnels.

- Meraki Insight WAN Health

  The WAN Health feature is specifically designed to monitor ISP connections, and it will help with troubleshooting and reporting for these connections. In addition to active/primary ISP uplinks, WAN Health will also monitor secondary/failover connections (such as WAN2 and LTE connections).


Meraki Dashboard:
Intuitive Centralized Management
Meraki Cloud
Zero-Touch Cloud Provisioning:
Can be remotely deployed in minutes
Branch Meraki MX
Store Meraki MX
Built-in SD-WAN
HQ Meraki MX
Store Meraki MX
Comprehensive Security in a Single Box
Branch Meraki MX
Store Meraki MX

Cisco Meraki Z Cloud Managed Teleworker Gateway

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
- Built-in 4G LTE (Category 3) wireless WAN (Meraki Z3C)
- USB port for 3G/4G connectivity
- GE downlinks for printers, phones and other wired devices
- PoE output for VoIP phones and other powered devices
- Built-in 802.11ac Wave 2 wireless access point
- Up to 4 SSIDs with integrated enterprise security and personal/guest access
- Sleek, low profile design
- Optional desk stand

Getting Started
What’s New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

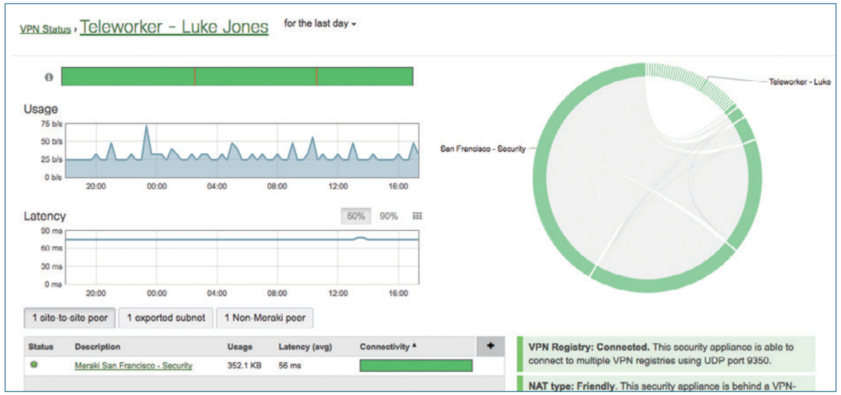
Cisco Meraki Z Cloud Managed Teleworker Gateway

Overview | Platform Spec | Licenses & Accessories

Product SKU	Recommended Clients	Throughput		WAN Ports		LAN Ports		WLAN	Power Supply	Rack Mount
		Stateful Firewall	VPN	GE	4G LTE	GE	GE PoE	11ac AP		
Z3-HW	5	100 Mbps	50 Mbps	1	-*1	3	1	●	External	-*2
Z3C-HW-WW	5	100 Mbps	50 Mbps	1	●	3	1	●	External	-*2

*1 Cellular Modem is required.

*2 Desktop or Wall mountable with included mount hardware. Vertical Desk Stand (MA-STND-1) is available.



VPN Status › Teleworker - Luke Jones for the last day

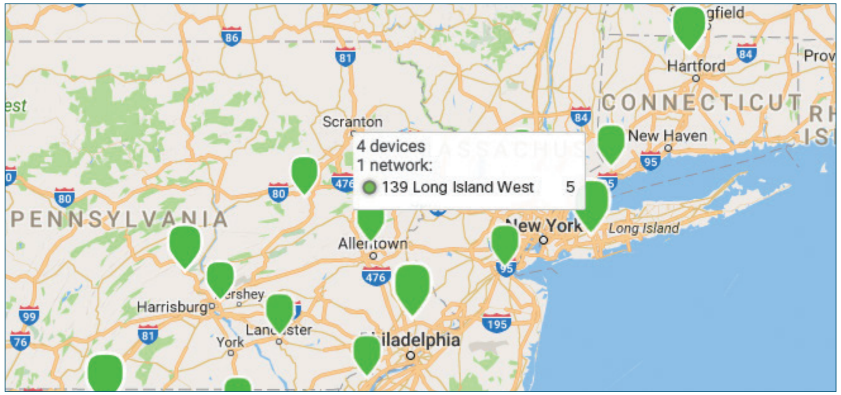
Status	Description	Usage	Latency (avg)	Connectivity ▴
●	Meraki San Francisco - Security	352.1 KB	56 ms	

VPN Registry: Connected. This security appliance is able to connect to multiple VPN registries using UDP port 9350.

NAT type: Friendly. This security appliance is behind a VPN-

Auto Configuring Site-to-Site VPN

Multi-Site Management via the Meraki Cloud



Secure - Security

Cisco Meraki Z Cloud Managed Teleworker Gateway

WEB

Cisco Meraki Enterprise Licenses for Cisco Meraki Z Series

Product SKU					Compatible Models
1-Year	3-Years	5-Years	7-Years	10-Years	
LIC-Z3-ENT-1YR	LIC-Z3-ENT-3YR	LIC-Z3-ENT-5YR	LIC-Z3-ENT-7YR	LIC-Z3-ENT-10YR	Z3
LIC-Z3C-ENT-1YR	LIC-Z3C-ENT-3YR	LIC-Z3C-ENT-5YR	LIC-Z3C-ENT-7YR	LIC-Z3C-ENT-10YR	Z3C

Cisco Meraki Insight Licenses for Cisco Meraki MX Series

Product SKU			Supported Throughput	Compatible Models
1-Year	3-Years	5-Years		
LIC-MI-XS-1YR	LIC-MI-XS-3YR	LIC-MI-XS-5YR	100 Mbps	Z3, Z3C

Cisco Meraki Vertical Desk Stand for Cisco Meraki Z3

Product SKU	Description
MA-STND-1	Vertical Desk Stand

Cisco Meraki MV Cloud Managed Smart Cameras

WEB

Bringing Meraki Magic to the Video Security World

The Cisco Meraki MV Cloud Managed Smart Cameras bring powerful, advanced analytics to the typical security camera world. With a powerful processor —the same kind found on many of today's smartphones— and an innovative architecture which minimizes physical infrastructure as well as software requirements, these smart cameras from Cisco Meraki represent a shift from cameras simply ensuring physical safety and security, to providing powerful business intelligence as well.

Highlights

- Centralized Cloud Management: The Meraki dashboard provides secure monitoring and management of all your cameras from anywhere in the world
- Edge Storage: Up to 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 Cisco Meraki MV
- 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

Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

Secure - Security

Cisco Meraki MV Cloud Managed Smart Cameras

Overview | Platform Spec | Licenses & Accessories | Why Meraki MV?

Model	Indoor					Outdoor
Product SKU	**MV12WE-HW**	**MV12W-HW**	**MV12N-HW**	**MV22-HW** NEW	**MV32-HW** NEW	**MV72-HW** NEW
Camera	1/3" 4 MP (2,688 × 1,520) progressive CMOS image sensor	1/3" 4 MP (2,688 × 1,520) progressive CMOS image sensor	1/3" 4 MP (2,688 × 1,520) progressive CMOS image sensor	1/3" 4 MP (2,688 × 1,520) progressive CMOS image sensor	1/3" 8.4 MP (2,058 × 2,058) progressive CMOS image sensor	1/3" 4 MP (2,688 × 1,520) progressive CMOS image sensor
	2.8 mm focal length	2.8 mm focal length	3.8 mm focal length	3 ~ 9 mm vari-focal lens	1.19 mm focal length	3 ~ 9 mm vari-focal lens
	Horizontal 114° Vertical 61° Diagonal 132°	Horizontal 114° Vertical 61° Diagonal 132°	Horizontal 73° Vertical 44° Diagonal 86°	Horizontal 36 ~ 112° Vertical 20 ~ 57° Diagonal 42 ~ 138° Tilt: 65° Rotation: +/- 90° Pan: 354°	Horizontal 180° Vertical 180°	Horizontal 36 ~ 112° Vertical 20 ~ 57° Diagonal 42 ~ 138° Tilt: 65° Rotation: +/- 90° Pan: 354°
	Minimum illumination 0.18 Lux (standard) 0.01 Lux (night mode)	Minimum illumination 0.18 Lux (standard) 0.01 Lux (night mode)	Minimum illumination 0.18 Lux (standard) 0.01 Lux (night mode)	Minimum illumination 0.18 Lux (standard) 0.01 Lux (night mode)	Minimum illumination 0.18 Lux	Minimum illumination 0.18 Lux (standard) 0.01 Lux (night mode)
	Built-in IR illuminators effective up to 15 m	Built-in IR illuminators effective up to 15 m	Built-in IR illuminators effective up to 15 m	Built-in IR illuminators effective up to 30 m	-	Built-in IR illuminators effective up to 30 m
Video	Full HD (1,920 × 1,080) H.264 encoding up to 20 fps	Full HD (1,920 × 1,080) H.264 encoding up to 20 fps	Full HD (1,920 × 1,080) H.264 encoding up to 20 fps	Full HD (1,920 × 1,080) H.264 encoding up to 20 fps	4.2 MP (2,058 x 2,058) H.264 encoding up to 15 fps	Full HD (1,920 × 1,080) H.264 encoding up to 20 fps
Microphone	●	●	●	●	●	●
Storage	128 GB SSD	256 GB SSD	256 GB SSD	256 GB SSD	256 GB SSD	256 GB SSD
Interface	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)	1 x GE 1 x 11b/g/n (2.4 GHz) 1 x 11a/n/ac (5 GHz)
Power	802.3af/at	802.3af/at	802.3af/at	802.3af/at	802.3af/at	802.3af/at
Dimensions	106 mm x 74 mm (diameter × height)	106 mm x 74 mm (diameter × height)	106 mm x 74 mm (diameter × height)	149 mm x 97 mm (diameter × height)	106 mm x 45.86 mm (diameter x height)	165 mm x 103 mm (diameter × height)
Weight	286 g	286 g	286 g	706 g	215 g	1,247 g
Weather-Proof IP66	-	-	-	-	-	●
Vandal-Proof IK10	-	-	-	-	-	●

Secure - Security

Cisco Meraki MV Cloud Managed Smart Cameras

WEB

Overview | Platform Spec | Licenses & Accessories | Why Meraki MV?

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 Meraki MV

Cisco Meraki Power Injector & Power Supply for Cisco Meraki MV Series

Product SKU	Description	Compatible Models
MA-INJ-4-xx	PoE Injector (802.3at)	All Meraki MV
MA-PWR-MV-LV	Low Voltage (12 VDC/24 VAC) Power Adapter	All Meraki MV

Cisco Meraki Mount Kits for Cisco Meraki MV Series

Product SKU	Description	Compatible Models				
		MV12WE	MV12W	MV12N	MV22	MV72
MA-MNT-MV-10	Wall Mount Arm	-	-	-	-	●
MA-MNT-MV-20	Pole Mount	-	-	-	-	●
MA-MNT-MV-30	Wall Mount Arm	●	●	●	-	-
MA-MNT-MV-31	Wall Mount Bracket	-	-	-	●	-

Cisco Meraki MV Cloud Managed Smart Cameras

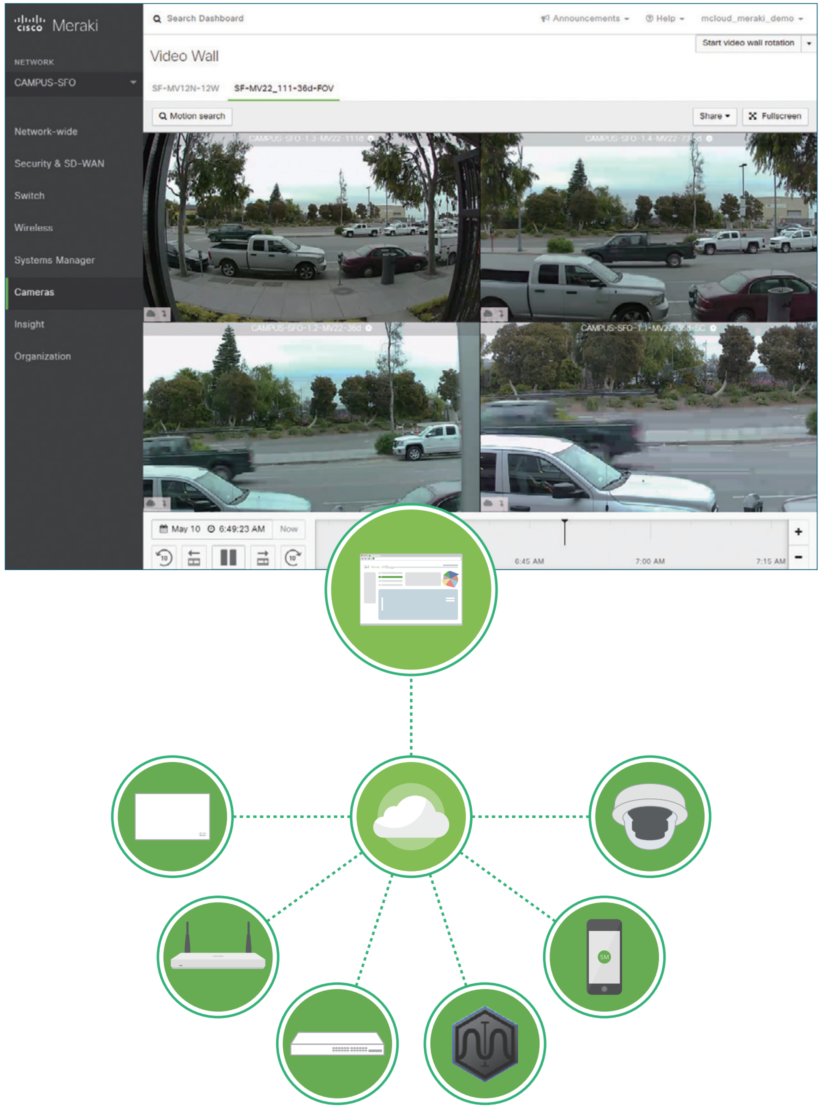
Cloud Management Architecture

Cisco Meraki's architecture provides feature rich network management without on-site management appliances or Wi-Fi controllers.

Every Meraki device —including access points, switches, security appliances, and cameras— connects over the Internet to Meraki's datacenters, which run Meraki's cloud management platform.

These connections, secured via SSL, utilize a patented protocol that provides real time visibility and control, yet uses minimal bandwidth overhead (typically 1 kbps or less.)

In place of traditional command-line based network configuration, Meraki provides a rich web based dashboard, providing visibility and control over up to tens of thousands of Meraki devices, anywhere in the world. Tools, designed to scale to large and distributed networks, make policy changes, firmware updates, deploying new branches, etc. simple and expedient, regardless of size or location. Meraki's real time protocols combine the immediacy of on-premise management applications with the simplicity and centralized control of a cloud application.



Getting Started
What's New
Feature Story
Collaborate
Compute
Security
ASA 5500-X
Firepower 2100
AnyConnect
AMP for Endpoints
Umbrella
Meraki MX
Meraki Z
NEW Meraki MV
Connect
Switches
Wireless
Routers
Services

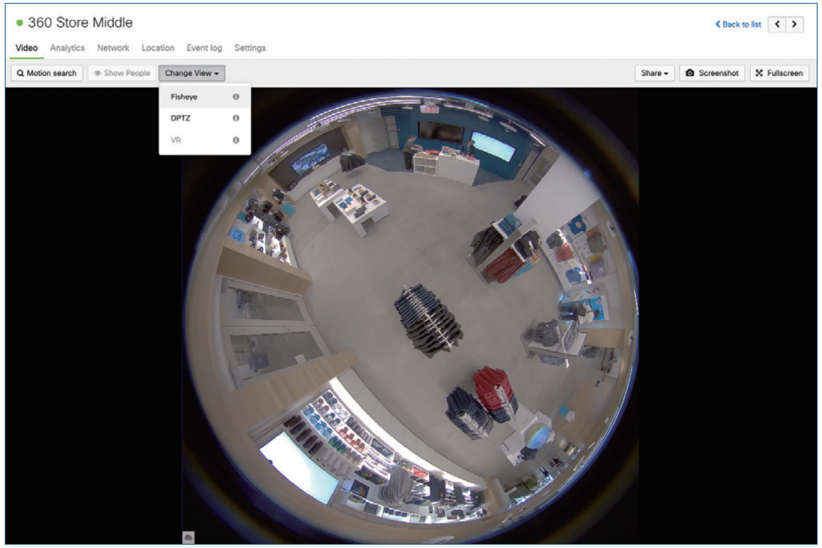
Cisco Meraki MV Cloud Managed Smart Cameras

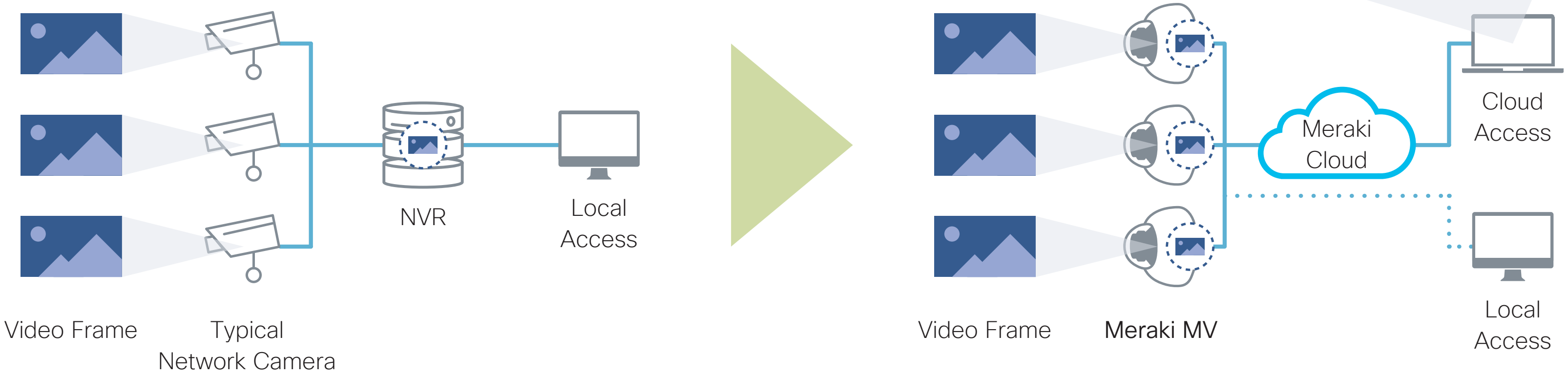
Overview | Platform Spec | Licenses & Accessories | Why Meraki MV?

Cutting Edge Architecture

Cisco Meraki's expertise in distributed computing has come to the security camera world. With cloud-augmented edge storage, the Cisco Meraki MV provides ground breaking ease of deployment, configuration, and operation. Completely eliminating the Network Video Recorder (NVR) not only reduces equipment CAPEX, but the simplified architecture also minimizes lifetime OPEX costs.

Each Cisco Meraki MV comes with integrated, ultra reliable, industrial-grade storage. This cutting edge technology allows the system to efficiently scale to any size because the storage expands with the addition of each camera. Plus, administrators can rest easy knowing that even if the network connection cuts out, the cameras will continue to record footage.





Cisco Meraki MV Cloud Managed Smart Cameras

Beyond Just Security

The Cisco Meraki MV utilizes a powerful onboard processor to analyze video and provide valuable insights without the need to send those video files to the cloud or a local server.

- **Motion Heat Maps**

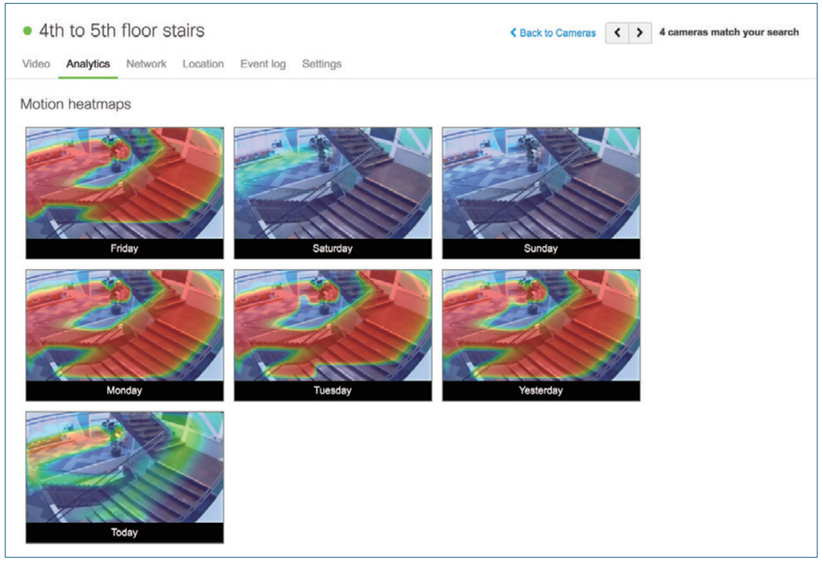
  Quickly assess foot traffic in a retail store or monitor where hotel guests are congregating in the lobby. Motion heat maps only require a small amount of metadata, rather than bulky video files, to provide results with big impact.

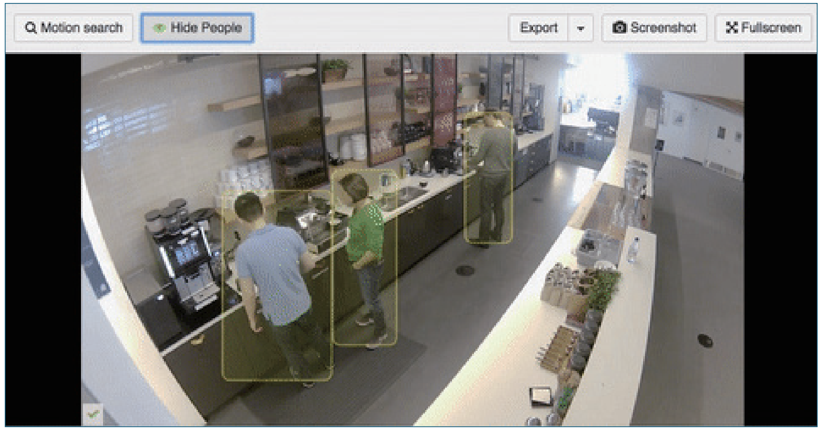
- **Object Detection**

  Learn which displays are attracting the most customers or how many people came to the office last Thursday. The ability to detect people using computer vision and increase accuracy over time through machine learning will provide deep business insights that were previously only possible with bulky servers.

- **Privacy Matters**

  All Cisco Meraki MV analytics functionalities are anonymized to ensure privacy while still providing intelligence. You'll know that a customer entered your store at 3:38, but not that her name is Sarah.


4th to 5th floor stairs
Back to Cameras
4 cameras match your search
Video
Analytics
Network
Location
Event log
Settings
Motion heatmaps
Friday
Saturday
Sunday
Monday
Tuesday
Yesterday
Today


Motion search
Hide People
Export
Screenshot
Fullscreen