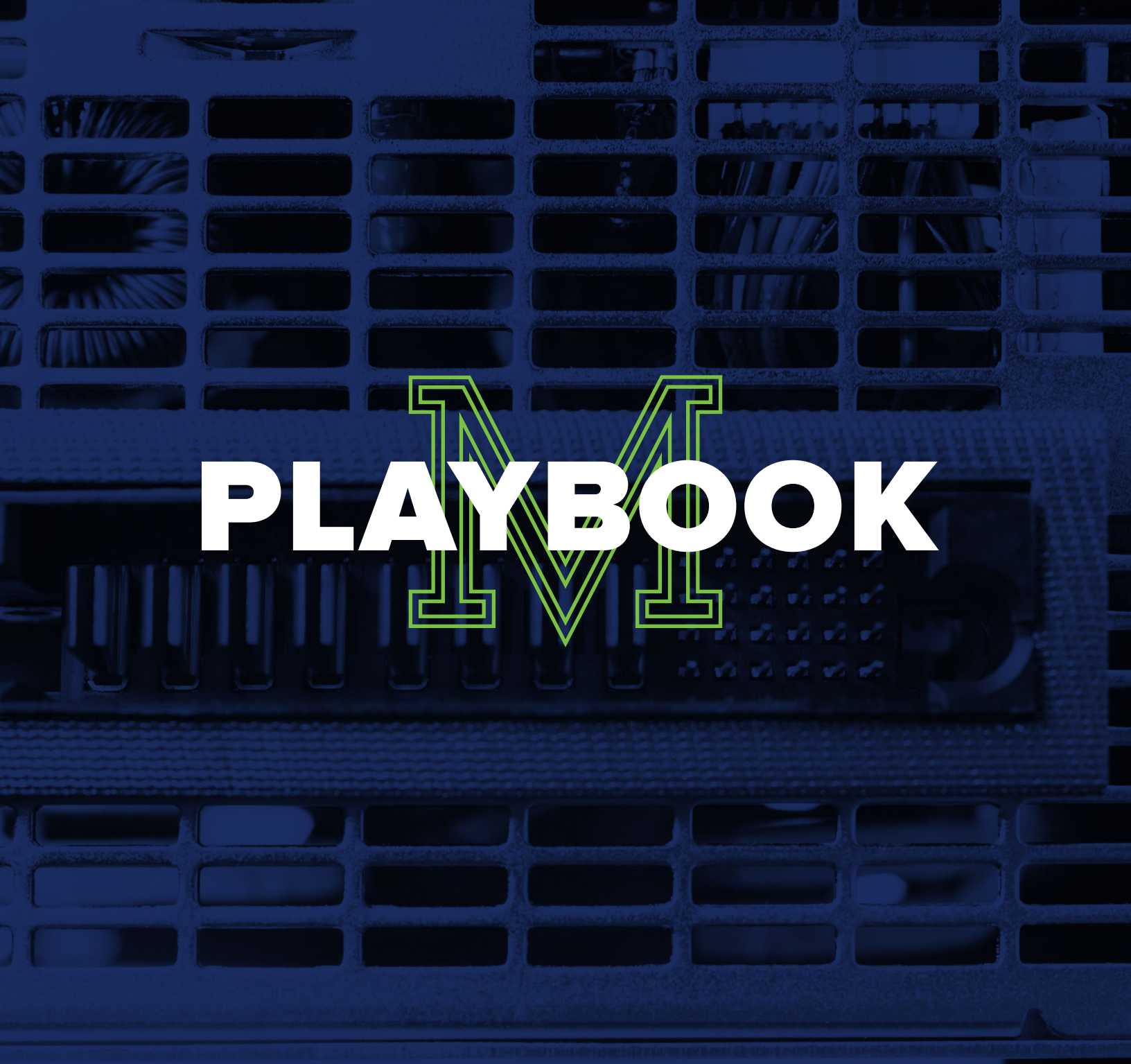


PLAYBOOK

SECURITY MADE SIMPLE

PARTNER

Table of Contents

General Overview

IT administrators have a difficult job of not only installing networking gear, keeping it updated, but also managing everything from clients to applications. If this weren't enough, they must also consider security. With so many different types of users trying to access the network – employees, guests, contractors – and different types of devices - corporate-owned laptops, employee-owned smartphones, IoT devices - IT administrators need a scalable way to manage network, device, and user access and security.

This results in IT teams trying multiple vendors, with disparate dashboards, manual integrations and several boxes to secure their network. In fact, more than 25% of organizations use 1-20 vendors to try and secure their networks.[1] This vast array of disparate solutions obfuscate rather than simplify the security landscape. Eventually, IT admins give up and throw in a basic firewall. While they understand the value of implementing a security posture that affects every layer of the network, they normally do not have the manpower and time required to implement these solutions. Malicious attackers take advantage of those vulnerabilities. Over 43% of cyber-security attacks target SMBs[2] with lean IT teams and greater than 74% of these attacks exploit inadequate network access and security policies.[3]

Meraki comes to the rescue! With a single dashboard, you can now not only manage your entire network but also apply sophisticated security and access policies. The cloud-based Meraki dashboard ensures that all products are patched and up to date at all times. Meraki is also open and has extensible APIs to further integrate with the Cisco security portfolio.

These new Meraki products and features provide end-to-end security from the client to the application. With these new capabilities, your customers will increase productivity and reduce errors from manual, repetitive tasks. Meanwhile, you can provide a differentiated solution that allows customers to dynamically scale their automation and security efforts across the full stack.

When you sell Meraki, you add value to your customers by future-proofing their investment as new features are continually released. Meraki also gives you an opportunity to upsell and cross-sell since customer networks with full stack Meraki gear work better together.

Read on to learn more about the products and features we are launching. If you have additional questions, please reach out to your Meraki sales representative.

Happy Selling!

1 Cisco Annual Cybersecurity Report 2018
2 Cisco Annual Cybersecurity Report 2018
3 Cisco Annual Cybersecurity Report 2018

Hardware Updates

OVERVIEW

The MS390 combines the power of Cisco's UADP 2.0 ASIC with the simplicity of the Meraki dashboard to micro-segment different users and devices in a network . This can be used to apply powerful security and access policies so that the customer's business doesn't become the next data breach headline. With modular uplinks, power supplies, and a custom-built ASIC, the MS390 is the most powerful access switch in the Meraki portfolio that solves a host of problems for IT admins.

NOW ANNOUNCING

MS390 is the most powerful access switch ever produced by Meraki which combines the simplicity of cloud-managed IT with the power of purpose-built Cisco silicon. In addition to traditional switching functions, the MS390 provides the option of enabling sophisticated security and access policies based on micro-segmentation of user-groups instead of difficult-to-decipher individual IP addresses. Additional key features include the following:

- Helps customers meet the most demanding quality-of-service requirements
  using the purpose-built UADP 2.0 ASIC
- Offers 3x the throughput (480 Gbps) over its predecessor (MS350) and features a full 48-port mGig SKU with hot-swappable modular uplinks where customers can choose between 1G / 10 G / 40Gbps uplinks as needs of the network change
- Features improved physical stacking which reduces latency to <1 second for faster stack convergence in case of a switch failure which is critical for enterprise deployments
- Includes StackPower which pools all available power supply to become an additional power redundancy source

CUSTOMER CHALLENGES

Most enterprise switching networks are error-prone, complicated, and require manual configuration using CLI. With the Influx of Wi-Fi 6 capable access points, the steady deluge of traffic from IoT devices, and the increase in the average number of devices per user, there will be an increase in throughput and strain to the current switching infrastructure. This will make manual configuration and policy setting expensive and unmanageable. While Wi-Fi 6 access points are able to deliver higher bandwidth, the current cabling was designed for only 1 Gbps. The MS390 series of switches come with Multigigabit technology that extends the life of existing cabling at 1 to10 Gbps capability.

KEY TAKEAWAYS

The UADP 2.0 ASIC on the MS390 series of switches makes it easier to deliver intent-based networking everywhere. Customers can micro-segment users based on who they are instead of where they are to apply sophisticated access and security policies. MS390's feature-rich hardware also delivers on easier stack-management and efficient power management with the unparalleled simplicity of the Meraki dashboard.

USE CASES

The MS390 switch is great for customers that want the best-in-class, cloud-managed switches to match Wi-Fi 6 access points and those who are expanding to a new campus, branch, or building, and also to those who want to micro-segment users to apply access and security policies.

UPSELL OR CROSS SELL OPPORTUNITIES

MS390 can cross-sell ISE.

TARGET CUSTOMERS

- MS350 or MS355 customers that are ready for a refresh
- MR45 or MR55 customers that require a higher throughput switch
- Government
- Retail
- Healthcare
- Financial Services
- Higher Ed and K-12

OBJECTION HANDLING

What advantages does this have compared to the Catalyst 9300 series?

The MS390 combines the power of the UADP 2.0 Cisco ASIC which is at the heart of the Catalyst 9300 series with the simplicity of the Meraki dashboard. If a customer values the simplicity and the scale offered by the Meraki dashboard but also wants the power of advanced hardware, the MS390 is the answer.

How do I justify the price increase when compared to the MS350 / MS355?

MS390 combines powerful enterprise switching features with the simplicity of cloud-management for the first time. It comes with StackPower, improved physical stacking, modular uplinks, and the UADP 2.0 ASIC which enables you to apply advanced access security and access policies.

What if I want to integrate with non-Cisco Security vendors?

Meraki has a rich legacy of simplifying powerful standards-based technologies and making expertise available to everyone. From OSPF to RADIUS, Meraki has always allowed for interoperability and will continue to do so in the future.

Is there any benefit to using an MS390 if I have access points from another vendor?

Applying intent-based policies at scale with Adaptive Policy is a unique Cisco advantage. The mGig option and PoE budget available can be used to manage network capacity and bring efficiency to power management across any vendor's APs.

For additional information, please review the MS390 series FAQ found in the appendix.

Software and Feature Updates

Adaptive Policy

OVERVIEW

As a company grows and adds new devices, users, and applications, the traditional method of redoing the collection of IP addresses in the network is a daunting task. In addition to this, IP addresses do not provide user, device, and application information. Adaptive Policy aims to put security front and center by adding the who, what, and when of each communication line to IP addresses, without compromising switch hardware resource and capacity.

NOW ANNOUNCING

Adaptive Policy is a software feature built for the MS390 to provide an additional layer of security based on the intent of the user, device, and application. It implements network policies that automatically adjust to the business environment based on the intent of the client, user application or device.

CUSTOMER CHALLENGES

Many networks lack security and assurance. With so many types of security offerings in the market, it can be difficult for customers to know which solution to implement, especially when many solutions are complex, costly, complicated, and difficult to scale. They often require multiple on-prem hardware devices to implement and manage, making it difficult for lean IT teams to feel confident in their security offering.

KEY TAKEAWAYS

Adaptive Policy solves today's network problems by providing effective security, reduced operational costs, powerful automation, greater visibility, better hardware efficiency, and increased business productivity.

USE CASES

Adaptive Policy is great for large organizations that are looking to segment their network, to gain more application and resource control, and to prioritize end device quarantine and remediation. It is the perfect solution for customers who put a priority and a premium on security, all while looking for a simple and scalable solution.

UPSELL OR CROSS SELL OPPORTUNITIES

Adaptive Policy can be cross-sold with ISE as well as Meraki Wi-Fi 6 APs (MR45/55).

TARGET CUSTOMERS

- Healthcare
- Enterprises with branch locations
- Financial Institutions
- Existing Cisco ISE and Cisco Catalyst customers

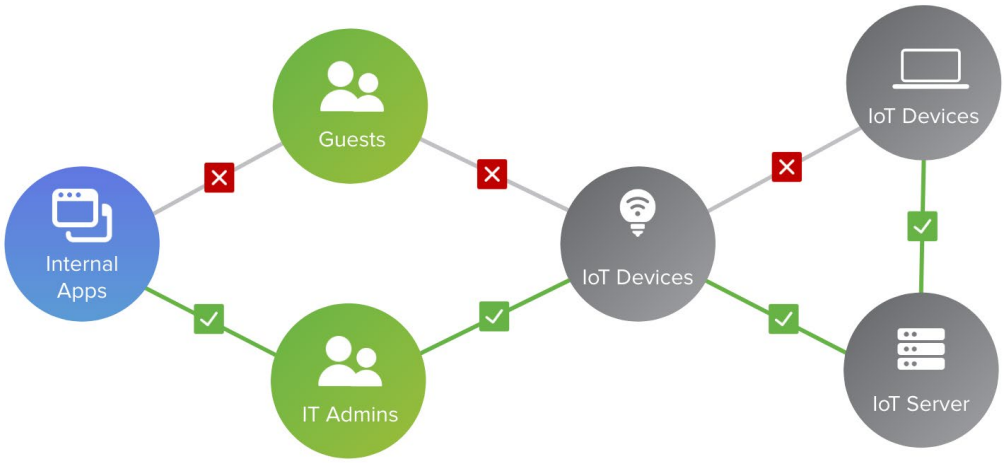
OBJECTION HANDLING

If the customer has already bought more complex solutions that work, why would they switch to Meraki?

Other solutions have continuous high overhead, require additional hardware to support, are not centralized, and do not provide as much visibility as the Meraki cloud infrastructure model.

PRICING

Adaptive Policy is available with the purchase of the Advanced MS390 License.



SecureConnect

OVERVIEW

Networking hardware is susceptible to potential threats. SecureConnect is the simplest and most effective way of securing switch ports and automating device configurations. No other vendor enables this level of security in just a few clicks.

NOW ANNOUNCING

SecureConnect is a software feature available for all MS models from MS210 and above, as well as all 802.11ac and 802.11ax MR models. SecureConnect enables MS to detect and verify that the MR connected to the port belongs to the same organization and then automatically pushes configurations down to the connected MR.

CUSTOMER CHALLENGES

IT teams often do not have time to manually check the security status of devices, and many customers do not have enough budget to implement reliable security and authentication solutions. At the same time, networking hardware (access points and switches) are becoming more vulnerable to potential threats and, as more devices are brought into the network, errors can arise from improper configuration. Rogue access points can be plugged into open switch ports which result in being a source of threats. On top of this, robust 802.1X security and authentication methods to secure switch ports are complicated to set up.

KEY TAKEAWAYS

SecureConnect provides customers with reliable security, extensible automation, increased productivity, and eliminates potential configuration errors. It speaks to the benefits of the Meraki licensing model as well as the power of the Meraki cloud to deliver future software features our customers deserve. Meraki continues to solve security needs with cross-product features so that customers invested in Meraki can continue benefiting from the Meraki solution.

USE CASES

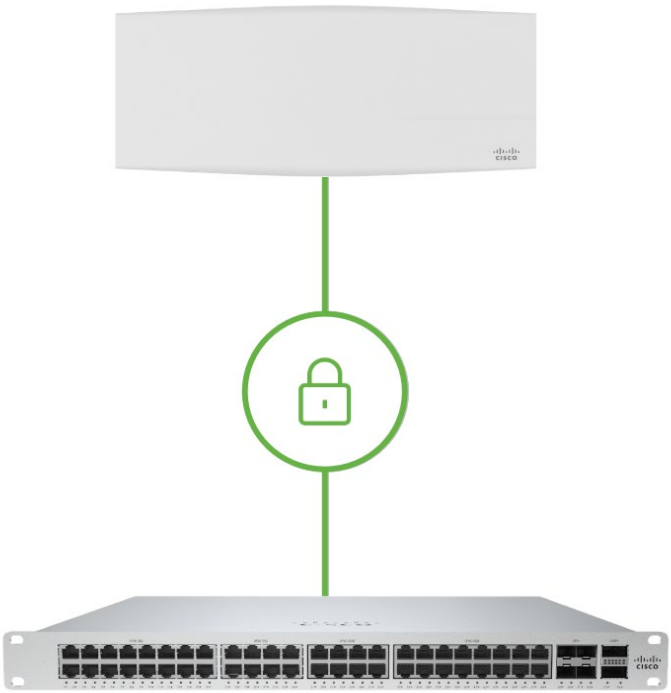
Current Meraki MR and MS customers can take advantage of this feature. Net new customers (any size or in any industry) interested in MR and MS integrations and looking for scalable, automated hardware security are a good fit for this feature.

UPSELL OR CROSS SELL OPPORTUNITIES

With SecureConnect, there are many more opportunities to sell MR and MS together. Cross sell MS to MR-only customers, and MR to MS-only customers

PRICING

These features are available at no additional cost as part of the functionality of the current Meraki switch (MS) licenses.



Trusted Access

OVERVIEW

Being certain about who is trying to connect, with what device type, and when is far from the IT admin's reality. Meraki Trusted Access provides visibility into users and devices as well as enables secure network access seamlessly.

NOW ANNOUNCING

Meraki Trusted Access is a software feature that enables organizations to create a secure network connection between corporate assets and personal devices without the need to install a MDM agent/profile. Trusted Access requires MR + SM to enable. It is available for iOS, macOS, and Android devices.

CUSTOMER CHALLENGES

Today's networks have diverse device types and end users with varying network needs. Control over many devices (PCs, tablets, cell phones, cameras, IoT) and many end-users becomes a daunting task. The need to be constantly aware of what (and when) each end-user and device is trying to do on the network is a burden for IT.

KEY TAKEAWAYS

Meraki Trusted Access provides customers flexible authentication methods combined with advanced security. It offers an enhanced user experience, with visibility into users and devices. It also helps automate device onboarding and enforcement of security policies. Additionally, Meraki Trusted Access allows for custom integrations with the use of APIs.

USE CASES

Customers looking to implement scalable, secure network access without managing the devices themselves will find Trusted Access a good fit. Existing SM customers can also take advantage of this for their BYOD and temporary employee deployments.

TARGET CUSTOMERS

- Organizations that support BYOD
- Organizations requiring secure guest Wi-Fi where a splash page and/or password does not suffice
- Organizations with temporary or contracted Employees

UPSELL OR CROSS SELL OPPORTUNITIES

For net new customers, MR + SM can be bundled together. There is also the ability to cross sell SM to MR-only customers; MR to SM-only customers.

PRICING

This feature is available at no additional cost as part of the functionality of the current Meraki endpoint management (SM) license. No extra costs, no extra licenses. Just a simple 1:1 SM license to endpoint device will suffice.

Trustworthy Systems

OVERVIEW

Cisco Meraki is a differentiator in the market with its hardware full stack (MR access points, MS switches, and MX SD-WAN security appliances) supporting Cisco Trustworthy Systems.

NOW ANNOUNCING

Trustworthy Systems are a suite of Cisco solutions that ensure code running on its hardware platforms is authentic, unmodified, and operating as intended. It includes technologies such as image signing, secure boot, and Cisco Trust Anchor module (TAm). The multilayered approach, including a hardware-level root of trust, a unique device identity, and validation of all levels of software during startup, establishes a chain of trust for the system. Cisco Meraki hardware products now all support Cisco Trustworthy Systems.

CUSTOMER CHALLENGES

In 2015, SYNful Knock was a malware attack that targeted Cisco devices, reminding us how severely counterfeit products and cyber attacks can jeopardize any network.

KEY TAKEAWAYS

Cisco Trustworthy Systems promises security and trust in its hardware products in order to prevent threats such as counterfeit products and cyberattacks. The Meraki full stack is an enterprise solution that can now be trusted with a Trustworthy Systems network infrastructure.

PRICING

These features are available at no additional cost as part of the functionality of all Meraki products.

Umbrella + MR License

OVERVIEW

Customers can now secure their networks by combining the power of Cisco Umbrella's DNS security solution with the simplicity of the Meraki dashboard. The new MR Advanced and Upgrade license automatically enables Meraki-defined policies at the DNS layer in your network. With the new license, customers can also gain visibility into blocked DNS events from within the Meraki dashboard. IT administrators no longer have to manually integrate Umbrella with their MR access points and can now scale security deployments across multiple sites in minutes.

NOW ANNOUNCING

Meraki is launching a new license that provides customers with granular visibility into blocked internet events using the Security Center in the Meraki dashboard. Customers can also deploy predefined policies without manual integration. With the addition of Security Center to the Meraki dashboard, customers will also be able to monitor, protect, and troubleshoot their wireless networks at a DNS level. New customers can purchase the Advanced license SKU to access these joint features, and existing wireless customers can buy the Upgrade license SKU to enable protection against malware, C2 callbacks, and phising, powered by Umbrella on their Meraki network.

CUSTOMER CHALLENGES

In today's world, many technology vendors offer complex deployments, often with their own dashboard for monitoring and managing network policies. It's difficult for IT admins to focus on security full-time and scale their efforts with disparate dashboards. These IT admins require not only a centralized view for easier daily management, but also demand a way to protect users and guests from threats like malware and ransomware.

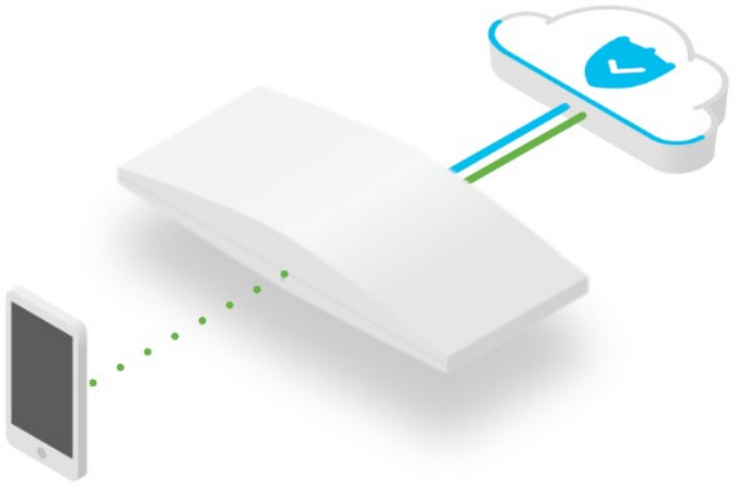
KEY TAKEAWAYS

The new license that combines Umbrella and MR brings unparalleled simplicity and centralization. Customers can deploy DNS layer security across all Meraki APs over the cloud without the need for additional hardware or virtual machines. Meraki also has created API end-points to fetch and deploy predefined policies to protect users against most internet threats. IT administrators can now deploy DNS layer security at scale, across multiple networks to create a simple and secure digital workplace.

Umbrella + MR License

USE CASES

This new licensing is best for organizations who prioritize simplicity, scale, and centralized security management. This license is particularly relevant for organizations who need to meet compliance standards (such as CIPA), networks with many BYOD devices, and networks where admins want to seamlessly secure guest Wi-Fi.



TARGET CUSTOMERS

- SLED
- Retail
- Education (K-12)
- Government
- Retail & Hospitality
- Professional Services
- SMB customers with lean IT teams
- Service Providers* who use pre-defined policies

** Umbrella has a specific solution for SPs who prefer to create custom policies which is not available through this license. If those SPs want to use the Meraki dashboard, they'll have to use manual integration like before.*

UPSELL OR CROSS SELL OPPORTUNITIES

- Existing MR customers
- Existing SMB customers
- Existing Umbrella customers

OBJECTION HANDLING

Why do I need security for my wireless network if I already have a firewall?

Traditional approaches like enabling a basic firewall will only protect you from a very small range of attacks. However, attacks are increasing in sophistication, and legacy firewalls are failing because they are not based on real-time analysis. The new class of attacks can easily be hidden amongst legitimate traffic and slip through firewalls. DNS security on Meraki APs powered by Cisco Umbrella provides you with multiple levels of defense against internet-based threats and enables you to extend protection from your network to branch offices. Umbrella integrates secure web gateway, firewall, DNS-layer security, and cloud access security broker (CASB) functionality for the most effective protection against threats.

Why is the new license so expensive?

This new single license is actually cheaper than purchasing the license for Meraki APs and Umbrella separately. You get additional features like the industry-leading Security center and the ease of viewing and managing your DNS events right from the Meraki dashboard without manual integration. 53% of cybersecurity attacks result in damages of $500,000 or more and the aim of this integration is to prevent customers from being hacked and becoming the next data breach headline.

What if the customer says, "We don't have the budget at the moment!"?

Let's get the customer a free trial to see the value of this technology, and then we can always provide the Upgrade (LIC-MR-UPGR) license down the line when their budget opens up.

What if the customers says, "Sounds awesome, but I don't have enough time to implement additional security."?

Umbrella and Meraki are both delivered over the cloud, and they work without any manual integration. Once you purchase the license, DNS security is automatically enabled in the Meraki dashboard and you get access to the Security Center with the pre-defined DNS security policies. So there is no hassle for you to set this up.

For additional information, please review the Umbrella + MR License FAQ found in the appendix.

API Integration of MX with Cisco Defense Orchestrator (CDO)

OVERVIEW

Cisco Defense Orchestrator (CDO) is a cloud-based management solution that allows you to manage security policies and configurations with ease across your Cisco security products, now including the Meraki MX.

NOW ANNOUNCING

CDO now supports the Meraki MX. It strengthens security by aligning policies throughout an organization regardless of the Cisco security product. This simplifies managing security policies across multiple Cisco security products to prevent inconsistencies and gaps. Customers with a mix of Cisco security products including the Meraki MX will find value by using CDO to unify, maintain, and update policies across all locations in their organization.

CUSTOMER CHALLENGES

IT and security admins have a tough job creating and maintaining security policies, applying templates across devices, and making sure everything is up to date.

KEY TAKEAWAYS

CDO is a powerful solution that unifies security management across a hybrid Cisco and Meraki infrastructure.

USE CASES

This cloud-based solution with an open API framework allows teams to easily apply and update settings across hybrid Cisco and Meraki deployments with minimal training and effort. Customers with a hybrid solution of Cisco and Meraki security products will find the most value in this solution.

API Integration of MX with Cisco Defense Orchestrator (CDO)

OBJECTION HANDLING

Doesn't the Meraki dashboard already do this?

The Meraki dashboard can orchestrate and unify security policies across Meraki devices. Now with CDO, admins can unify and update policies across a mix of Cisco security products, including Meraki MX appliances.

UPSELL OR CROSS SELL OPPORTUNITIES

Because the CDO allows admins to unify policies across Cisco security technologies, this is an ideal tool for customers looking to implement a hybrid of Cisco security, including the Meraki MX, across campus and branch locations.

PRICING

This is an existing Cisco tool and product already available in CCW that now supports security policies on Meraki MX appliances.

Identity Pre-Shared Key (iPSK)

OVERVIEW

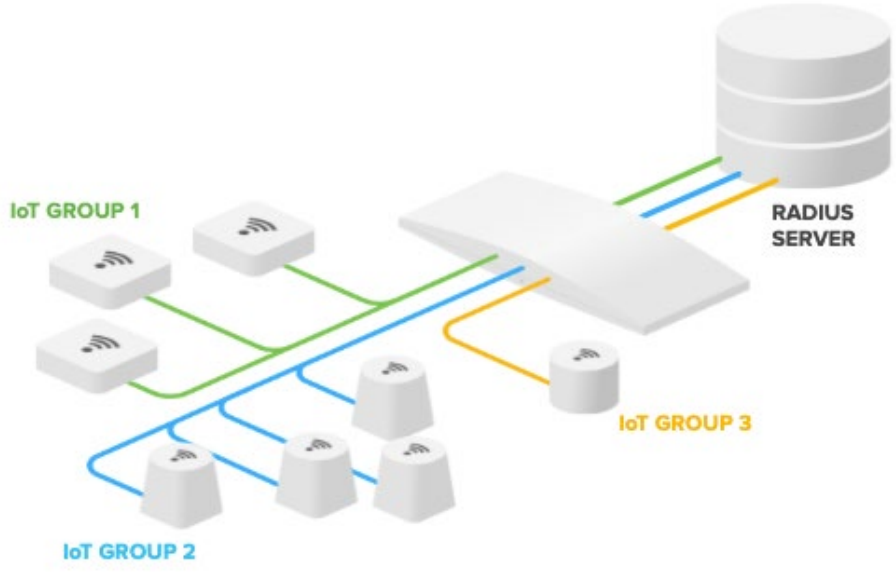
With IoT devices proliferating, network admins are dealing with an exponential increase in the number of devices connecting to wireless networks. Not all of these devices support 802.1X authentication, which makes authentication difficult. WPA-PSK is used today, but can result in the possibility of a key being shared to unauthorized users. Securing a wireless network will be made much simpler with iPSK (Identity Pre-shared Key).

NOW ANNOUNCING

iPSK is a new MR feature that authenticates wireless devices more securely that previous methods such as WPA-PSK. It does not require additional certificates or 802.1X. Instead of a single pre-shared key being shared to any device connecting to a SSID, a unique PSK is correlated with the device's MAC address and is authenticated via a RADIUS server. This feature also allows separate group policies to be assigned within a single SSID, based on the PSK used. For example, all devices using PSK "Meraki123" will automatically be assigned group policy 1, while devices using PSK "Meraki456" automatically receive group policy 2.

CUSTOMER CHALLENGES

Networks have a rapidly growing number of devices connecting wirelessly, and keeping these devices secure is a challenge. Providing users with a pre-shared key can compromise a network if it gets in the wrong hands. Although creating multiple SSIDs can help segment devices, it also degrades the performance of the wireless network. There is also the desire to contain instances where the PSK is shared with the public. For example, the County Government PSK is shared on a meeting board in a public conference room.



Identity Pre-Shared Key (iPSK)

KEY TAKEAWAYS

This feature allows organizations to secure their networks without creating multiple SSIDs, which can harm wireless performance. It provides additional security to organizations undergoing digital transformation.

USE CASES

Any network with many IoT devices (point-of sale, thermostats, cameras) where IT admins want to provide secure access to everybody with the simplicity of a PSK but the unique access of 802.1X.

UPSELL OR CROSS SELL OPPORTUNITIES

It is highly recommended to cross-sell iPSK with ISE.

TARGET CUSTOMERS

- SLED
- Retail
- Hospitality
- Enterprise

PRICING

This feature is available at no additional cost as part of the functionality of the current Meraki access point (MR) line as an additional function in Dashboard.

Firewall Object Groups

OVERVIEW

Firewall Object Groups allow network entities such as telephony, printers, and more to be mapped to an IP address or subnet. These network objects can then be grouped to simplify firewall rules on the MX.

NOW ANNOUNCING

Firewall Object Groups is a new MX feature that simplifies the process of creating and managing multiple firewall rules.

CUSTOMER CHALLENGES

Creating firewall rules on a line-by-line basis with no logic can be time consuming and error prone. Adding logical groupings consolidates the number of firewall rules needed and simplifies creation and management.

KEY TAKEAWAYS

It is now easier to create and manage firewall rules than ever before. This new process improves MX performance, and as a result, improves the simplicity of managing the network.

USE CASES

Many large organizations have multiple firewall rules to define access rules for different parts of the network. Firewall Object Groups help to simplify this previously manual process. Existing MX customers can immediately take advantage of this feature with their current devices, and prospective MX customers will be able to save time on their configuration and management.

PRICING

This feature is available at no additional cost as part of the functionality of the current Meraki MX security & SD-WAN appliance line.

In Other (Partner) News...

Camera

OVERVIEW

All Meraki MV smart cameras are built with true end-to-end encryption that it is on by default and cannot be turned off. With the addition of Trustworthy Systems, MV cameras are built with a tamper-resistant chip, installed with digitally-signed software to prevent exploitation by attackers. These features are available at no extra cost and come included with the Meraki smart camera (MV) line.

CUSTOMER CHALLENGES

For many customers, securing video with end-to-end encryption is challenging and often not possible. It's also difficult to keep camera systems secure to avoid risk of exploitation. To mitigate these concerns, some organizations keep cameras entirely off the network, limiting their ability to access the system or view video remotely.

KEY TAKEAWAYS

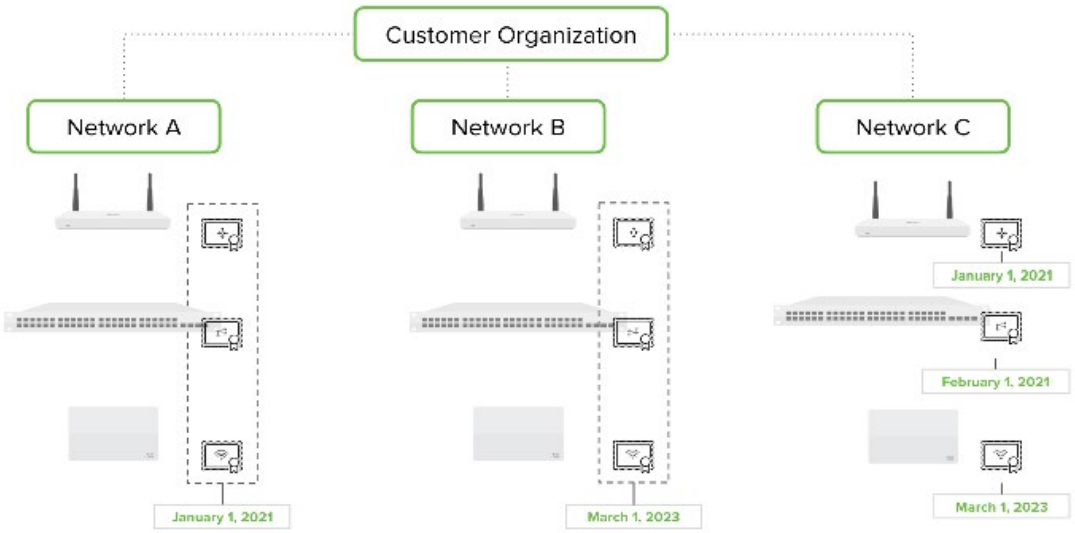
These features secure access to video stored on the camera and video in transit. They ensure that the software on the camera has not been tampered with to prevent exploitation by attackers. As you pitch the Meraki security story to your customers, the Meraki smart cameras are a great product to introduce to your customers to protect their physical security without compromising network security.

Per-Device Licensing

OVERVIEW

Cisco Meraki is introducing Per-Device Licensing - a new licensing model that is applied on a per-device basis, rather than a coterminous model. All devices within a Meraki network or organization could have a single expiration date, or may have individual expiration dates based on customer preference.

For example, suppose an organization had 2 separate Enterprise AP licenses, one license for 1-year (365 days) and another for 5 years (1825 days). If the devices and licenses were claimed on the same day, one of the wireless APs would have an expiration date of 1 year from the date claimed and the other wireless AP would have an expiration date 5 years from the date it was claimed.



WHAT IS THE VALUE PROPOSITION

For customers who want to manage license expiration dates per location, per business entity, etc. per-device licensing gives them that level of flexibility. They can purchase 3 years for location A in January and 3 years for location B in June. They're able to independently track the expiration dates for each location and bill them accordingly when they are up for renewal.

KEY FEATURES

- **Partial renewals** - Customers can now renew a subset of devices or network independently of one another.
- **License activation window** - Licenses will not start to burn until they are assigned or 90 days after purchase
- **APIs** - Meraki will make APIs available to all customers to support the claim, monitoring and operational workflows as it relates to licensing
- **Move devices & licenses** - Customers can move licenses/devices between their organizations without the need for Meraki support
- **Device shutdowns** - Only devices with expired licenses are shut down, not organizations

WHEN ARE THESE CHANGES HAPPENING?

We are aiming to make per-device licensing available to customers in October. Customers who are interested in the model will have to call into Meraki Support in order for their organization to be converted.

Later in the year (2019), Meraki will allow customers to self opt-into per-device licensing via dashboard.

DO ALL CUSTOMERS HAVE TO USE PER-DEVICE LICENSING?

No. Current customers will have the option to opt-into per-device licensing when it becomes available. New customers will still default to the current co-terminous model when they create a new dashboard organization, but will have the option to move to per-device licensing.

ORDERING INFORMATION

The way orders are placed and claimed in the Meraki dashboard does not change. The customer still places and order for the same SKUs and receive a single Meraki Order # along with a single Meraki License Key. They are then able to claim either the order # or license key into their dashboard organization as they do today.

Customers interested in Umbrella+MR licensing offers must adopt the Per Device Licensing model immediately - they cannot remain or start on a coterminous licensing model. Existing customers can start converting from co-term to per-device licensing as of September 24. New customers will be required to adopt per-device licensing at the time of purchase. However, customers can use the 1-Day/Per-Day license available for the Umbrella SKUs as workaround to still use cotermination. See Umbrella FAQs for more details.

For additional information, please review the Per-Device Licensing FAQ found in the appendix.

Appendix

MS390 Series FAQ

Does my aggregation and core switch need to be Cisco?

Meraki has a rich legacy of simplifying powerful standards-based technologies and making expertise available to everyone. From OSPF to RADIUS, Meraki has always allowed for interoperability and will continue to do so.

Will Perpetual PoE, SecureConnect and other Cat 9300 features be available on this?

Meraki will continue to simplify powerful technology. While we currently only have Perpetual PoE, we will explore the addition of other solutions in the future depending on customer needs. The UADP 2.0 ASIC is at the heart of our MS390 switches supports the development of powerful features that can be deployed seamlessly from the Meraki dashboard.

Can I stack this with other Meraki switches?

MS390 is the most powerful switch in the Meraki portfolio and the only switch that comes with enhanced features like StackPower, StackFailover, Modular uplinks, and the The UADP 2.0 ASIC. Because of this, it can only be stacked with other MS390s.

Can I integrate my existing Catalyst Switching products in the Meraki dashboard, or transition my MS390 to be directly managed as if it were a Catalyst Switch?

The MS390 was designed to address the overwhelming demand from our customers who want to harness the power of the UADP-class ASIC with the simplicity of the Meraki dashboard. MS390 delivers best-in-class advanced security and access policies built on the back of the UADP 2.0 ASIC, and designed to be managed from the dashboard for seamless customer experience. Hence, it would be challenging to directly manage an MS390 directly or to manage the Cisco Catalyst portfolios from the Meraki dashboard.

What features will be included with the MS390?

At launch, the MS390 will include feature parity with the MS350. Additionally, advanced micro-segmentation features will also become available in the future, exclusively on the MS390 since they are the only switch which has innovative Cisco technology inside it.

What hardware-specific features will be available on the MS390?

It will also include a 24-port mGig model, 48-port model with 12mGig ports, 48-port 5G mGig model, 10G and 40G modular uplinks, and 480G stacking.

When will some of the additional advanced technologies be enabled?

Our initial focus is enabling Adaptive Policy - micro-segmentation built upon a base of Security Group Tags - and Meraki SecureConnect. We're excited to hear what customers would find most valuable thereafter and build them into our dashboard.

Will the MS390 advanced policies work with Cisco ISE?

Yes, Cisco Meraki recommends ISE as the RADIUS and identity platform.

I'm familiar with Catalyst technology. How does the MS390 differ?

The MS390 focus is on simplicity. It is managed via the Meraki dashboard, so you will find no console. Just like the rest of our Meraki products, it connects out of the box to the Meraki dashboard, making it easy to become part of your network faster.

For additional information on how the MS390 fits into the rest of the Meraki switch family, please review this Partner Guide or visit the switching page on the Meraki website.

Umbrella + MR License FAQ

Is there a difference in functionality between Meraki Umbrella license and the Meraki and Umbrella API integration?
Yes! The Meraki Umbrella license combines an existing MR software license with Umbrella license functionality.

What are the main differences of the new Meraki single SKU?

1. Pre-defined policies, rather than customizable policies.
2. Blocked DNS events are visible exclusively in the Meraki dashboard since customers will no longer have access to the Umbrella dashboard with this license.
3. The single license SKU is limited to on-network protection.

Note: The manual API integration between Meraki MR and Umbrella works with all Umbrella packages: WLAN, Insights, Professional, and Platform, and provides protection against threats on and off-network. In addition, the API integration enables dual dashboard access, custom policy creation, and full Umbrella reporting. This would require two different licenses like before and is only recommended if the customer wants to build custom policies.

Can I selectively apply Umbrella policies on particular networks?
The pre-defined policies are enabled by default. You can choose to disable them on specific networks.However, applying custom Umbrella policies is not possible with the new license.

What happens when I add a non-Umbrella MR to a network with MRs running the Umbrella license?
If an AP without an Umbrella license is added to a network that has the feature enabled, customers will have 30 days to remove the non-Umbrella AP to stay in compliance.

Do I get access to the Security Center?
Yes! The new license enables access to the Security Center in the Meraki dashboard to view all blocked security events.

Who do I reach out to for support with the new SKU?
All Umbrella and Meraki AP queries under this license will be handled by the Meraki support team.

When is the Meraki Single SKU orderable?
The Meraki Single SKU will be orderable December 2019.

How does co-termination work when I have multiple UMB SKUs or UPGR SKUs?
Umbrella integration with Meraki requires customers to move to Per-Device-Licensing - they cannot remain or start on a co-terminous licensing model If customers want to use this SKU, they have to convert the organization or move the APs to a new organization.

Meraki Per-Device-icensing is available for customers in December 2019. For customers who still want to keep the co-terminous model on the new SKU, refer to the Per-Device-Licensing FAQ found in this appendix.

Is there a license SKU I can buy for my existing APs?
Yes! If you have an existing Meraki AP. You can buy the LIC-MR-UPGR SKU to enable DNS security powered by Umbrella on your network.

Can I leverage manual integration to create group policies?
Yes! If you want to create custom group policies, you will have to manually integrate and also use two different dashboards to create and deploy policies. You will also have to buy two separate licenses

Per-Device Licensing FAQ

How does the Meraki per-device licensing model work?

Meraki devices use the Meraki cloud for centralized management and control. The Meraki cloud is licensed on a "per device, per year" basis. Each device is licensed for a set duration with an expiration date.

Do customers need to have a license for every piece of Meraki hardware?

Yes, every Meraki hardware device requires a cloud license. Meraki hardware without a license won't pass traffic.

When the customer converts to the new model, what changes?

When the customer converts to the new model, their co-termination date will be 'spread' across all the devices in their organization. Nothing will change with their expiration date, but the customer will then be able to manage licenses at the device level. Their expiration date will remain the same until they add more licenses/ devices or renew them.

What about Systems Manager?

Systems Manager will work in a similar way to device licenses. A customer can purchase as many SM seats as they desire and they will assign the SM seats to specific networks. For example, if the customer orders 100 SM seats, they can assign 50 to Network A and 50 to Network B. They can then enroll devices up to the number of seats assigned to the network. They can renew and add seats independently of one another.

How will customers transition to the new model?

When available, customers will have the option within their Meraki dashboard organization to opt-in to the new model.

When a customer is converted to the new licensing model, Meraki will take their current organization's expiration date and apply it across all the devices within the organization. If there are extra licenses, an additional license will be generated with the same expiration date.

Example: If the customer's co-term date for the org is 1/1/2025 and the customer has 1,000 APs (Device count) and 1,100 licenses (License count)... when Meraki performs the conversion, the 1,000 APs will have individual licenses with an expiration date of 1/1/2025 and there will be 100 AP licenses in their license inventory with an expiration date of 1/1/2025 that can be used to apply to devices without licenses (e.g a new device).

Once customers switch to the new model, can they go back?

No. Once a customer transitions to the new model, they will not be able to convert back.

Can a customer move a license between a co-term organization and a per-device (new model) organization?

No, if the customer wishes to move licenses between organizations, they must both be on the new licensing model.

Will customers have time to transition?

Yes. Meraki will not be migrating current customers over to per-device licensing for the foreseeable future (>1 yr). New customers will be on the current coterminous model and have the option to opt-into per-device licensing. Current customers will have the same option to stay on the coterminous model or move to the per-device model.

Per-Device Licensing FAQ

What about new customers?

New customers will still default to the current coterminous licensing model. Like existing customers, they will have the option to opt-into per-device licensing after creating their new dashboard organization.

Do customers need to change the way they order licenses?

No, the ordering process stays the same. When a customer places a license (or license and hardware) order, they will still receive a single order number and license key. When the order or the license key is claimed, individual license ids will be generated that can be assigned to the individual devices.

Are SKUs changing?

SKUs will remain the same. 1-day license SKUs will be the only addition/change in the per-device licensing model.

What are 1-day License SKUs?

For customers who have multiple expiration dates across devices and want to have a single expiration date (preserving co-termination model), they can purchase 1-day license SKUs for their products. If there are two different expiration dates, the license expiration date can only be 'trued-up' to equal to or later than the further expiration date.

Example, if a customer has two devices one with an expiration date of January 1, 2020 and another device with an expiration date of January 31, 2020, the customer can purchase (30) 1-day SKUs and apply it to the first device.

Customers cannot split license time and apply it across multiple devices. For example, if a customer has an additional 1yr license and 12 devices, they can only apply it to a single device. They cannot break it apart and apply 1 month across 12 devices.

Can I have an MX with Advanced Security and an MX with Enterprise in a single organization?

No. An organization has to either consist of all advanced security licenses (MX) or enterprise edition.

What happens when the license runs out?

Customers can purchase a renewal through an authorized Meraki partner. If the device is not renewed, customers will no longer be able to manage the device via the Meraki cloud and the device will cease to function. This only applies to the individual device that has expired.

My customer wants to know more information, who do I reach out to?

If your customer is looking for more information, reach out to your Meraki sales representative.

Will there be more documentation and information?

Yes. Meraki will be providing in-depth documentation, FAQs, and how-to videos upon launch.

Feature and Product Availability

See below for estimated availability dates. Orderability is subject to change or may require special instructions.

MS390 Orderability

December 5, 2019

Worldwide except below regions and countries.

February 2020

Brazil

April 2020

Nigeria

Oman

June 2020

Belarus

Indonesia

Ukraine

Not Launching at this Time

China

MG21-HW-NA and MG21E-HW-NA Orderability (please note: at this time we will only be launching in the countries listed below.)

December 5, 2019

Canada

USA

February 2020

Mexico

April 2020

Argentina

MG21-HW-WW and MG21E-HW-WW Orderability (please note: at this time we will only be launching in the countries and regions listed below.)

December 5, 2019

Australia

Bahrain

Egypt

EU

India

Indonesia

Israel

Japan

Kenya

Malaysia

Taiwan

Saudi Arabia

Singapore

South Korea

Vietnam

February 2020

Hong Kong

New Zealand

Nigeria

Thailand

Uruguay

April 2020

Israel

Oman

Philippines

South Africa

United Arab Emirates

June 2020

Belarus

Morocco

Serbia

Ukraine

Software and Feature General Availability

Already Shipping

Trustworthy Systems

Identity Pre-Shared Key (iPSK)

MR Advanced and Upgrade Licenses*

November 2019

Trusted Access

December 2019

Per-Device Licensing General Availability

Early 2020 - Beta

Adaptive Policy

SecureConnect

Firewall Object Group

The Umbrella + MR Advanced and Upgrade Licenses is currentlty available as early access on Wi-Fi 6 APs and APs running firmware version r26. Please note that these licenses will not be available in Russia or Mainland China.

cisco Meraki