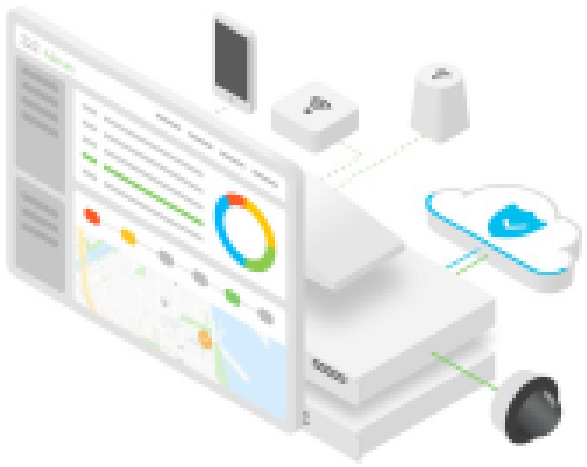
Security Made Simple
Playbook

Table of Contents

General Overview

IT administrators have a difficult job of not only installing networking gear and 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.

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.

(1) Cisco Annual Cyber-security Report 2018
(2) Cisco Annual Cyber-security Report 2018
(3) Cisco Annual Cyber-security Report 2018

Hardware Updates

SECURITY MADE SIMPLE

MS390 Series

OVERVIEW

The MS390 combines the power of Cisco's UADP2.0 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 UADP2.0 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 / 10G / 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.

KEY TAKEAWAYS

The UADP2.0 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.

Software and Feature Updates

SECURITY MADE SIMPLE

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.

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.

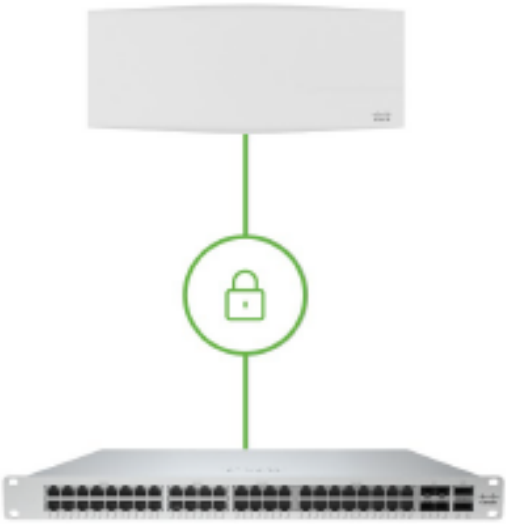
SecureConnect

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 or MS integrations and looking for scalable, automated hardware security are a good fit for this feature.

PRICING

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



SECURITY MADE SIMPLE

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.

KEY TAKEAWAYS

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

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 booth, 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.

KEY TAKEAWAYS

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

SECURITY MADE SIMPLE

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 phishing, powered by Umbrella on their Meraki network.

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.

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.

KEY TAKEAWAYS

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

SECURITY MADE SIMPLE

Identity Pre-Shared Key (iPSK)

OVERVIEW

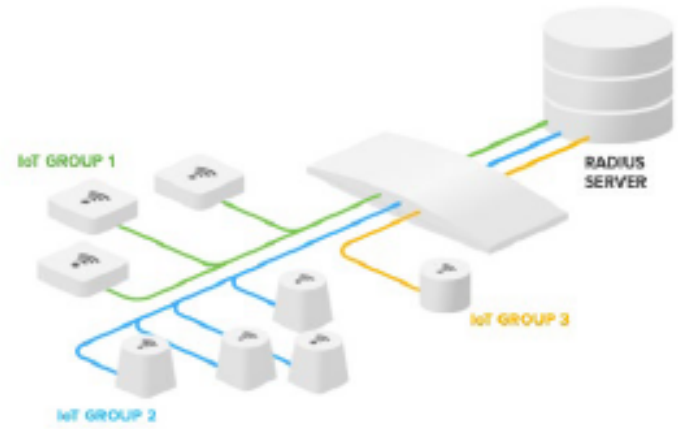
With IoT devices proliferating, network admins are dealing with an exponential increase in the number of devices connecting to wireless networks. Not all of these devices support 802.1X authentication, which makes authentication difficult. WPA-PSK is used today, but can result in the possibility of a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

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.

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.



SECURITY MADE SIMPLE

Firewall Object Groups

OVERVIEW

Firewall Object Groups allow network entitles 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.

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.

TO WATCH CISCO MERAKI'S
SECURITY MADE SIMPLE WEBINAR

CLICK HERE