Meraki

SOLUTION OVERVIEW

A Scalable Approach to Network Security and Microsegmentation

An overview of Cisco Meraki Adaptive Policy

Table of contents

Make your network and security work together 3

Adaptive Policy: Intelligent, intent-based security and network segmentation at scale 7

How does Adaptive Policy work? 10

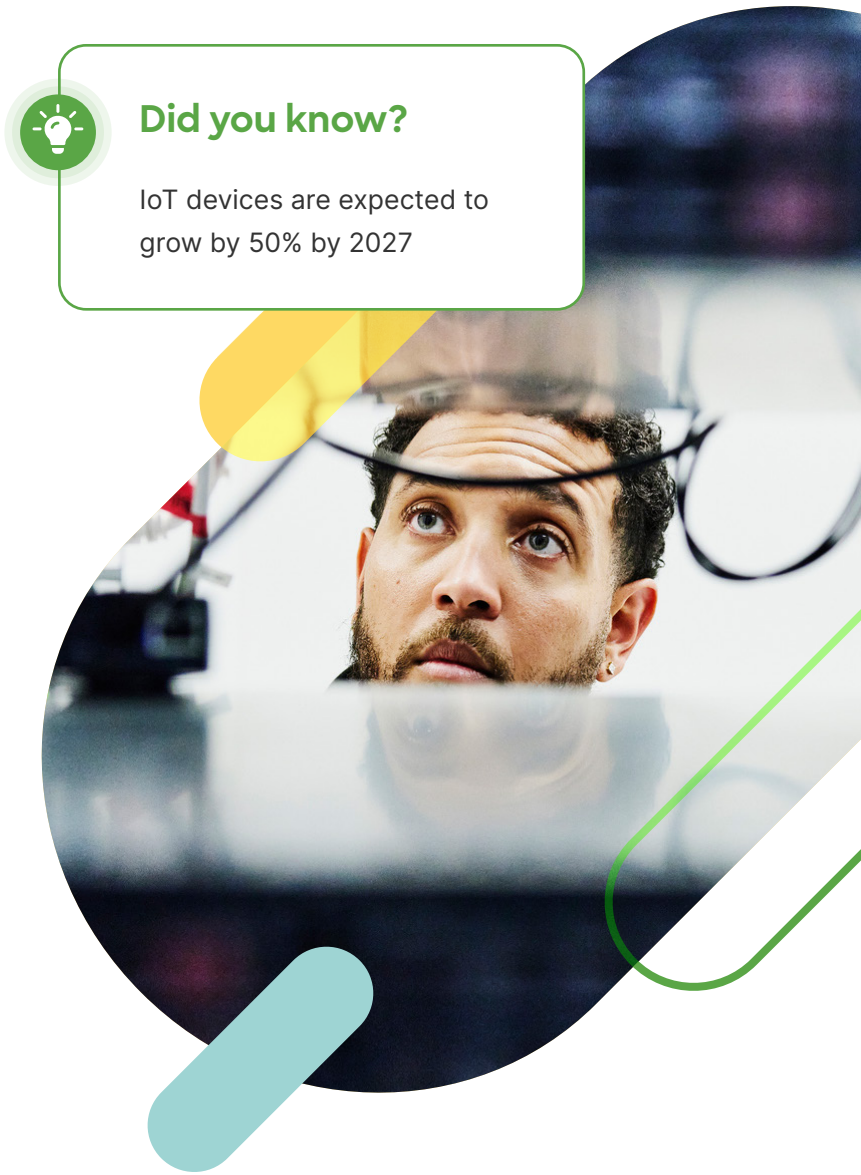
OT simple zone and conduit policy enforcement through SGTs 13

Streamline security operations and realize business outcomes from day one 18

Summary: Building a foundation for NetSecOps partnerships 21

Make your network and security work together

The network is the backbone of enterprise productivity in today's interconnected world. It's also the most vulnerable point of entry for cyberthreats. The surge of intelligent, data-generating devices—from smart cameras to IoT sensors—will revolutionize productivity and user experiences. At the same time, it raises significant challenges to network performance, security policy, and the teams who manage and maintain network integrity. **This duality between smart devices and the resources to make them work is our new reality.**



Did you know?

IoT devices are expected to grow by 50% by 2027

As the sheer number of devices, applications, users, and locations grows, your network complexity grows along with it. The problem? Traditional VLAN-based security policy approaches aren't up to the job. They lack context and introduce skill gaps and challenges that disrupt your IT and security teams' ability to keep things moving across your distributed sites. While zero-trust network access (ZTNA) is effective in giving the right users private app access without placing them on the network, it may not work for all scenarios. For example, ZTNA will not be a good fit on a campus with operational technology (OT) devices that are unable to implement ZTNA connectors and outdated vendor-managed Windows 7 devices that lack support for the essential single sign-on (SSO) protocols that are required for ZTNA integration.

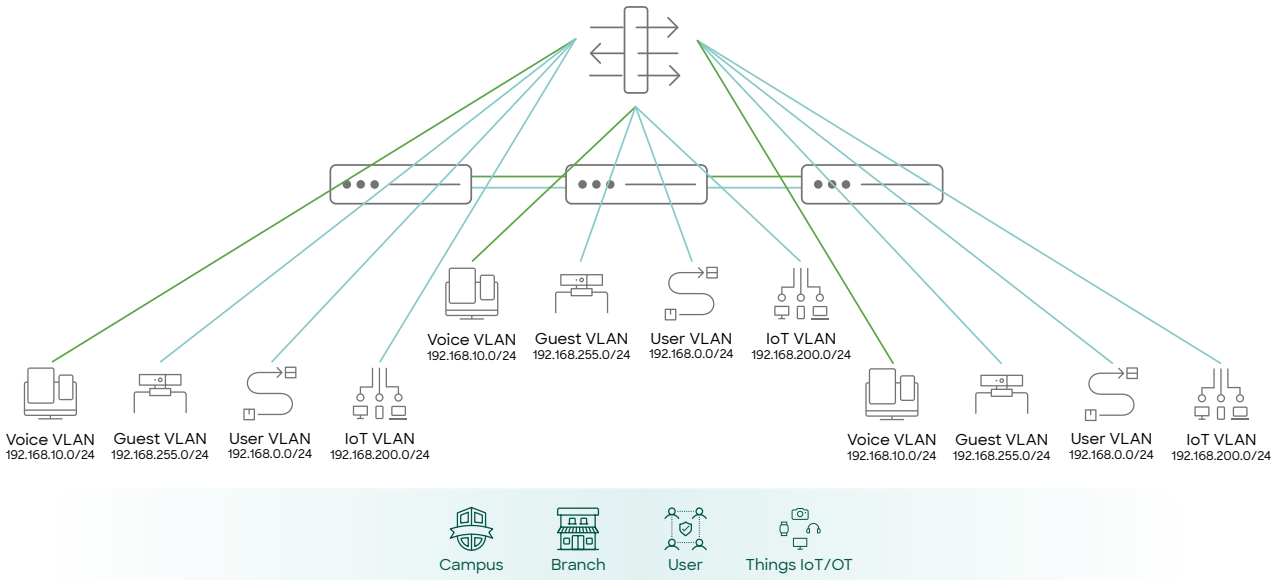


Figure 1: Example of VLAN policies in one location.

Within this **complexity**, security leaders wrestle with critical questions:

- **Scale:** How do I minimize and monitor exposure at scale in my organization?
- **Clarity:** How do I monitor and make sure security policy is up-to-date and create easy-to-read policies with context and business intent that covers who, what, and when?
- **Control:** How do I prevent the propagation of ransomware across my network?
- **Compliance:** How do I maintain compliance and pass security audits?

These challenges multiply exponentially as more sites are introduced. Organizations need a solution that both strengthens security and simplifies network access policy management at scale. Cloud-managed switches are integral to connectivity—which means they play a vital role in boosting network performance and implementing a zero-trust framework at scale.

“Mean Time to Enforcement” (MTTE)

Is the mean time it takes for an identity system to learn the identity of the endpoint and convey that identity to the enforcement point. This can range from single seconds to tens of seconds normally. The way the systems convey the identity to the enforcement point is called a control plane.

Adaptive Policy: Intelligent, intent-based security and network segmentation at scale

With Cisco Meraki, you and your team get a centralized experience for managing end-to-end networks across wired and wireless, security, and IoT. This powerful platform provides the flexibility and scalability to grow alongside your business effortlessly.

You’ll work alongside our Meraki pioneers, who are consistently breaking new ground and leading the way in cloud-managed networks.

Unlock the speed and depth of telemetry and application visibility for faster mean time to detection (MTTD) and faster mean time to resolution (MTTR). Your network team can make configuration changes in one place and push to selected locations, which means no more manual processes and no room for potential human errors.

You can manage and enforce security policies at scale with the intuitive, scalable Meraki dashboard without the traditional control planes method for boosted operational efficiency and effectiveness with faster mean time to enforcement (MTTE) across all your locations.

Boost uptime and productivity at cloud scale

By dynamically segmenting your network based on “who” is using it (identity), the “why,” and “how” they’re using it (context), Adaptive Policy allows you to secure the right access to your network resources. That’s where Meraki cloud microsegmentation shines.

Gone are the days of manually managing thousands of static IP access control lists (ACLs) that would force you to re-architect the network infrastructure every time you change your policies.

Shared context provides the same policy for wired and wireless access (supported across MX security appliances/MR access points/MS switches). It automatically and dynamically applies the appropriate IP agnostic[1] policies to users and devices to bolster your security.

[1] IP agnostic policies refer to security policies that will be created and enforced more effectively and flexibly regardless of IP addresses.

Security segmentation with Adaptive Policy

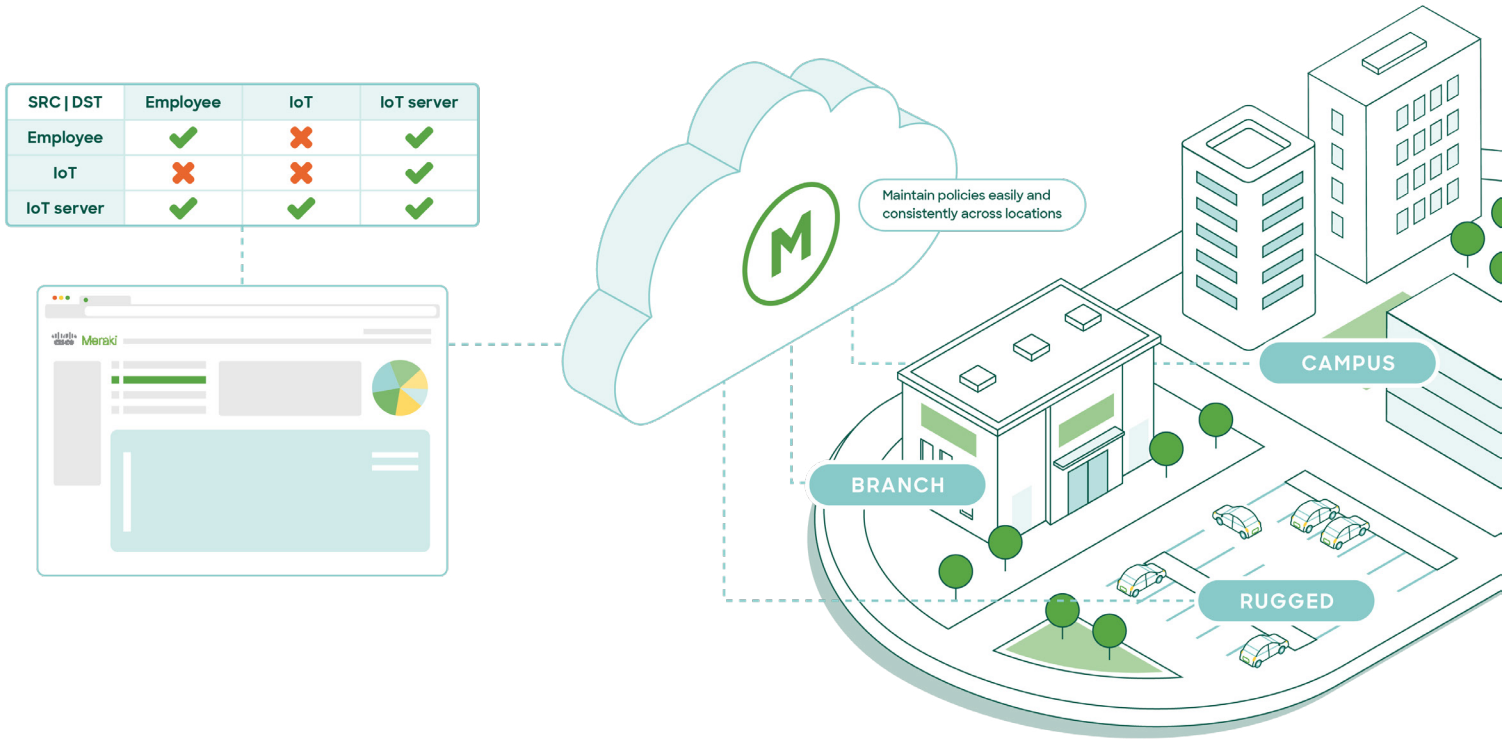


Figure 2. Consistent policy across networks.

Cloud-managed microsegmentation is less error prone, eases SecOps effort, and cuts down on costs.

Policy and groups are configured in the dashboard and pushed to Adaptive Policy nodes like any other Meraki configuration change, making this approach scalable and effective.

How does Adaptive Policy work?

Network segmentation is essential to keeping critical business assets safe, but traditional segmentation approaches are complex and can be difficult to gracefully introduce to existing environments. You need a new approach to balance agility and security.

With Adaptive Policy, controls are simply defined with endpoint roles, not IP addresses. By classifying systems using human-friendly logical groups denoted by Security Group Tags (SGTs), security policies can be defined using the identity of the user or device. They are also more flexible and simpler to manage than using IP address-based controls.

IP addresses don't tell you the role of a system, the type of application a server hosts, the purpose of an IoT device, or the threat-state of a system. SGTs can denote any of these.

SGTs can also simplify rules in security applications, along with access control lists used across wired and wireless networks.

In addition, SGT capabilities have been published through the IETF and are now used by a variety of networking and security vendors. This allows for interoperability with existing security applications from a non-Cisco vendor without rearchitecting the policies.

This brings us to the most significant benefit of using SGTs: microsegmentation. The topology-independent nature of SGTs means teams can implement and change microsegmentation patterns—without the work of reconfiguring network devices or redesigning the network. As SGTs work independently of IP address space, VLANs, and VRFs, they can be used anywhere on the network, so you can decouple the segmentation policies from the underlying network infrastructure.

This approach is much easier to set up and manage than VLAN-based segmentation. It also avoids the processing impact associated with IP ACLs on network devices. When used in Cisco cloud-managed Catalyst switches and MS130 switches,[2] SGT-based policies operate at wire-rate, so segmentation policies can be applied without impacting network performance or availability. These policies also let you restrict lateral movement—something traditional segmentation methods like IP ACLs, VLANs, and VRFs cannot do.

Using Adaptive Policy with Security Group Tags simplifies network segmentation and boosts security without sacrificing agility or flexibility.

[2] Adaptive Policy supports on MS130 mGig models and MS130R

OT simple zone and conduit policy enforcement through SGTs

Over the last decade, more and more devices that historically operated in closed-loop systems (operational technology) have moved into the IT space. Doing so makes real-time delivery of data from the OT edge to the IT space possible, which enables rapid just-in-time (JIT) manufacturing and lower maintenance costs.

What were once low-level protocols for system communications in OT environments have converged into protocols within the networking realm, which made rapid deployment and centralization of control, monitoring, and analysis of those systems possible. Securing both OT environments and the networks they traverse has become paramount to keeping critical business applications and infrastructure protected.

Security concepts in OT networks use the terminology of “zones” and “conduits.” Essentially, a zone is an SGT or group of devices that have the same security policy, while conduits are communications between zones that can be associated to a policy between groups.

Getting started, the process can be broken down into four steps:

- **Take an inventory:** Know which assets are in your environment.
- **Define the zones:** These are assets in the topology that would leverage the same policy and communications.
- **Define the conduits:** Conduits are the communication requirements between zones, like telemetry streaming to a centralized analysis engine or even communication between OT devices in different zones.
- **Map the zones:** Zones go into unique Adaptive Policy Groups (SGTs) and conduits to policies between groups.

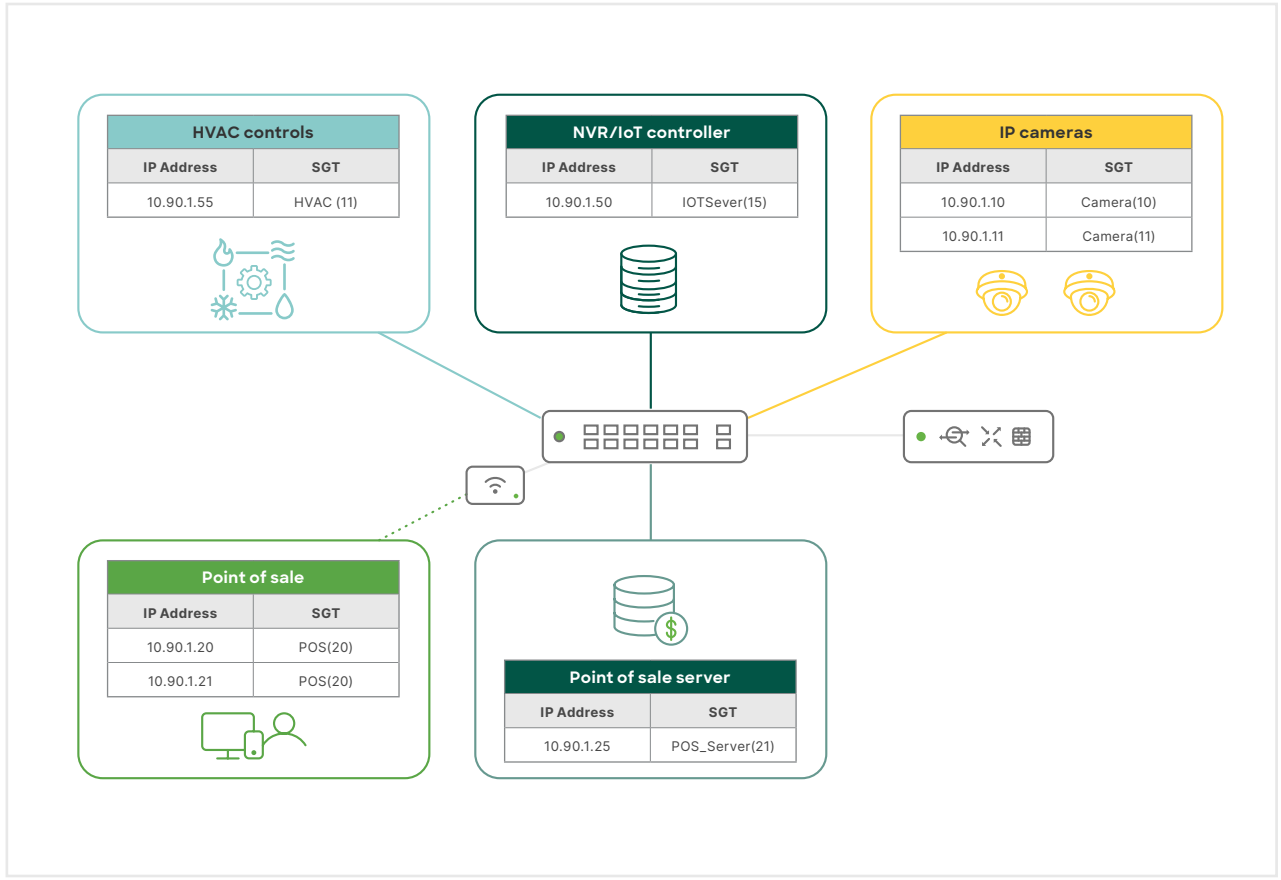


Figure 3. An example topology containing different devices, from environmental (HVAC), building security and IOT, and PCI. The endpoints are divided into groups that share the same policy and communication requirements.

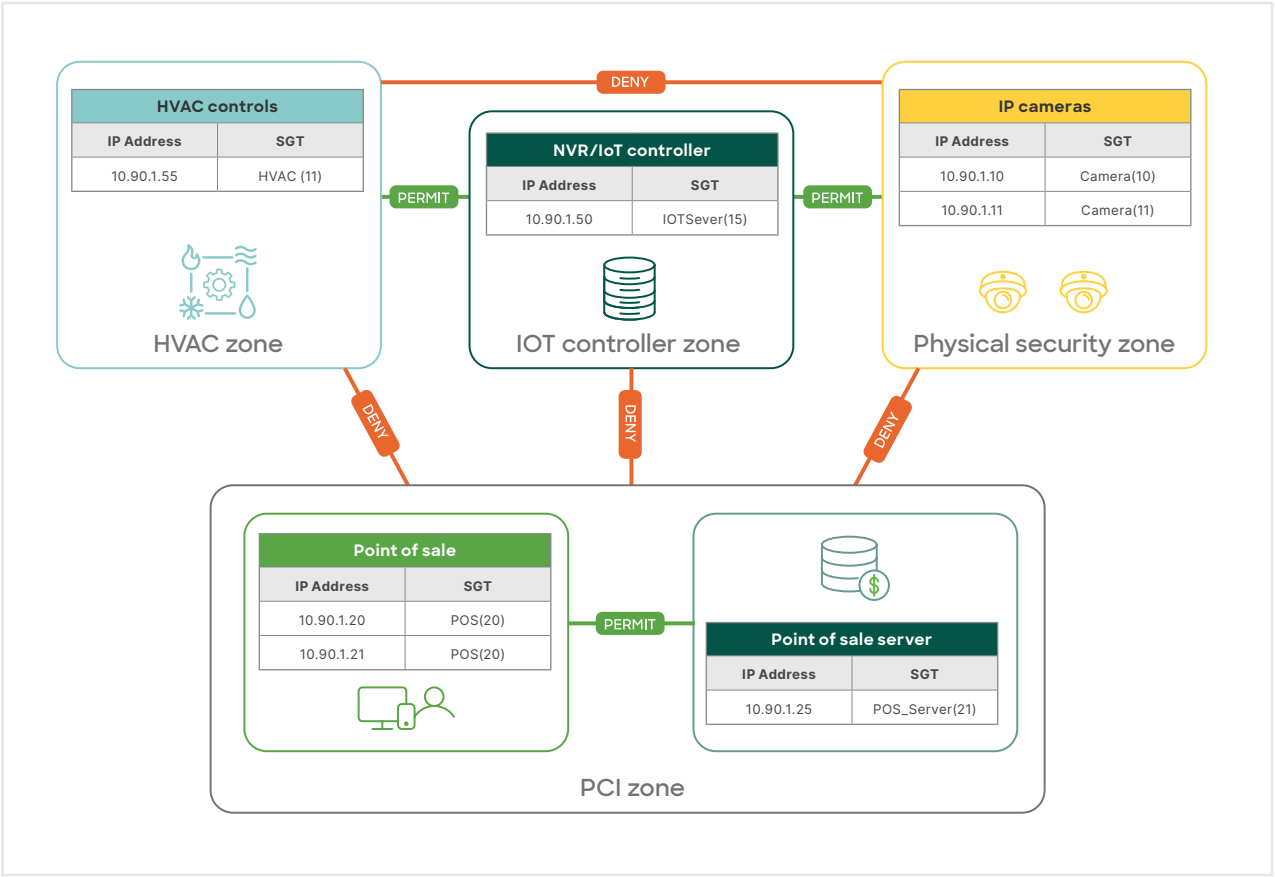


Figure 4. Group the different zones (SGTs) and then map their communication needs. You can do this in either a simple (permit/deny) or more complex way using custom policies to limit communication down to specific protocols between groups.

Source/ Destination	POS (20)	Camera (10)	POS_Server (21)	IOT_Server (15)	HVAC (11)
POS (20)	Deny	Deny	Permit	Deny	Deny
Camera (10)	Deny	Deny	Deny	Permit	Deny
POS_Server (21)	Permit	Deny	Permit https	Deny	Deny
IOT_Server (15)	Deny	Permit	Deny	Permit https	Permit https
HVAC (11)	Deny	Deny	Deny	Permit	Permit

Figure 5. The policy in this case can be quite simple, restricting communication only to specific groups.

Streamline security operations and realize business outcomes from day one

With Adaptive Policy, you can reduce your attack surface, protect your system against cyberthreats, and stop unauthorized access. Your Meraki cloud dashboard tracks policy enforcement and logs with precision, making it easy to chart policy accuracy for adjustment and streamline compliance management.

True zero-touch provisioning also lets you set up devices and security policies remotely so connected devices are fully compliant. You can avoid potential human error, speed up the scaling process, and be confident that security policies are consistently applied across devices from the moment they connect to the network—with or without dedicated on-site IT teams.

Getting the entire end-to-end network and security policy on one single dashboard means you get:

FASTER TIME TO DEPLOY

Traditional VLAN-based security policy may take months to deploy. With Adaptive Policy, security policy can be created and deployed on a new site in days. By skipping complex manual configuration, you can deploy consistent security measures at scale, rapidly onboard new devices and users, and minimize potential downtime.

LOWER COST OF MAINTENANCE

Get rid of manual adjustments for each device by using group-base policies and automatic updates. Plus, cut down on the operational costs associated with traditional security policy upkeep and get an always-on, robust, and dynamic security posture that evolves as you need it to.

FASTER TIME-TO-RESOLUTION

Make connections between insights faster so your IT teams can quickly identify and troubleshoot security issues with end-to-end network telemetries and visibility in one place. Limit lateral movement and effectively restrict malware propagation simply by applying least-privilege policies across campus and branch networks, even within groups of similar endpoints.

EASILY MEET COMPLIANCE AND AUDIT REQUIREMENTS

Adaptive Policy makes compliance simple by giving you the tools to segment networks and monitor traffic, making it easier to demonstrate that the network is secure and policies are being enforced. Built-in tools like Policy Hit Counter help you visualize the policy matrix and makes fine-tuning policy a breeze.

FASTER TIME TO ENFORCEMENT

In-line tagging allows security policy to be enforced more effectively and accurately compared to a traditional identity firewall with control planes method, since the identity is conveyed with the frame or packet. It simplifies policy sets by removing the need for IPs and rule changes when the host changes.

These benefits ultimately mean a better and safer user experience and a more productive network and security team.

Summary: Building a foundation for NetSecOps partnerships

Adaptive Policy creates a collaborative environment where security and network operations teams have a common framework and a set of tools for managing network policies. It aligns team goals, simplifies communication, and uses a more proactive and agile approach to deploying and maintaining an efficient and effective network and security management.

Meraki

Continuous network performance and network integrity start here

Learn more

For hardware and software requirements, please see details on the Adaptive Policy Overview documentation.