Cisco SASE with Meraki:

Get in the Fast Lane to SASE

Beyond the Quaint: Complexity of a Distributed Environment

The notion of users solely or primarily working from an office, accessing applications in the organization's data center, is almost quaint. While it remains a slice of reality, it's typically a small slice. Today, users work from anywhere – at home, in the field, from a coffee shop, on an airplane, or from a little league game. They need to secure access to applications and resources virtually everywhere.

The Challenge: Securing the Distributed Enterprise with Lean IT

As users, data, and applications become ever more distributed and varied, IT and security teams face mounting challenges. High numbers of poorly integrated security tools, the resulting security gaps, and the difficulty of scaling networks for evolving workloads create a heavy burden. Additionally, as organizations move from generative AI experimentation to agentic AI execution, the challenge morphs from asking AI questions to trusting AI to autonomously act. For lean, resource-constrained IT teams, the burden is even higher. Managing complexity, while supporting hybrid work and accelerating demands of AI, is a daunting task.

You need to efficiently enforce security for all users, devices, and agents—from any location—who access private resources (in on-premises data centers and the cloud), SaaS applications, AI platforms/tools, and the open internet. Your IT team, highly skilled yet stretched thin, requires a streamlined approach. You need a unified platform for networking and security that delivers deep protection without disrupting your lean IT model, reducing user productivity, or increasing the risk of a breach. You need to keep it uncomplicated.

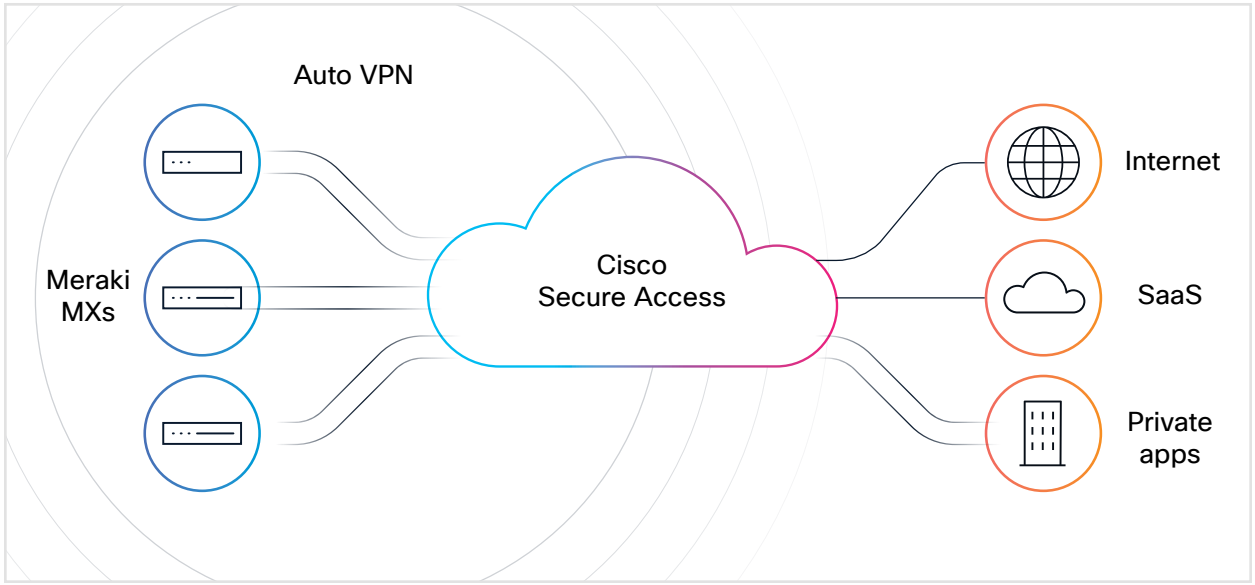
The Solution: Networking and Security Together

Get in the fast lane to SASE. Cisco Secure Access Service Edge (SASE) with Meraki provides a simple, elegant solution for securing access across your hybrid workforce. By automating the connection of your Meraki SD-WAN to Cisco Secure Access, a full Security Service Edge (SSE) solution, you can effortlessly upgrade your organization to a SASE architecture that delivers robust security across your highly distributed environment.

Using a straightforward, cloud-delivered approach with industry-leading automation, Cisco SASE with Meraki provides efficient, resilient, and secure traffic routing directly from the familiar Meraki dashboard to Secure Access. For traffic that you choose to protect with Secure Access, you can gain the multi-layered, deep security of a full SSE solution to dramatically increase security protection and lower risk to your organization.

Key Benefits and Capabilities

- **Simplified Onboarding (Up to 15X Faster):** Easily connect Meraki organizations to Secure Access via the Meraki Integrations page and stay securely connected with automated API key management. Leverage Meraki Auto VPN to automatically establish secure primary and secondary tunnels between your MX sites and Cisco Secure Access, driving up to 15X* faster deployment than manual tunnel creation. Then iteratively add increased security protections, at your pace and according to your organization's priorities, via Secure Access.
- **Advanced Security & Proactive Protection**: The addition of Secure Access to your Meraki SD-WAN environment expands and deepens security protections for SaaS and internet access, private applications access, and remote access. Advanced security is baked-in – including Zero Trust Network Access (ZTNA) for granular control of remote user access, Cisco-unique protection for AI use and AI agents, infusion of rich identity data to sharpen access decisions, and data loss prevention (DLP) to prevent data exfiltration. These protections, plus many more, combine to radically reduce risk.



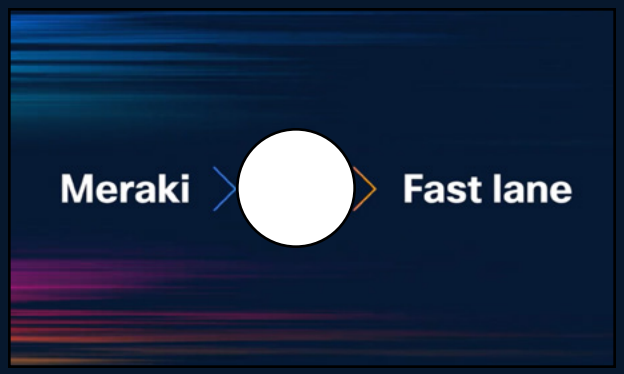
- **Automated Failover & Built-in Resiliency:** Replace manual discovery, investigation, and tunnel reconfiguration with automatic "no-touch" failover. Each enrolled Meraki SD-WAN appliance establishes multiple Auto VPN tunnels across available uplinks to two data centers, driving accelerated recovery from a down tunnel.
- **Flexible Cloud Connectivity:** Meraki spokes can establish new Auto VPN tunnels to Secure Access while seamlessly maintaining existing MX Hub tunnels and connectivity, ensuring zero disruption to your current routing architecture.
- **End-to-End Visibility:** Monitor WAN, cloud, and edge environments for complete insight and control, providing significant reduction in detection and investigation time.

By jumping in the fast lane to SASE and converging your Meraki MX with Cisco Secure Access, you gain advanced security, deeper visibility, and more granular control across all locations and users—lowering your costs and administrative overhead.

*Backed by internal testing of realistic before and after scenarios.

Take the Next Step

Experience the fast, simple, secure, and resilient way to protect your organization.



Watch the video