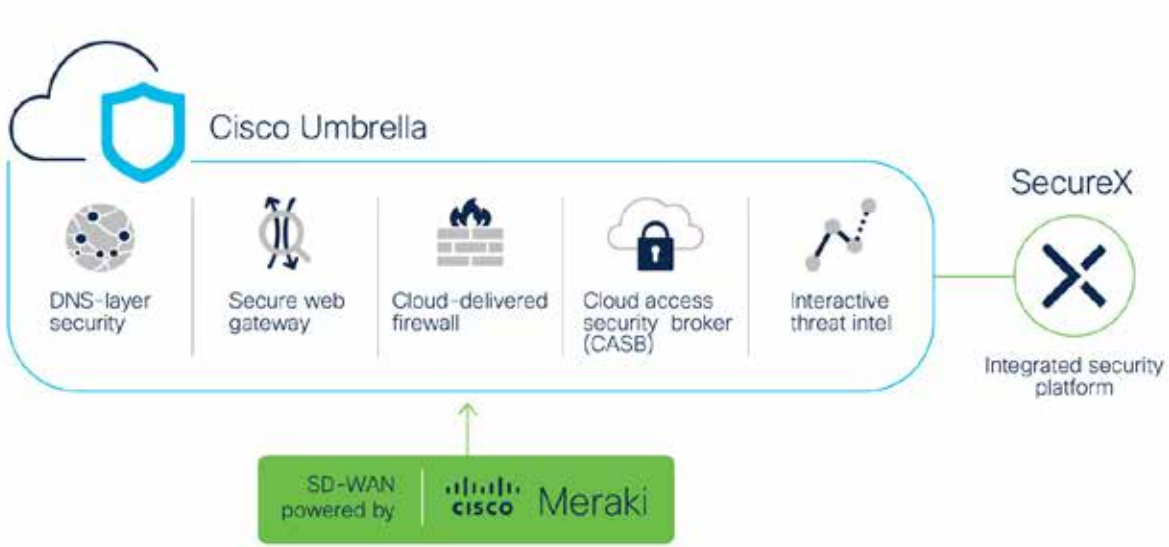
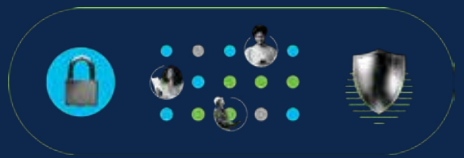
Meraki MX and Cisco Umbrella integration offers simple, flexible deployment

Are you an existing Meraki MX customer? Or are you considering Meraki MX for your on-premise security and SD-WAN needs? If so, you should explore Umbrella's leading cloud-native security. Meraki MX and Umbrella integration provides an effortless start to your Secure Access Service Edge (SASE) journey. With simplified IPsec tunnel connectivity, you'll get fast deployment of Umbrella across your distributed locations. Streamlined network configuration and security enforcement make it easy to secure cloud access and protect users against internet threats on- or off- network.





What is SASE?

Gartner coined the term Secure Access Service Edge (SASE) to describe combining comprehensive WAN capabilities with comprehensive network security functions to support the dynamic secure access needs of digital enterprises. Cisco's approach to SASE combines leading security and SD-WAN functionality to help secure access wherever users and applications reside.

Unified security with flexible enforcement

Umbrella unifies DNS-layer security, secure web gateway, cloud access security broker and application-aware firewall functionality to simplify management and improve security efficacy. With flexible policies, you can support use cases, ranging from basic DNS-layer protection to advanced web and application inspection to make sure your business is safe.

The Cisco Umbrella global cloud architecture delivers network resiliency and reliability to keep your performance fast, and your connections secure. Automatic failover ensures high availability to give your users the secure,seamless experience they expect.

By deploying Umbrella across your Meraki MX devices, you'll get the simple and scalable security you need to make sure your SASE journey is a success. Here are just a few of the benefits:

Simple

- Fast protection of users across your distributed network with simple, flexible deployment options
- Higher security efficacy with less effort and less resources

Secure

- Multiple layers of security from a single, cloud-native service
- Flexible policy enforcement for any use case
- Off-network protection using Umbrella without a VPN
- Continuous protection with automatic failover

Scalable

- Consistent high-performance security for multi-cloud demands
- SSL decryption at scale not possible with on-premise hardware

Integration Features

Capability description	Why it matters
Meraki MX enabled devices using Umbrella device integration will automatically redirect DNS traffic to Umbrella resolvers with a single configuration change.	Ensures all devices in branch office locations are protected by Umbrella. Makes it easy to deploy Umbrella policies across many devices without leaving the Meraki dashboard.
Appends EDNS (Device ID and Client IP) to the DNS packet	Encrypts all DNS traffic and adds attribution down to the internal IP (client)
Supports split DNS to exclude internal DNS requests from being sent to Umbrella resolvers	Allows users to reach your local network's local resources (computers, servers, printers, etc.) on internally hosted domains that rely on local DNS servers
Supports DNSCrypt proxy to encrypt DNS traffic	Secures DNS traffic from eavesdropping and man-in-the-middle attacks
Allows traffic forwarding to Umbrella using IPSec tunnels for cloud-delivered firewall and secure web gateway inspection	Provides additional security controls and granularity to protect users with direct internet access
Offers traffic exclusion (VLANs/subnets)	Enables basic traffic controls by IP address or interface

Take a test drive

To try Umbrella, visit signup.umbrella.com and sign up for a free 14-day trial in minutes with no credit card or phone call required.

Connection® PUBLIC SECTOR SOLUTIONS
we solve IT®

For more information about Umbrella or how to start a free 21-day Umbrella trial, contact an Account Manager today.

1.800.800.0019 ■ www.connection.com/cisco-ps