Mako Networks/Meraki Comparison

Mako Networks and Meraki share many similarities but target different verticals and have key variances that matter for their respective markets.

Mako Networks solutions are targeted at distributed enterprises with features and functions designed specifically to deliver benefits across multi-thousand site estates including those that are supported by MNSPs and/or franchised and thus more complicated in structure.

Meraki has traditionally focused its technology on campus deployments and has expanded to the lower end of Cisco's traditional enterprise market. Mako Networks on the other hand has always addressed the challenges of distributed enterprise security, connectivity, and business continuity.

Both technologies have their own hardware devices that are cloud managed. The Mako Central Management System (CMS) is designed to be fully utilized by distributed retail enterprises and franchise groups where different levels of access to retailer LANs and WANs are required. The CMS simplifies deploying and managing large numbers of customer sites consistently and securely, with features including Enterprise Templates and cascading security profiles, which allow for role-based, nested security access across multiple entities. Meraki's cloud management is designed to be used by core IT personnel and offers significantly less flexibility in access levels and template-based security. Mako also offers PCI-certified templates, reviewed by a QSA to assist merchants in meeting PCI obligations in a streamlined and highly effective way.

Mako technology was designed from inception around network security across any available broadband, (including cellular) and was created to support thousands of remote locations for thousands of unique customers. Meraki technology was built primarily to deploy and manage campus environments, supporting large numbers of devices at a single site.

Meraki is owned by Cisco and by association gains access to many opportunities a smaller independent business like Mako does not. However, Mako is highly agile and development cycles can be dynamic, even to the point of being reactive to specific customer and partner requirements.

Mako devices have specific variants designed for the market being served, whether that be for US or other global markets. For example, xDSL using customer-supplied equipment is prevalent in the UK and Europe but not the US. Meraki delivers a single US-centric solution internationally. Mako is headquartered in the US but was founded in New Zealand and has significant international experience.

Mako technology has always been successfully sold to the world's largest distributed enterprises whereas Meraki technology has traditionally been sold to SMBs and large campus locations - it has struggled to win large, distributed enterprises. Designed specifically for the distributed enterprise and franchise type organizations, Mako's pricing structure carries a strategic advantage along with the targeted feature set.

FEATURE/FUNCTION	MAKO	MERAKI
Target Market	Distributed enterprise with a strong focus on the distributed retail enterprise. Mako's DNA is distributed networking security.	Campus/enterprise with a strong focus on larger footprint environments requiring many switches and access points. Secondary focus is SMB. Meraki's DNA is distributed wireless access points.
Role-Aware Cloud Management	Yes. Mako CMS is designed to be accessed by users throughout the distributed enterprise and incorporates role-based user control to ensure users only get access to the Mako devices and functionality they need.	No. Meraki cloud management is an all-or-nothing service which usually means only a limited number of IT personnel have access. This model limits the value proposition of cloud management in larger organizations.
No Localized Management	Yes. Mako devices may only be configured via the Mako CMS. This architecture is a key reason why the Mako System carries a PCI DSS certification. Mako devices do not have default user names or passwords.	No. Meraki devices can be configured locally as well as via the cloud. This capability requires additional physical security to be implemented to ensure devices cannot be manipulated by bad actors.
No Reset Button	Yes. Mako Security Gateways do not have a reset button. This enhances physical security and ensures configuration cannot be removed should a bad actor have physical access to the device. Mako devices are "reset" via the CMS which requires an appropriate level of MFA-controlled access.	No. Meraki devices have a local reset button requiring additional physical security to be implemented to ensure devices cannot be manipulated by bad actors.
PCI DSS Certification	Yes. The entire Mako System carries a PCI DSS Service Provider certification. This certification makes it easier for a distributed enterprise to meet many of their PCI obligations (and for a Mako partner to deliver such services).	No. Meraki does not have a PCI DSS certification. Like many networking solutions, Meraki technology can be made PCI compliant by configuring (and maintaining) devices appropriately, placing significant burden of risk on Meraki partners and end clients.
Enterprise Configuration Templating	Yes. Mako functionality includes the ability to create layered configuration and security templates to enable fast and consistent configuration across large deployments. Mako ETs may be used to restrict CMS configuration access to the templated content from users below the template owner (e.g., a retail brand may use a Mako ET to ensure their branded retail locations' POS environments cannot be overridden by their dealers).	No. Meraki has very limited templating capability compared to Mako. Meraki's architecture does not support role-based access throughout a distributed organization to the same extent that Mako's does.

FEATURE/FUNCTION	MAKO	MERAKI
Extensive Diagnostic Toolset	Yes. Mako CMS delivers a wide range of diagnostic tools to assist help desk and technical personnel troubleshoot all aspects of Mako devices and WAN connectivity. Users cannot remotely access a Mako device. Diagnostics are run via the CMS which reaches out to a Mako devices and presents the diagnostic result to the user in their web browser.	No. Meraki diagnostics are very limited and proper troubleshooting usually requires SSH access to the device. This type of access reduces the security of the device and makes troubleshooting more difficult and cumbersome.
Cloud Management	Yes, with complete control over all aspects of a Mako device.	Yes, but some configuration changes can only be completed by Meraki support personnel.
Integrated Cellular	Yes, most Mako Security Gateways feature built-in commercial grade cellular modules with extensive diagnostics.	Yes, although most Meraki security gateways utilize consumer-grade USB cell modules with basic diagnostics. Some Meraki devices have built-in cellular modules but their control and diagnostic capability is not as strong as Mako's offerings.
Hardware Devices Supported	Security Gateways, Managed Switches, APs, VPN Concentrators	Security Gateways, Managed Switches, APs, VPN Concentrators, Cameras, Sensors
SD-WAN/VPN	VPN Cloud delivers multiple levels of redundancy and resiliency including geographic, device and circuit. Mako also supports zero-packet loss VPNs for uninterruptable VoIP call.	Traditional VPN options with routing protocol support. Meraki can be slow to implement changes, i.e., IKEv2 just entered release candidate stage although IKEv1 is deprecated and shouldn't be used.
Unrestricted WAN Speed	Yes. All Mako devices will take full advantage of the interface's capabilities.	No. Meraki often artificially limits the WAN speed of their devices (such as the MX range).
Licensing	Simple, delivers most functions as standard. Pricing is in the medium range for the target market.	Complex and difficult to understand. Pricing is in the high range for the target market.
Security	Next-generation stateful-inspection firewall with IDS/IPS capability. Mako's approach of no local configuration and no reset button adds significant physical security.	Next-generation stateful-inspection firewall with IDS/IPS capability.
Deployment	Tools for large scale deployment included. Multi-thousand site deployments common.	No specific toolset for very large deployments.