

# Meraki Cloud Controller Data Centers

## Datasheet



## Robust, scalable, and highly available infrastructure

Meraki's customers build their networking infrastructure on top of Meraki, so availability, disaster recovery, and security are crucial. We built the entire Meraki solution with these requirements in mind, so that a Meraki based network is more reliable than any alternative on the market.

## Features

### Redundant Architecture

Meraki's Cloud Controller runs out of five geographically distributed co-location facilities across the U.S. and Europe. All customer configuration data and statistics are securely mirrored across three data centers for multi-layered redundancy.

### High Availability

The Meraki system treats component failures such as disk, server, or switch failures as routine. Automated failure detection, redundant alert systems and rapid failover mechanisms ensure that Cloud Controller availability is maximized even in the event of hardware failure. Network management access will be restored in minutes.

### Disaster Tolerant

Each top-tier co-location facility is equipped to minimize the possibility of failures. Each data center features diesel generators for backup power, redundant high speed carrier connections, and seismic reinforcement. In the event of a catastrophic data center failure, such as a major earthquake, your Meraki networks will fail over to one of our mirrored sites. This failover will happen automatically, without intervention on your part and with minimal to no disruption to clients on your network.

### Connectivity Failure Resistant

Connectivity failures can be caused by Internet routing problems, e.g., a carrier disruption between your network and Meraki. Meraki networks are designed to tolerate internet connectivity failures gracefully. Your network will continue to provide service to associated clients. However, some features such as hosted splash pages, network channel optimization, real time statistics as well as the ability for administrators to make configuration changes to the network will not be available until connectivity is restored.

### Incredibly Secure

Traffic from client devices associated to a Meraki network is routed directly to its end point, and does not pass through Meraki data centers. Information about your network, such as user passwords, pass keys, and credit card numbers, is secured both in flight and at rest. All communication between the data center and each Meraki access point takes place over a secure SSL tunnel. Sensitive data is only stored in an encrypted format. Automated intrusion detection, firewall protection and stringent remote access restrictions ensure that only authorized Meraki personnel have remote access to the Cloud Controller. Multiple layers of physical security, including biometric readers, are present.

# Specifications

---

## › Availability Monitoring

- 99.99% uptime
  - 24x7 automated failure detection (all servers tested every five minutes from multiple locations)
  - Rapid escalation procedures across multiple operations teams
  - Triple-redundant, independent alert systems in case of outage
- 

## › Redundancy

- Five geographically dispersed data centers
  - Network configuration and statistics data replicated across three independent data centers
  - Hot spare data current within 60 seconds
  - Nightly archival back-up
- 

## › Interruption Recovery

- Rapid failover to hot spare in event of hardware failure
  - No end user impact unless using Meraki-hosted splash (configurable splash bypass for guest and public networks)
  - Distributed architecture means that a hardware failure event affects only a small percentage of customer networks
  - Weekly failover procedure drills
- 

## › Cloud Controller Security

- 24x7 automated intrusion detection
  - IP and port-based firewall protection
  - Restricted remote access by IP address, verified by public key (RSA)
  - No password-based access
  - Automated administrator alerts for configuration changes
- 

## › Out-of-Band Architecture

- Storage of network configuration data and statistics only
  - End user data does not traverse through data center
  - All sensitive data (e.g. passwords) stored in encrypted format
- 

## › Physical Security

- Security guards monitor all traffic into and out of the data center 24/7, ensuring that entry processes are followed
  - A high security card key system is utilized to control facility access
  - Digital video surveillance of all entries, exits, and cabinets is conducted
  - Biometric readers
- 

## › Disaster Preparedness

- Sophisticated sprinkler system with interlocks to prevent accidental water discharge is provided
  - Diesel generators provide backup power in the event of power loss
  - UPS systems condition power and ensure orderly shutdown in the event all power is lost
  - Each data center has service from at least two top-tier carriers
  - Seismic bracing is provided for the raised floor, cabinets, and support systems
  - Data center failover is provided in the event of catastrophic failure
- 

## › Environmental Controls

- Over-provisioned HVAC systems provide cooling and humidity control
  - Flooring systems are dedicated for air distribution
- 

## › Certifications

- SAS70 type 2
-