Cisco Meraki Privacy and Security Practices

List of Technical and Organizational Measures

Introduction

Meraki takes a systematic approach to data protection, privacy, and security. We believe a robust security and privacy program requires active involvement of stakeholders, ongoing education, internal and external assessments, and instillment of best practices within the organization.

Physical Access and Admittance Control

To deny unauthorized persons access to data processing systems in which Customer Data is processed.

This is accomplished by:

- Secure account credentials including two-factor authentication.
- Account security protections (strong passwords, maximum number of failed attempts, IP based login restrictions, etc.)
- Change management including change logs and change event alerting.
- 24x7 automated intrusion detection.
- A high security card key system and biometric readers are utilized to control facility access.
- All entries, exits, and cabinets are monitored by video surveillance.
- Security guards monitor all traffic into and out of the data centers 24x7, ensuring that entry processes are followed.
- Software development life cycle and change management / change control policy and processes.
- Product development secure coding guidelines and training policy and procedures.
- Access to Customer data restricted to personnel based on appropriate business need and limited by functional role.

Access Control

To prevent data processing systems from being used without authorization.

This is accomplished by:

- Software development life cycle and change management / change control policy and processes.
- Access to Customer Data restricted to personnel based on appropriate business need and limited by functional role.
- Information security responsibilities for employees.
- Audit trails policy and procedures, and history and log retention policy and procedures.
- Data control and access control policies and procedures.

Data Access Control

To ensure that persons authorized to use systems in which Customer Data is processed only have access to the Customer Data as they are entitled to in accordance with their access rights and authorizations, and to prevent the unauthorized reading, copying, modification or deletion of Customer Data.

This is accomplished by:

- Access to Customer Data restricted to personnel based on appropriate business need and limited by functional role.
- Audit trails policy and procedures, and history and log retention policy and procedures.

Data Transfer Control

To prevent the unauthorized reading, copying, modification or deletion of Customer Data which is under Meraki's control while Customer Data is being transferred electronically, transported or recorded on data storage devices, and to ensure that the intended recipients of Customer Data who are provided with Customer Data by means of data communication equipment can be established and verified.

This is accomplished by:

- Encrypted communication between Meraki hardware devices and Meraki's servers (HTTPS / SSL), as well as between Meraki's servers.
- Logging of activity of administrators (time, IP, and approximate location (city, state) of logged in administrators).
- Account passwords stored in encrypted format on Meraki servers.
- Full disk encryption on all Meraki servers

Input Control

To ensure it is possible to establish an audit trail as to when and by whom Customer Data has been entered, modified, or removed from systems being used by (or on behalf of) Meraki to process Customer Data.

This is accomplished by:

- Logging of activity of administrators (time, IP, and approximate location (city, state) of logged in administrators).
- Access to Customer data restricted to personnel based on appropriate business need and limited by functional role.
- Data control and access control policies and procedures.
- Customer's ability to block entirely Meraki's access to Customer's Hosted Software account and prevent Meraki from accessing Customer Data.
- Session timeouts.

Order/Instruction Control

To ensure that Customer Data processed by or on behalf of Meraki can only be processed in accordance with the Customer's instructions.

This is accomplished by:

- Change management including change logs and change event alerting.
- Audit trails policy and procedures, and history and log retention policy and procedures.
- Customer can entirely block Meraki's access to Customer's Hosted Software account thereby preventing Meraki from accessing Customer Data.

Availability Control

To ensure the protection of Customer Data which is under the control of Meraki against accidental destruction or loss.

This is accomplished by:

- 99.99% uptime service level agreement.
- Customer network configuration data and statistical data replicated across independent data centers with no common point of failure.
- Real-time replication of data between datacenters (within 60 seconds).
- Nightly archival backups for customer configuration data and statistical data.
- 24x7 independent outage alert system with 3x redundancy.

Intended Use Control

To ensure that Customer Data collected is only used for the intended purpose under the Agreement.

This is accomplished by:

- Customer Data used exclusively to provide the features and functionality available in the hosted software.
- Customer Data is automatically processed according to the specific features enabled by the customer and as required to secure and maintain the infrastructure.
- Change management including change logs and change event alerting.
- Audit trails policy and procedures, and history and log retention policy and procedures.
- Customer can entirely block Meraki's access to Customer's Hosted Software account thereby preventing Meraki from accessing Customer Data.

Documentation

Meraki keeps documentation of organizational and technical measures in case of audits. Meraki takes reasonable steps to ensure that its employees and other persons at Meraki physical locations are aware of and comply with the organizational and technical measures set forth in this document.

Additional Measures

Out-of-Band Architecture

- Only network configuration and usage statistics are stored in the cloud.
- Data stored or transmitted by means of Customer's network does not traverse Meraki's servers.

Cloud Services Security

- Daily vulnerability testing of datacenter infrastructure.
- Protected via IP and port-based firewalls.
- Remote access restricted by IP address and verified by public key (RSA.)
- Systems are not accessible via password access.
- Administrators automatically alerted on configuration changes.

Cloud Services Infrastructure

- Data centers are certified by industry-recognized standards such as ISO 9001:2008, ISO 27001, PCI DSS, SSAE16, and ISAE 3402 (SAS70) including Type II.
- Configuration standards for all system components policy and procedures.
- 24x7 automated failure detection — all servers are tested every five minutes from multiple locations.

Disaster Preparedness

- Data centers feature sophisticated sprinkler systems with interlocks to prevent accidental water discharge.
- Diesel generators provide backup power in the event of power loss.
- UPS systems condition power and ensure orderly shutdown in the event of a full power outage.
- Seismic bracing is provided for the raised floor, cabinets, and support systems.
- In the event of a catastrophic datacenter failure, services failover to another geographically separate datacenter.

Organization and Personnel

- Formal assignment of information security responsibilities by the Security Director and the Meraki Security Team.
- A formal security awareness program.
- Documentation and business justification for use of all services, protocols and ports allowed.
- Management of service providers policy and procedures.
- Criminal background review of all Meraki personnel.
- Rapid escalation procedures across multiple operations teams.

Document History

Version	Revision Date	Notes
1.0	2015	Initial Release
1.1	19 February 2018	Updated for 2018, updated formatting
1.2	05 November 2020	Updated for 2020
1.3	23 November 2020	Removed sections that no longer apply to Meraki, as we no longer perform ISO gap analyses, and password rotations are outdated