# Garanties

Sécurité, fiabilité et confidentialité des services Cloud de Cisco Meraki

## En bref

- Niveau de service (SLA) de 99.99%
- Authentification forte
- Architecture redondante hautement disponible
- Datacenters audités SAS 70 type II

Cisco Meraki propose le service réseau Cloud le plus vaste du marché. Le service Cloud de Meraki fait fonctionner plus de 18000 réseaux dans le monde. Meraki détient également la plus grande expérience du Cloud, fort de son service de production opérationnel en continu depuis six ans. Des milliers de professionnels de l'informatique comptent sur la plateforme de réseau Cloud de Meraki, parmi lesquels des entreprises, des hôpitaux, des banques et des commerces de détail.

Ce document constitue le principal recueil d'informations sur la sécurité, la confidentialité et la fiabilité associées aux services Cloud hébergés de Meraki. Vous y trouverez des informations sur les sujets suivants :

- Nos datacenters, nos processus de sécurité et nos certifications
- Nos méthodes de sauvegarde des données
- Les meilleures pratiques pour sécuriser le réseau de votre entreprise
- La façon dont les réseaux de Meraki continuent de fonctionner lors d'une déconnexion du Cloud
- Des informations, des outils et les meilleures pratiques sur la conformité PCI
- L'accord de niveau de service (SLA) Meraki de 99.99% de temps de fonctionnement

## Conception des datacenters Meraki

Le service Meraki est installé en colocation dans des datacenters de Tier 1certifiés SAS70 type II. Ces datacenters sont dotés d'une sécurité physique et de la cyber-sécurité qui se fait de mieux, ainsi que d'une conception hautement fiable. Tous les services Meraki sont répliqués sur plusieurs datacenters indépendants, si bien que les services accessibles par les clients bénéficient d'une reprise rapide en cas de panne exceptionnelle d'un datacenter.

### Contrôle de la disponibilité

- Accord de niveau de service (SLA) de 99.99% de temps de fonctionnement (soit moins d'une heure par an)
- Détection automatique de panne 24 heures sur 24 et 7 jours sur 7 – tous les serveurs sont testés toutes les cinq minutes à partir de plusieurs emplacements différents
- Procédures de remontée hiérarchique rapide dans plusieurs équipes opérationnelles
- Système indépendant d'alerte de fuite avec une triple redondance

### Redondance

- Cinq datacenters dispersés géographiquement
- Les données de chaque client (configuration réseau et mesures de consommation) sont répliquées sur trois datacenters indépendants
- Réplication en temps réel des données entre datacenters (sous 60 secondes)
- Sauvegardes d'archivage de nuit

### Reprise après inciden

- Reprise rapide sur disque de secours en cas de panne matérielle ou due à une cause naturelle
- Architecture hors bande préservant les fonctionnalités du réseau de l'utilisateur final, même en cas de déconnexion des services Cloud de Meraki
- Procédures de reprise renforcées chaque semaine

### Sécurité des services Cloud

- Détection automatique d'intrusion 24 heures sur 24 et 7 jours sur 7
- Protection par pare-feux IP et au niveau des ports
- Accès distant restreint par adresse IP et vérifié par clé publique (RSA)
- Systèmes non accessibles par mot de passe
- Les administrateurs sont automatiquement alertés des modifications de configuration

### Architecture hors bande

- La configuration réseau et les statistiques de consommation seules sont stockées dans le Cloud
- Les données de l'utilisateur final ne transitent pas par le datacenter
- Toutes les données sensibles (par exemple les mots de passe) sont stockées en format chiffré

### Sécurité physique

- Utilisation d'un système par carte-clé et de lecteurs biométriques de haute sécurité pour contrôler l'accès à l'installation
- Toutes les entrées, sorties et les armoires sont contrôlées par vidéosurveillance
- Des agents de sécurité surveillent tous les déplacements en entrée et en sortie des datacenters, 24 heures sur 24 et 7 jours sur 7, pour assurer l'application des processus d'entrée

### Protection anticipée en cas d'incident

- Les datacenters sont équipés de systèmes d'aspersion sophistiqués et verrouillés pour éviter tout déversement accidentel d'eau
- Des générateurs au fioul fournissent une énergie de secours en cas de coupure de courant
- Des systèmes d'alimentation sans coupure régulent le courant et assurent une mise hors service organisée en cas de coupure totale de courant
- Chaque datacenter bénéficie des services d'au moins deux opérateurs de premier plan
- Le plancher surélevé, les armoires et les systèmes de soutien bénéficient d'un entretoisement parasismique
- En cas de panne exceptionnelle d'un datacenter, les services sont repris à partir d'un autre datacenter distinct géographiquement

### Contrôles de l'environnement

- Des systèmes CVCA optimisés assurent un contrôle du refroidissement et de l'humidité
- Les systèmes de plancher se chargent de répartir l'air

### Tests réguliers de tentative d'intrusion

- Tous les datacenters de Meraki subissent des tests quotidiens de tentative d'intrusion par un tiers indépendant

### Certification des datacenters

- Les datacenters de Meraki sont certifiés SAS70 type II

## Plan de contrôle hors bande

Le plan de contrôle hors bande de Meraki sépare les données de gestion du réseau des données des utilisateurs. Les données de gestion (par exemple configuration, statistiques, contrôle, etc.) partent des dispositifs de Meraki (points d'accès WiFi et routeurs) vers le Cloud de Meraki par connexion Internet sécurisée. Les données des utilisateurs (navigation Web, applications internes, etc.) ne circulent pas par le Cloud mais partent directement vers leur destination sur le LAN ou par le réseau WAN.

Avantages d'un plan de contrôle hors bande:

### Évolutivité

- Débit illimité: pas de goulots d'étranglement d'un contrôleur centralisé
- Ajout de dispositifs ou de sites sans tunnel MPLS

### Fiabilité

- Haute disponibilité assurée par un service Cloud redondant
- Le réseau fonctionne, même si le trafic de gestion est interrompu

### Sécurité

- Aucun trafic des utilisateurs ne passe par les datacenters de Meraki
- Conformité complète à HIPAA / PCI

### Que se passe-t-il si mon réseau se déconnecte du contrôleur dans le Cloud de Meraki ?

Grâce à l'architecture hors bande de Meraki, la plupart des utilisateurs finaux ne sont pas affectés si les points d'accès WiFi et les routeurs de Meraki ne peuvent pas communiquer avec les services Cloud de Meraki (par exemple en cas de panne temporaire du réseau étendu) :

- Les utilisateurs peuvent avoir accès au réseau local (imprimantes, fichiers partagés, etc.)
- Si la connexion au réseau WAN est disponible, les utilisateurs peuvent se servir d'Internet
- Les règles réseau (règles des pare-feux, qualité de service, etc.) continuent d'être appliquées
- Les utilisateurs peuvent s'authentifier via 802.1X/RADIUS
- Les utilisateurs WiFi peuvent circuler entre les points d'accès
- Les utilisateurs peuvent lancer et renouveler les locations DHCP
- Les tunnels VPN en place continuent de fonctionner
- Les outils de configuration en local restent disponibles (par exemple configuration IP des dispositifs).

Pendant la période d'inaccessibilité du Cloud de Meraki, l'administration, le contrôle et les services hébergés sont temporairement indisponibles :

- Les outils de configuration et de diagnostic ne sont pas disponibles
- Les statistiques de consommation sont stockées localement jusqu'à ce que la connexion au Cloud soit rétablie, moment auquel elles sont transmises au Cloud.
- Les pages d'accueil et les fonctions associées ne sont pas disponibles

## Outils de sécurité et meilleures pratiques pour les administrateurs

Outre son architecture hors bande sécurisée et ses datacenters renforcés, Meraki offre plusieurs outils aux administrateurs en vue d'optimiser la sécurité de leurs déploiements réseaux. En utilisant ces outils, ils bénéficient d'une protection, d'une visibilité et d'un contrôle optimisés de leurs réseaux Meraki. Cette page présente des informations sur la façon de renforcer rapidement et facilement la sécurité de vos comptes meraki.com et les meilleures pratiques que nous recommandons pour le contrôle et l'audit des comptes. Pour de plus amples informations, se référer au manuel sur le contrôleur dans le Cloud de Meraki.

### Activer l'authentification forte

L'authentification à double facteur ajoute une couche de sécurité supplémentaire au réseau d'une entreprise en nécessitant l'accès au téléphone d'un administrateur, en plus de son nom d'utilisateur et de son mot de passe, en vue de se connecter aux services Cloud de Meraki. L'implémentation de cette authentification forte de Meraki utilise une technologie SMS sécurisée, pratique et économique : après avoir entré son nom d'utilisateur et son mot de passe, l'administrateur reçoit par SMS un code à usage unique qu'il doit entrer pour que l'authentification soit complète. Au cas où un hacker devine ou découvre le mot de passe de l'administrateur, il ne sera toujours pas en mesure d'avoir accès au compte de l'entreprise dans la mesure où il ne détient pas le téléphone de l'administrateur. Meraki inclut l'authentification forte pour tous les utilisateurs professionnels sans coût supplémentaire.

### Renforcer les règles de mots de passe

Il est possible de configurer des règles de sécurité à l'échelle de l'entreprise pour vos comptes Meraki afin de mieux protéger l'accès au tableau de bord Meraki. Sous Entreprise > Configurer, il est possible de :

- Imposer une modification de mot de passe périodique (par exemple tous les 90 jours)
- Exiger une longueur et une complexité minimales pour les mots de passe
- Bloquer les utilisateurs après des tentatives répétées de connexion échouée
- Désactiver la réutilisation des mots de passe
- Restreindre les connexions par adresse IP

### Appliquer le principe du droit d'accès minimal par une administration basée sur les rôles

L'administration basée sur les rôles vous permet de désigner des administrateurs pour des sous-divisions spécifiques de l'entreprise et de préciser s'ils n'ont qu'un accès de consultation aux rapports et aux outils d'identification de panne, de supervision des accès invités gérés via Meraki Lobby Ambassador, ou s'ils peuvent faire des modifications de configuration du réseau. L'administration basée sur les rôles réduit les risques de mauvaise configuration accidentelle ou malintentionnée et cantonne les erreurs à des portions isolées du réseau.

### Activer les alertes par mail de modification de configuration

Le système de Meraki peut automatiquement envoyer des mails d'alerte lisibles par l'utilisateur lorsque des modifications de configuration réseau ont lieu, ce qui permet à tout le service informatique de rester au fait des nouvelles règles. Les alertes de modification sont particulièrement importantes pour les services informatiques vastes ou distribués.

### Auditer périodiquement la configuration et les identifiants

Meraki journalise l'heure, l'IP et l'endroit approximatif (ville, état) des administrateurs connectés. De plus, Meraki fournit un journal de modifications des configurations dans lequel des recherches peuvent être faites et qui indique quelles modifications de configuration ont été faites, par qui, et la division de l'entreprise concernée par la modification. L'audit des informations de configuration et de connexion apporte une grande visibilité dans votre réseau.

### Vérifier les certificats SSL

L'accès aux comptes Meraki ne peut se faire que par https, ce qui garantit que tous les échanges entre le navigateur d'un administrateur et les services Cloud de Meraki sont chiffrés. Comme pour tout service Web sécurisé, ne vous connectez pas si votre navigateur affiche des messages d'alerte de certificat, ce qui peut indiquer une attaque de type « man-in-the-middle ».

### Déconnexion en cas d'inactivité

Les utilisateurs sont avertis par notification 30 secondes avant d'être déconnectés, ce qui leur permet d'étendre leur session. Une fois le temps expiré, les utilisateurs doivent se reconnecter.

## Conformité au standard PCI pour les paiements par Carte Bancaire

Meraki offre une solution complète pour assurer un environnement WiFi conforme au PCI selon les normes strictes d'un audit PCI de niveau 1 (le niveau d'audit le plus rigoureux). L'ensemble enrichi de fonctions de sécurité de Meraki répond à toutes les normes de sécurité des données de PCI, ce qui aide les clients à mettre en place et à maintenir un réseau sécurisé, à protéger les données des détenteurs de cartes, à maintenir un programme de gestion des vulnérabilités, à implémenter de solides mesures de contrôle d'accès et à faire le suivi de la sécurité réseau.

Contrairement aux LAN WiFi classiques, l'infrastructure intelligente de sécurité de Meraki élimine la complexité dans la gestion, les

tests manuels et les difficultés d'une maintenance permanente qui conduisent à des vulnérabilités. Les fonctions de sécurité intuitives et économiques de Meraki sont idéales pour les administrateurs réseau et, par ailleurs, les outils d'administration puissants et finement granulaires, les protections des comptes, les audits et la gestion de modifications satisfont les responsables de la sécurité des systèmes d'information.

Grâce à une gestion centralisée depuis le Cloud, Meraki permet facilement et à moindre coût d'effectuer des déploiements, des contrôles et des vérifications de conformité au PCI du WiFi sur les réseaux distribués de toutes dimensions.

## Accord de niveau de service de Meraki

Pendant la durée de votre licence du contrôleur dans le Cloud de Meraki (le "Contrat") l'interface Web du contrôleur dans le Cloud de Meraki est opérationnelle et disponible pour le client au moins 99.9% du temps de chaque mois calendaire (L'"Accord de niveau de service de Meraki"). Si Meraki ne remplit pas les conditions de son accord de niveau de service et que le Client respecte ses obligations au titre de l'accord de niveau de service de Meraki, le Client a le droit de recevoir un crédit de service tel que décrit ci après. Cet accord de niveau de service de Meraki indique le seul et unique recours du Client en cas de manquement de la part de Meraki à honorer l'accord de niveau de service de Meraki.

**Définitions**
Les définitions suivantes s'appliquent à l'accord de niveau de service de Meraki.

"Période d'indisponibilité" s'applique dans le cas d'un taux d'erreur utilisateur de plus de cinq pour cent. La période d'indisponibilité se mesure en fonction du taux d'erreur côté serveur.

"Services couverts par Meraki" signifie le service du contrôleur dans le Cloud de Meraki, pour tout produit de Meraki.

"Pourcentage de bon fonctionnement mensuel" signifie le nombre total de minutes d'un mois calendaire moins le nombre de minutes d'indisponibilité subies dans le mois calendaire, divisé par le nombre total de minutes du mois calendaire.

"Crédit de service" signifie, comme suit, que Meraki ajoute un certain nombre de jours de service à la fin de la période de service, sans coût pour le Client.

**Le client doit faire une demande de crédit de service.**
Afin de recevoir tout crédit de service tel que décrit précédemment, le Client doit en avertir Meraki sous trente jour, à partir du moment où le Client devient éligible à un crédit de service. Le non respect de cette modalité annule le droit du Client à recevoir un crédit de service.

**Crédit de service maximum.**
Le nombre cumulé maximum de crédits de service que Meraki déclenche pour le Client pour toutes les périodes d'indisponibilité qui ont eu lieu au cours d'un mois calendaire ne doit pas dépasser quinze jours supplémentaires de service à la fin de la période de service du Client (ou la valeur de 15 jours de service sous forme de crédit financier pour un compte client facturé mensuellement). Les crédits de service ne peuvent pas être échangés contre ou convertis en somme financière.

**Exclusions de l'accord de niveau de service de Meraki.**
L'accord de niveau de service de Meraki ne s'applique pas à tout service qui exclut explicitement cet accord de niveau de service de Meraki (tel qu'indiqué dans la documentation afférente au service concerné) ou dans le cas de tout problème de performance : (i) causé par un cas de force majeure ou (ii) qui résulte de l'équipement du Client ou de l'équipement d'un tiers ou des deux (hors du contrôle principal de Meraki).