# Soluzione per la gestione della sicurezza dei sistemi aziendali

## Cisco Meraki MX

*"Appliance per la sicurezza gestite nel cloud.*
*Gestione centralizzata di sicurezza, networking e controllo delle applicazioni".*

Scopri l'appliance di sicurezza Cisco Meraki MX, la soluzione innovativa per la sicurezza informatica aziendale, particolarmente indicata per la gestione e il controllo della sicurezza delle connessioni in azienda, con la possibilità di connettere la sede principale alle sue diverse sedi.

La soluzione è gestita completamente dal cloud, pertanto è facile eseguire l'installazione e la gestione da remoto.

La serie MX include una gamma completa di servizi di rete che non necessitano di appliance aggiuntive. I servizi includono un firewall di prossima generazione, il content filtering, il filtro delle ricerche Web, la prevenzione delle intrusioni basata su SNORT®, il caching dei contenuti Web, l'ottimizzazione della WAN, multipli uplink WAN e il failover 4G.

**I servizi includono:**

- firewall di prossima generazione,
- content filtering,
- filtro delle ricerche Web,
- prevenzione delle intrusioni basata su SNORT®,
- caching dei contenuti Web,
- ottimizzazione della WAN,
- multi WAN,
- failover 3G/4G.

**Quali sono le sue principali funzionalità?**

- filtraggio di siti web e applicazioni
- gestione di connettività multiple e limitazione di banda
- antivirus e antimalware
- auto VPN
- possibilità di abbinamento con Access Point Meraki per gestione avanzata del Wi-Fi aziendale
- funzionalità avanzate nel controllo e ricerca delle periferiche

Ribo IT SOLUTIONS

cisco Meraki

# Caratteristiche

*"Cisco Meraki MX è la soluzione innovativa per la sicurezza informatica aziendale, gestita completamente dal cloud, facile da installare e gestire da remoto."*

## Funzionalità avanzate di Unified Threat Management (UTM)

- Controllo del traffico in base alle applicazioni: policy per la banda larga a seconda del tipo di applicazione di layer 7 (ad esempio, YouTube, Skype, P2P).
- Content filtering: filtro conforme a CIPA, applicazione della funzione di ricerca sicura (Google/Bing) e YouTube for Schools.
- Prevenzione delle intrusioni: il sensore IPS conforme a PCI utilizza SNORT®, il database di Sourcefire, leader nel settore della sicurezza delle reti.
- Anti-virus e anti-phishing: motore di Kaspersky per la protezione basato sui flussi.
- Policy di sicurezza basate sull'identità e gestione delle applicazioni.

## Leader nella gestione mediante cloud

- Gestione unificata delle reti WAN, LAN e LAN wireless da un solo dashboard basato su Web.
- I modelli di impostazioni facilitano la scalabilità in tutti gli ambienti, da quelli di dimensioni ridotte fino agli ambienti molto ampi che comprendono vari siti con decine di migliaia di dispositivi.
- Gestione basata sui ruoli degli utenti, invio di avvisi tramite e-mail per notificare eventuali modifiche della configurazione, altri problemi di configurazione e interruzioni dell'alimentazione elettrica, log delle modifiche utili per gli audit.
- Report archiviati su cloud con dettagli su utenti, dispositivi e utilizzo delle applicazioni.

## Architettura gestita dal cloud

Realizzate per l'architettura Cisco Meraki gestita dal cloud, le appliance della serie MX sono gli unici dispositivi di Unified Threat Management gestiti completamente mediante il cloud.

Le appliance MX eseguono il self-provisioning, acquisendo automaticamente le policy e le impostazioni di configurazione dal cloud. I potenti strumenti di gestione remota forniscono visibilità e controllo su tutta la rete e consentono di amministrare i sistemi senza la presenza di personale di rete in loco.

I servizi cloud offrono aggiornamenti continui del firmware e delle firme digitali, stabilendo automaticamente i tunnel della VPN da sito a sito e assicurando un monitoraggio della rete 24 ore su 24.

Inoltre, il dashboard di gestione della serie MX può essere usato direttamente dal browser eliminando il bisogno di formazione tecnica del personale.

## VPN site-to-site resiliente con failover 4G

- Auto VPN: generazione automatica di tabelle di routing, impostazione IKE/IPsec e scambio di chiavi di crittografia nel cloud sicuro Cisco Meraki.
- Failover automatico sul collegamento WAN secondario o sulla connessione 4G.
- Interoperatività con VPN con tecnologia IPsec conforme agli standard.
- Failover automatico da MPLS a VPN.
- VPN client: supporto L2TP IPsec per client nativi Windows, Mac OS X, iPad e Android senza costi di licenza basati sul numero degli utenti.

## Servizi gateway per le filiali

- Servizi di gestione DHCP, NAT, QoS e VLAN incorporati.
- Caching dei contenuti Web: velocizza l'accesso ai contenuti utilizzati più di frequente.
- Aggregazione dei collegamenti: combina più collegamenti WAN in un'unica interfaccia ad alta velocità con policy per QoS, controllo del traffico di rete e failover.
- Failover di layer 3: rilevamento automatico delle interruzioni per layer 2 e layer 3, e failover rapido compresi modem USB 3G/4G.
- Ottimizzazione della WAN: l'eliminazione dei dati ridondanti, l'ottimizzazione dei protocolli e la compressione consentono di ridurre il consumo della banda larga fino al 99%.

## Sicurezza assoluta per le reti perimetrali

La piattaforma hardware di MX è progettata appositamente per l'ispezione approfondita dei pacchetti di layer 7, grazie a funzioni di protezione avanzate quali IPS, content filtering, il filtro delle ricerche Web, l'anti-virus, l'anti-phishing e la connettività VPN IPsec; inoltre offre la velocità di trasferimento e la capacità richieste dalle moderne reti con uso intensivo della banda larga.

La tecnologia di fingerprinting del layer 7 permette agli amministratori di bloccare le applicazioni e i contenuti indesiderati, impedendo alle applicazioni non usate a scopo lavorativo, come ad esempio BitTorrent, di consumare banda larga preziosa.
Il motore Sourcefire SNORT® integrato offre una copertura eccellente per la prevenzione delle intrusioni, un requisito importante per garantire la conformità a PCI 2.0.
La soluzione MX utilizza anche il database di classificazione URL Webroot® BrightCloud per il content filtering conforme a CIPA/IWF e il motore Kaspersky® SafeStream per il filtro anti-virus/anti-phishing. Ma soprattutto, questi motori e firme leader del settore per la protezione del layer 7 vengono costantemente aggiornati attraverso il cloud, semplificando la gestione complessiva della sicurezza della rete e il lavoro degli amministratori IT.