

REMOTE ACCESS HOME SECURITY BUNDLE



The current work from home landscape has put an immense amount of pressure on Canadian organizations to continue doing business while dealing with all of the pains of working from home. It has also put a target on home internet as a new source for hackers to gather information. As corporate work from home policies continue to evolve there are many near, mid and long-term implications regarding your workforce's home security set up that must be considered.

Executives and other key employees are often considered high-value targets for hackers attempting to infiltrate a company's network and steal valuable information. Moreover, the increased number of services competing for home internet bandwidth, such as streaming services, gaming and IoT devices, is impacting performance.

Home infrastructure isn't typically designed with enterprise-grade security or capacity in mind. These weaknesses have become even more apparent today, while also making your workforce's home networks more attractive targets for bad actors to exploit. It is more important than ever to set your organization up for long-term success in a remote work landscape with secure access to corporate networks that is easy to configure, manage and stay up to date on patching.



REMOTE ACCESS HOME SECURITY BUNDLE

CDW has selected the combination of the Cisco Meraki MX64 firewall and Cisco Meraki MR36 access point as an effective network security solution to provide enterprise-grade performance and protection while simplifying the setup and management with a cloud-based portal as a single pane of glass that can be maintained by corporate IT remotely.

The solution can act as a stand-alone setup for home or integrate with your existing Meraki corporate deployment. This allows you to extend your corporate wireless network and integrate with Active Directory for identity-based security policies, while allowing you to create personal corporate wireless network for home use. The Meraki MX also supports site-to-site IPSec VPN if you require connectivity to other vendors. A stateful firewall that is positioned behind your workforce's ISP demarcation device, the MX64 has superior 1x GbE uplink and 4x GbE ports for direct connection of wired ethernet devices such as wireless access points, printers, scanners or VoIP handsets. Video conference, social media and gaming can be prioritized or restricted due to layer 7 firewall rules for secure and efficient remote operations by the home user or the corporate IT team through the web management portal.

FEATURES

- Stateful firewall with 250 Mbps of throughput and a high-performance Wi-Fi access point
- Layer 7 application visibility and traffic shaping
- Enterprise-grade network and security
- Easy one-click guest access creation
- Easy to update, patch and setup
- Optional advanced security licensing to filter content in line with existing investment in AMP and Umbrella*
- Cloud-based management with intuitive interface and Wi-Fi performance optimization
- ACI/Viptella/Meraki/UCS/Standard switching and routing
- ICE/Umbrella*/Firepower/RAS
- Advanced data centre, security, enterprise networking and collaboration architecture

BENEFITS

- Speed and throughput support most Internet bandwidth requirements
- Single pane of glass that makes it easy to configure, update and manage
- Prioritizes mission-critical applications and limits recreation traffic
- Flexible for corporate network integration
- Seamless home guest enablement
- Ensures superior Wi-Fi performance
- Our team provides assistance with setup, best practices and knowledge transfer for ongoing management

OUR TEAM CAN

- Leverage our entire account team – including over 700 Cisco Certified Sales Experts – to help you identify the fit and make any adjustments in sizing and licensing
- Work with you and your organization to determine what combination of solutions and tools best suits your needs and ensures your workforce is set up for success with secure access to corporate networks and efficient home Internet performance – no matter the landscape
- Bring our bench depth to bear, with the technical resources and expertise to provide PS for best practices, implementation and address bespoke corporate integration

WHY CDW FOR CISCO?

CDW is uniquely qualified to provide, service and manage this essential combination of Cisco Meraki solutions.

- **Cisco Gold Partner** – CDW has been named a Gold Partner for over five years, and we are one of only three Canadian companies to achieve the Cisco Master Security Specialization, as well as holding Master Specializations in Collaboration, Enterprise Networking, Cloud Builder and Cloud and Managed Services
- **First in our league** – CDW is ranked Cisco's #1 large strategic solutions producer in Canada
- **Market-leading resources** – Our bench strength includes over 500 certifications, 40 Certified Meraki resources, over 200 Cisco Certified Network/Design/Voice Professionals (CCNP) and over 60 Cisco Certified Internetwork Experts (CCIE), in addition to pre- and post-sales delivery experts
- **Advanced specializations support your organization's long-term success** – CDW offers advanced data centre, security, enterprise networking and collaboration architecture to provide you with a complete, full-service selection of tools and solutions

PARTNERED WITH:



**For more information, contact your CDW account team
at 800.972.3922 or visit [CDW.ca/security](https://www.cdw.ca/security)**



The terms and conditions of product sales are limited to those contained on CDW's website at CDW.ca. Notice of objection to and rejection of any additional or different terms in any form delivered by customer is hereby given. CDW®, CDW-G® and PEOPLE WHO GET IT® are registered trademarks of CDW LLC. All other trademarks and registered trademarks are the sole property of their respective owners.