cisco Meraki

5 Simple Ways to Secure Your Network in the Remote Working Era

The game has changed

Today, more than one-third of employees are fully remote and among hybrid workers, one-fifth prefer to solely work from home. As a result, organizations are developing long-term strategies to address the network needs of their work-from-home (WFH) teams.

Meeting these WFH expectations without compromising network security is undoubtedly one of the most complex challenges that IT managers have ever faced.

Yet, while they may have embraced newer approaches to work, many companies have not yet adopted policies that protect or address these work styles. In fact, although technologies exist to protect public and home Wi-Fi, cellular networks, and hotspots, 52% of businesses said they had sacrificed mobile device security in order to meet job deadlines or goals.

IT professionals can deliver the smooth experience users demand and the security every organization requires. This document answers questions like:

- What does a permanent work-from-home strategy look like for IT?
- How can IT minimize risk to the data when employees work remotely?
- How can IT ensure that users, applications, and IP are protected when there is limited visibility?
- How can IT gain control over endpoints and troubleshoot when users work remotely?

The facts

97% of organizations in the U.S. changed cybersecurity policies to support remote work.

84% of employees say network infrastructure is essential for a seamless WFH experience.

26% of security pros who previously worked remotely and must now sometimes work from an office want a new job.

The three security objectives in this era are:

Secure and protect the data of the business

Protect users working remotely

Ensure business continuity

5 questions every IT manager must answer

In order to find a secure long-term solution, we need to ask the right questions. Here are five to get you started:

01 Do you know where the biggest security threats to the business are coming from?

A lot of airtime is given to external cybersecurity threats such as phishing, hacking, and social engineering. Most organizations are aware of the implications to their network security and mitigate risks accordingly. However, threats can also come from internal sources such as employees attempting to access applications without permission, e.g. confidential HR systems.

We recommend that you identify and understand both internal and external risk factors when planning your long-term network security strategy.

02 Does your network have four points of protection?

One of the best ways to assess the risk to your network is to consider what would be at risk if someone gained access to a users's unlocked computer or phone?

We recommend having four points of protection to your network:

Endpoint protection:

Ensure all devices are secure by installing antivirus and anti-malware software to protect both data and hardware. And make sure devices can be easily flushed of data and factory reset if employees leave the organization.

Application protocols:

To prevent users inadvertently downloading untested software, malware or viruses, or breaking software licensing agreements, it's important to only allow authorized users to access applications.

Safeguarding identity:

The ability to identify and verify the user and device before granting access to the network and applications is critical.

Protecting the premises:

It is paramount to safeguard data and physical assets from external visitors and threats.

03 Are your users categorized?

Categorization of users is important in organizations because certain employees hold more sensitive data and therefore require different levels of security and support. We recommend the following starting point for categorization:

1 - VIP and executives

2 - Employees in departments with intellectual property, such as legal and human resources

3 - Other users

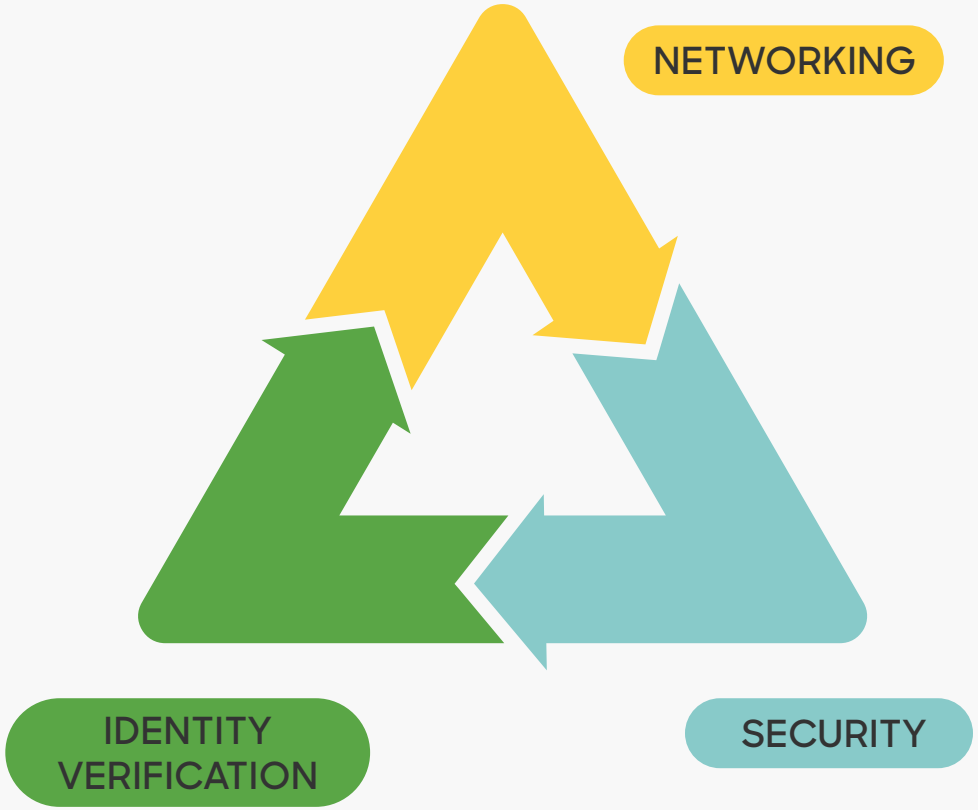
Once you have categorized user groups, you can easily verify their identities, grant permissions to access specific applications, identify the solutions that are applicable to their level of access, and provide the appropriate level of support. At most organizations, remote users secure their network access via a VPN.

04 Have you adopted a multitiered approach to network security?

Taking a multitiered approach to network security is critical due to the complexity, number of variables, and security threats to users, the business, and their data. We recommend you adopt a Secure Access Service Edge (SASE) architecture to secure your devices.

The SASE architecture incorporates three components:

1. **Networking:** safeguards premises, endpoints, and applications.
2. **End-to-end security:** secures connectivity.
3. **Identity verification:** protects and verifies users and devices.



05 Do you have visibility of your remote workers?

IT teams now face the challenge of having to monitor network performance remotely with little to no visibility. Therefore, troubleshooting becomes challenging for IT teams with less IT-savvy users who need to provide accurate information in order to diagnose problems correctly. We recommend installing an endpoint and/or access point solution to give IT admins increased visibility.

WINNING STRATEGY

Give your remote employees the first-class experience your corporate office teams enjoy.

Accelerate remote employee onboarding with seamless provisioning using Meraki Systems Manager.

Protect data and prioritize critical traffic via Meraki MX security and SD-WAN.

Keep teleworkers productive and get complete network and application visibility with the Meraki dashboard.

Deliver WFH joy without WFH tech headaches with Cisco Meraki. Find out more here.