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

cisco Meraki

The Game Has Changed.

88% of companies have encouraged or required employees to work from home in response to COVID-19 (Gartner, 2020). What was initially an interim solution to the pandemic, now requires a long-term strategy, as working from home (WFH) has become the new norm.

So this begs the question, is your network built to handle 2020 onwards?

Meeting these WFH expectations without compromising network security is undoubtedly one of the most complex challenges that IT managers have ever faced. The UK National Fraud & Cyber Security Centre reported that there was a 400% increase in cyber-crime since March 2020. This sudden increase leaves organisations vulnerable and with plenty of questions...

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

The facts.

54% of IT professionals think that remote workers are a greater security risk (OPENVPN)

99% of remote workers would like to continue doing so to some extent (Buffer,2020)

During the transition to remote work this year, employees struggled with three principal challenges:

38% VPN access

37% Wi-Fi connectivity and reliability

35% and video conferencing apps

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 be asking the right questions. Here are 5 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 cyber security threats such as phishing, hacking and social engineering. Most organisations are very 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 that they do not have permission for, e.g. access to confidential HR systems.

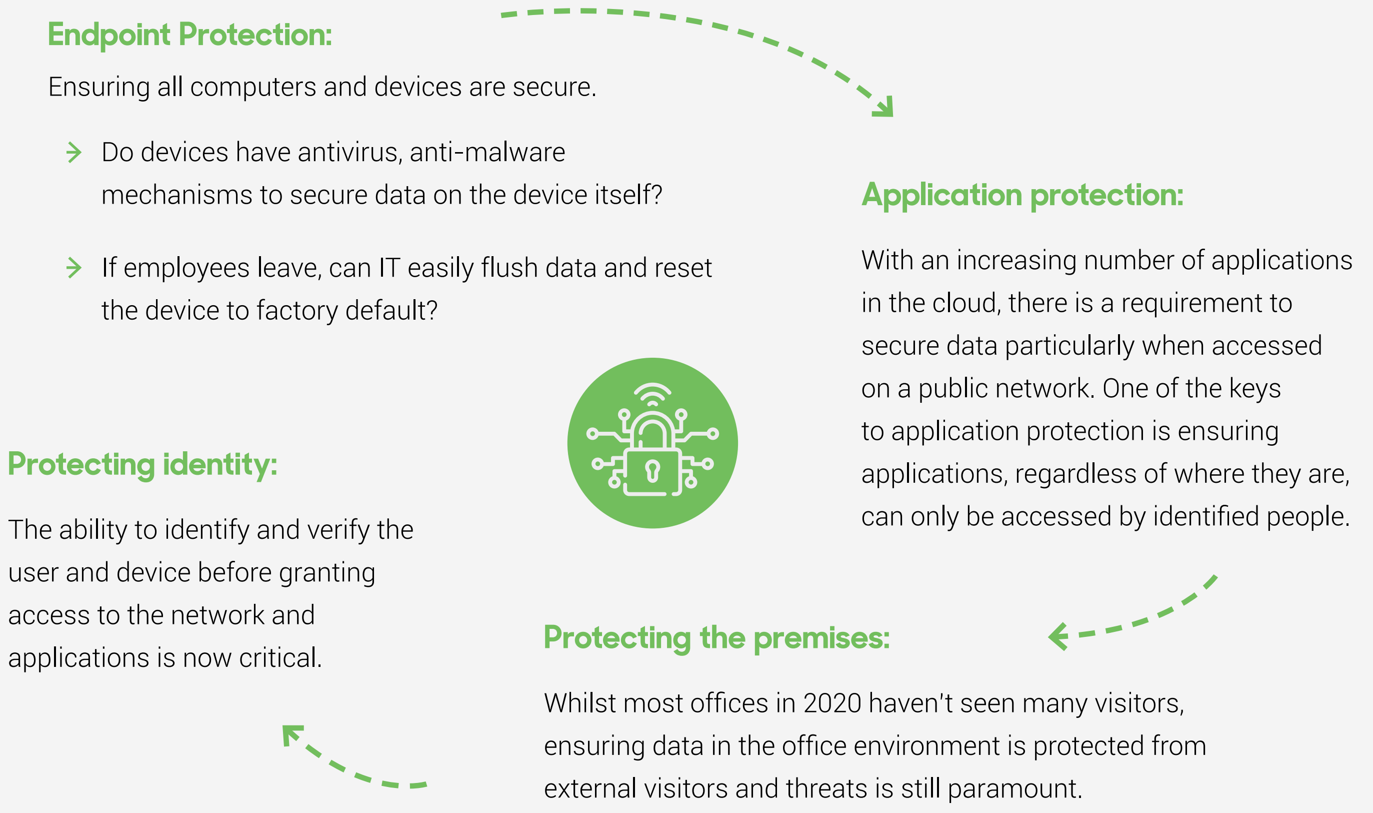
We recommend that you identify and understand both internal and external risk factors when planning your long-term network security strategy.

02

Does your network have four points of protection?

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

We recommended having four points of protection to your network:



Endpoint Protection:

Ensuring all computers and devices are secure.

- Do devices have antivirus, anti-malware mechanisms to secure data on the device itself?
- If employees leave, can IT easily flush data and reset the device to factory default?

Application protection:

With an increasing number of applications in the cloud, there is a requirement to secure data particularly when accessed on a public network. One of the keys to application protection is ensuring applications, regardless of where they are, can only be accessed by identified people.

Protecting the premises:

Whilst most offices in 2020 haven't seen many visitors, ensuring data in the office environment is protected from external visitors and threats is still paramount.

Protecting identity:

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

03

Are your users categorised?

Categorisation of users is important in organisations because certain employees hold more sensitive data and therefore require different levels of security and support. We recommend the starting point for categorisation would be:

1. VIP and Executives
2. Employees with IP e.g. Legal, HR
3. Other users

Once users have been categorised you can easily verify their identity, grant permissions to access certain applications, identify which solution is applicable to their level of access and provide the appropriate level of support. For most organisations, the majority of remote users will secure their network with a VPN.

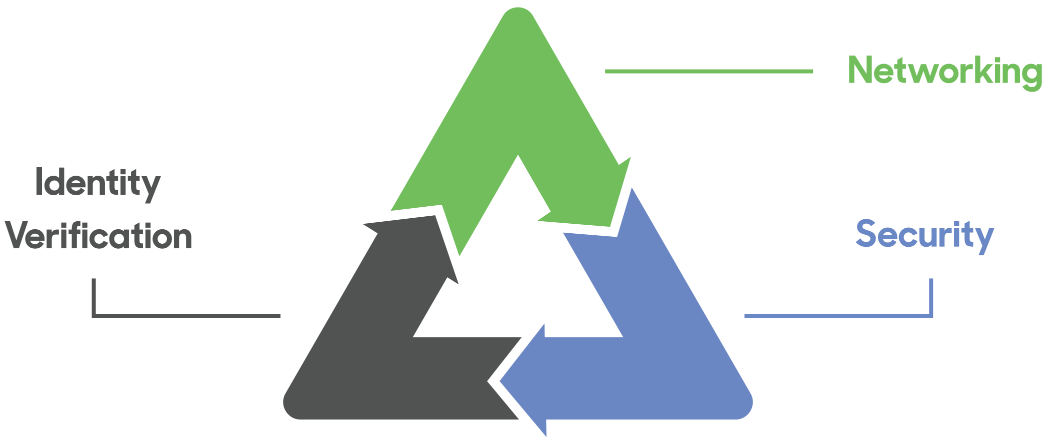
04

Have you adopted a multi-tiered approach to network security?

A multi-tiered 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 the Secure Access Service Edge (SASE) architecture, to secure your devices.

The SASE architecture incorporates three components:

1. **Networking** focuses on secure connectivity, whether that is in the home or office.
2. **End-To-End Security** focuses on protecting the premises, endpoint and application.
3. **Identity Verification** focuses on securing and verifying the user and device.



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. Troubleshooting, therefore, 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 end point and/or access point solution to give IT admins increased visibility.

48% of IT teams saw an increase in the number of support tickets from employees during the period of forced remote work (Bdaily)

WHAT'S NEXT?

Secure your network with Cisco Meraki

You + Meraki = Unstoppable

If any of the five must answer questions left you scratching your head, then Meraki has you covered. We would like to invite you to our upcoming webinar, **"How to protect your network in the era of remote working".** In this highly engaging chalk and talk style masterclass, we will deep dive into simple and cost-effective solutions to secure your network and remote users.

Tuesday 27th October 2020 **12pm-1pm** **Register Now →**

If you just can't wait to join our masterclass, check out three ways Meraki protects the remote workforce:

Providing Visibility - focuses on allowing IT administrators to troubleshoot, monitor performance and understand their remote networks.

End-to-End Security - focuses on protecting the premises, endpoint and application.

Enabling Identity Verification - focuses on two factor authentication, SMS verification and applying different security rules, depending on the users identity.