Executive Summary

The COVID-19 pandemic has disrupted the ways businesses operate and forced organizations to transform how and where the work is performed. Remote working used to be available for few employees—now it is the new norm and is here to stay. Remote working breaks the boundaries of office walls, allowing work to be performed anywhere. Although the flexibility of the hybrid workforce unleashes the freedom to work from anywhere, the extension of work locations has also unavoidably expanded the attack surface and threat landscape, making these new places security weak points for cyber criminals to launch cyberattacks. As cybersecurity becomes more impactful to digital transformation than ever before, enterprises must now expand and enhance their security capabilities to follow, enable, and contextually protect users depending on the locations they perform their work.

Unsecured Home-networking Environment

According to an Oberlo report in December 2020, 56.8% of the American workforce is working remotely at least part of time. In order to secure this workforce, many companies have invested heavily in identity authentication, access control, virtual private network (VPN), and antivirus on employee work devices and their enterprise systems to secure their business systems, applications, and data when accessed remotely. However, that is not enough. Often overlooked is the employee's home network, which plays a big part in this remote work ecosystem and is also a potential attack vector.
This “noisy” network environment creates a lot of potential entry points for hackers. They can enter from vulnerable home Internet-of-Things (IoT) devices that lack antivirus software; they can also get in from video streaming sites or from clicking on a malicious active directory. Once they enter a home network, they can easily listen to business communications through a work laptop, steal confidential business information, or launch ransomware attacks on a corporate system.

To make things worse, most of the home networks have few security measures. Even if they do, the security capabilities vary from home to home and fall far behind the enterprise-grade security available in the office. Home network security typically comes from consumer-grade Wi-Fi routers or gateway routers provided by service providers. Recently, several enterprise networking vendors also came up with their security solutions for teleworkers in response to growing remote working trends. However, none of these current solutions adequately address the security challenges of working from home.
Enterprise-grade Security With Centralized Management

For companies to secure the business communications and data from the office to working homes, they need a purposely designed solution with seamless, unified security. Some key ingredients in this solution include:

- Clear separation of the private and corporate network within the home network
- Enterprise-grade security with antivirus, ransomware protection, web filtering, and intrusion protection
- Real-time updates on risks and vulnerabilities through threat intelligence
- Central configuration, monitoring, and management for scalability and operational efficiency
- Traffic prioritization for mission-critical business applications

Optimal Wireless Coverage and Performance With Ease of Use

Remote workers need the same reliable performance that they have come to expect in the office. And their home solution needs to be easy to use so they can get up and running without time-consuming IT help. The ideal solution also needs to:

- Allow users the control of their private networks to ensure personal and family privacy
- Set up and manage private networks by employees via mobile app
- Offer Wi-Fi coverage for the whole house
- Secure employees’ private networks with advanced security features

Conclusion

To make working from anywhere scalable and sustainable, businesses should not only offer this flexibility to their employees but equip them with a series of security measures to ensure a safe and protective digital work environment, including a secured network at home.

The diversity of devices, users, and applications running on the home network creates an unsecured environment for work. The traditional gateway routers provided by home internet service providers and the wireless routers sold for home or business don’t have sufficient security capabilities to protect enterprise digital business. The secured work-from-home solution needs to be purposely built with enterprise-grade security, centralized management, scalability, and optimized performance for mission-critical business applications.
