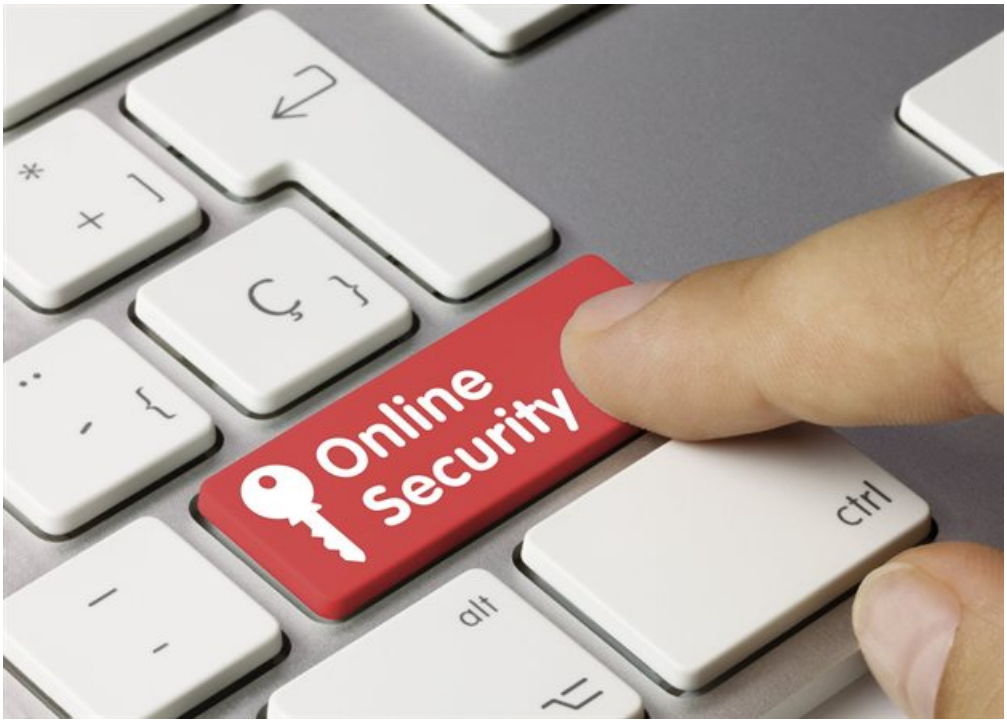
How to secure your remote workforce

By Doros Hadjizenonos

20 Mar 2020

For many organisations, the need to suddenly enable a remote workforce at scale has overtaken long-term plans they may have had to gradually extend remote work capacity. In such a context, time is of the essence, and security must be the cornerstone of business continuity and remote work programmes.



© momius - Fotolia.com

Here are factors every organisation should consider to support a secure move of traditional on-site workers to remote locations:

- Educate employees about the new risks facing them as they work from remote locations. Ensure that all are apprised of the risk of phishing attacks and the need to work only through authorised, secure corporate channels.

- Every newly-remote worker should have a secure device and access to email, internet, teleconferencing, limited file sharing, and function-specific capabilities from their remote work site. They also require access to Software-as-a-Service (SaaS) applications in the cloud, such as Microsoft Office 365. Ensure that all users have a laptop loaded with all of the essential applications they need to do their job.

- Ensure that all remote user devices have a pre-configured client to provide VPN connectivity to corporate headquarters.

- Use multi-factor authentication to prevent cybercriminals from using stolen passwords to access networked resources. To further secure access, issue each user with a secure authentication token, be it a physical device (such as a key fob), or software-based (like a phone app), for an additional layer of validation when making a VPN connection or logging into the network.

- Remote workers who require advanced access to network resources to do their jobs, such as systems administrators, support technicians, emergency personnel, and executive management teams, may require additional authentication and security layers. Pre-configured wireless access points enable secure connectivity from a user's remote location to the corporate network through a reliable, secure tunnel. For a more secure connection, a wireless access point can be combined with a desktop-based next-generation firewall to enable persistent connections, advanced admission control, and a full spectrum of advanced security services, including Data Loss Prevention. These users also require a telephony solution that supports voice over IP (VoIP) to ensure secure communications. Both physical and soft client models are available that enable users to make or receive calls, access voicemail, check call history, and search the organization's directory.

- A secure and scalable headend will be needed to ensure that the sudden increase of remote workers needing access to network resources can be accommodated. A central authentication service connected to the network's active directory, LDAP, and Radius enables remote workers to securely connect to network services at scale. This solution should also support single sign-on services, certificate management, and guest management.

- A next generation firewall should be in place to securely terminate VPN connections, provide advanced threat protection – including the analysis of malware and other suspicious content.

- In a sandboxed environment, with high-performance inspection of clear-text and encrypted traffic. Inspection of encrypted data is extremely processor-intensive, so advanced security processors designed for this purpose are necessary to avoid a bottleneck.

To ensure business as usual with minimal - or no - break in services, solutions must be easily deployable and configurable, ideally with zero-touch provisioning, to support a quick transition to a remote. At the same time, they must deliver full security visibility and control regardless of their deployment environment. This ensures that your organisation can quickly respond with minimal impact on productivity and profitability.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- How to secure your remote workforce - 20 Mar 2020

View my profile and articles...