Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Securing remote workforces at scale

Business continuity plans (BCPs) are being reviewed and put into action to protect Australian businesses as the outbreak of COVID-19 starts to affect the economy. For many businesses, BCPs are designed to help the organisation recover after a single disastrous event. Therefore, they don't always include ways to support a workforce operating remotely for an extended time. Doing so requires a strong focus on security to avoid adding further challenges for businesses to cope with during uncertain times, according to Wavelink, a Fortinet distributor.

One of the key issues of transitioning to a remote workforce is helping employees who are used to working in a physical office get set up to work from alternate locations, often their homes. This can create networking and security issues depending on the employee's existing set-up.

Ilan Rubin, managing director, Wavelink, said, "When employees aren't used to working from home, their home networks generally aren't secured to a corporate standard. This creates vulnerabilities that cybercriminals can leverage. During times of disruption and uncertainty, cybercriminals become especially active because they know there will be plenty of security gaps they can take advantage of.

"Every company's BCP should start with a strong security posture that protects the organisation and its employees regardless of whether they're working from physical offices or from remote locations."

There are six key steps organisations should consider when transitioning on-site employees to remote locations:

1. VPN and endpoint security: VPN connectivity to corporate networks reduces the risk of a successful cyberattack or information breach.

2. Multifactor authentication: this basic security measure can make it harder for cybercriminals to use stolen credentials to access corporate networks. This could include a secure authentication token that can be used to provide an additional layer of authentication.

3. Persistent connectivity: some workers require more reliable connectivity because of the nature of their roles. These workers can be supported by preconfigured wireless access points that connect to the corporate network through a reliable, secure tunnel.

4. Secure telephony: Voice over IP (VoIP) phone solutions can ensure secure communications and let workers communicate as though they were in the office, using the corporate phone network.

5. User and device authentication: a central authentication service can let remote workers securely connect to network services at scale. This solution should support single sign-on services, certificate management, and guest management.

6. Advanced perimeter security: a next-generation firewall can secure the perimeter and provide advanced threat protection, including analysing malware and other suspicious content. This element must be scalable to prevent bottlenecks that reduce productivity for remote workers.

Ilan Rubin said, "Organisations should have comprehensive BCPs in place regardless of external circumstances, such as COVID-19, because the nature of disasters is that they're difficult to predict. Given many knowledge workers could theoretically work from home indefinitely with the right tools in

place, it's essential for organisations to make sure they can do so securely. This type of resilience will help organisations survive and even thrive during any potential lockdown or escalation of the current crisis, as well as cope well with any future scenarios."