Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Overcoming challenges around securing SD-WAN

Software-defined wide area networks (SD-WANs) help overcome networking challenges that make branch-level activities slower than those processed at the network core. SD-WAN delivers better application performance along with deeper visibility into traffic. However, businesses shouldn't assume that SD-WAN is easy to secure when, in fact, the opposite is usually true, according to Wavelink, distributor of Fortinet security solutions.

Ilan Rubin, managing director, Wavelink, said, "SD-WAN delivers significant benefits but it's those very benefits that can make it incredibly challenging to secure. Because it enables direct internet access from devices from anywhere in the network, this means branch security solutions need to take SD-WAN into account alongside split-tunnel challenges created by running various services and remote users from branch resources. This creates complexity that needs to be simplified with an integrated security and network solution."

However, this can be easier said than done, especially considering the global shortage in relevant security skills. Experienced cybersecurity professionals are already under pressure and can struggle to develop a clear strategy to leverage existing security solutions to protect SD-WAN. Without strong security built-in to existing solutions, effective security can be overlooked.

Even existing security solutions may not be sufficient to protect SD-WAN. They are unlikely to be sophisticated and wide-ranging enough to provide strong protection beyond encrypting traffic and detecting malware.

Ilan Rubin said, "The best and most reliable way to secure SD-WAN is using built-in security tools. Embedding these tools directly into the solution overcomes challenges around the distributed nature of connections and services carried by SD-WAN. These tools should include a next-generation firewall, intrusion protection systems, web filtering, anti-virus, anti-malware, encryption, sandbox, and high-speed inspection of encrypted data.

"It's important that this security is natively embedded into SD-WAN to reduce the device footprint and to avoid retro-fitted solutions. Ideally, businesses should deploy SD-WAN functionality through a next-generation firewall device, which lets the business centrally manage the tools and orchestrate security policies through a single pane of glass. This simplifies security management while ensuring a more robust approach."

It's equally important to ensure security solutions deployed as part of the SD-WAN solution integrate seamlessly with other security solutions across the network. This helps raise the level of security across the entire network and helps preserve IT resources, reducing security overhead and letting the company achieve better security despite the skills shortage.