Wavelink

Global Technology | Local Knowledge

MEDIA RELEASE

The problem with too many security options

Businesses are spoiled for choice when it comes to IT and network security. However, this doesn't necessarily mean that they're getting the right solutions or the best protection, especially given the growing complexity of networks and increasing sophistication of cybercriminals. Part of the problem is a lack of universal standards or a way to verify the claims made by security vendors. Businesses need to understand which of the myriad available solutions will deliver real results as opposed to those that cost money without delivering tangible benefits, according to Fortinet distributor, Wavelink.

Ilan Rubin, managing director, Wavelink, said, "While the security and threat landscapes are constantly changing, one thing remains constant; security breaches can be catastrophic to the organisation under attack. Security decision-makers need to see through the hype created by security vendors so they can choose the right solution for their business.

"It's important to change the thinking from a granular approach to solving individual problems to an overarching approach that secures the entire network. Any tool that works in isolation is unlikely to deliver strong value to the organisation. Instead, businesses should look for tools based on open standards and interoperability, and tools that offer broad coverage. The fewer tools an organisation uses, the less complex and hard-to-manage their security will be."

Wavelink recommends that businesses rely on third-party tests and recommendations instead of vendor data sheets. Furthermore, it's important to recognise that the solutions that work for one organisation won't necessarily deliver the same benefits for another organisation, so understanding how the proposed tools work in organisations in a similar industry or with similar operating challenges is critical.

Ilan Rubin said, "Just as a new car buyer would insist on test-driving a vehicle instead of just believing the manufacturer's marketing hype, so IT security professionals must test the tools they're considering using to ensure they work as advertised and will deliver the promised benefits. Just because a vendor says a tool is powered by artificial intelligence or was purpose-built for cloud doesn't mean it's strictly true. And, it doesn't mean that solution is right for the organisation anyway, even if all the claims are correct.

"The most effective solution is likely to be one that takes an integrated and holistic approach, and delivers visibility into every device, application, and network connection."

With literally hundreds of security solutions, platforms, and tools available, it's practically impossible for organisations to thoroughly consider each one on its merits and create a unified, strategic security fabric for the business. To save time and money, and increase the chance of getting the best solution for the organisation's budget, businesses should partner with a security provider that can offer third-party-verified solutions and tailored, expert advice.

Ilan Rubin said, "Working with a security partner takes the burden of choice and management off the IT team's shoulders, freeing IT professionals up to focus on innovation and proactive growth-related activities. It can help the business move faster while reducing costs, safe in the knowledge that the organisation is as protected as it can be."