Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

What organisations must demand from security technology in 2020

Every year, the cybersecurity landscape continues to become more dangerous with attackers finding new and more sophisticated ways to breach even the most up-to-date security systems. The last decade has seen cybersecurity elevated from being the sole responsibility of the IT manager to becoming a key element of risk management for boards. The next decade will continue to see cybersecurity maintain its place as one of the most important business risk considerations for organisations of all sizes, according to Wavelink, a Fortinet distributor.

Ilan Rubin, managing director, Wavelink, said, “Innovation is essential for business survival but often brings security challenges with it. However, rather than slow down innovation to avoid security issues, organisations should ensure that security is built in to every aspect of their operations from the ground up, including new applications or business systems. And, as Australia for example, gears up for 5G networks, the same fast connectivity that facilitates business will also provide opportunities for cybercriminals to move faster.”

Wavelink has identified five key capabilities organisations should demand from their cybersecurity solutions in 2020:

1. A broad approach

Gone are the days when organisations needed to choose best-of-breed point solutions to secure each individual aspect of the network. Instead, businesses need to choose a cybersecurity approach that protects the organisation from end to end. This includes cloud deployments, Internet of Things (IoT) networks, and geographically distributed network environments. Gaining full visibility into the entire network, regardless of architecture or location, is crucial to be able to protect it.

2. Automation

Cybercriminals are harnessing artificial intelligence (AI) and its subset, machine learning, to mount attacks faster and more successfully. Organisations simply can’t rely on manually managed cybersecurity solutions anymore. As attacks blitz organisations, the time it takes to discover and remediate an attack becomes longer, increasing the amount of damage that can be done. It’s therefore essential to use automated solutions that can combat these attacks as quickly as they’re mounted. This will help increase cyber resiliency.

3. SD-WAN protection

As more organisations adopt software-defined wide area networks (SD-WAN), which routes traffic not through private data centres but over public internet connections, the security implications are significant. SD-WAN networks aren’t inherently secure so it’s essential for organisations to add comprehensive network security when they deploy the SD-WAN.

4. Segmentation

One of the most common types of cyberattacks occurs when cybercriminals gain access to one part of the network, such as through a compromised email account, and then work their way through to the entire network. This is the equivalent of using one front door key to access an entire apartment building. Network segmentation can help avoid this situation by requiring users to have the right key for each segment of the network. This way, unauthorised access to one part of the network won’t give attackers access to the entire organisation.

5. Management and analytic tools

Not every organisation can afford the resources required to have maximum coverage. Therefore, it's important to understand where to deploy finite security resources. Security solutions with management and analytic tools can provide more efficient administration, visibility, intelligence, and real-time insights so the security solution has less chance of being misconfigured or overly complex, while ensuring best use of available security resources.

Ilan Rubin said, "Most organisations understand by now that it's not a matter of if they're attacked but when. Hardening the organisation's security posture, maximising the use of existing resources, and improving the organisation's cyber resiliency are crucial to avoid becoming a victim of a successful cyberattack. Organisations should seek help from knowledgeable security partners to determine the right approach for their needs."