Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Why threat intelligence is essential to keep SMBs cyber secure

Small and medium businesses (SMBs) that believe they are immune to cyberattacks because of their size are quickly realising that they're just as much at risk as any other business. And, because SMBs often lack the resources for a comprehensive and robust security posture, cybercriminals may be even more inclined to target them. Therefore, SMBs must employ threat intelligence to help guide their cybersecurity strategies to ensure investments are directed to the right areas, according to Fortinet distributor, Wavelink.

Ilan Rubin, managing director, Wavelink, said, "SMBs need to understand the sophistication and severity of the threats they face. Cybercriminals are constantly improving their attack methods and are focused on mobile and Internet of Things (IoT) targets. Given SMBs face an ongoing cybersecurity skills shortage, often rely on point products and legacy solutions, and tend to have less training and less-strict cybersecurity hygiene, many SMBs are vulnerable to attack."

To ensure a strong security posture, SMBs need to stay ahead of the modern threat landscape. This means choosing solutions that offer comprehensive threat intelligence capabilities that identify modern threats across the network. Effective threat intelligence will include global and local information for best results. This will let organisations determine where to allocate resources for best protection. Doing so is essential to overcome the key threats facing SMBs. These include:

Threat development

Attackers are evaluating the effectiveness of attacks including the costs involved in creating and modifying attack methods. Research has shown that, in the third quarter of 2018 alone, unique malware variants grew by 43 per cent while unique daily malware detections rose 62 per cent. (1)

Mobile and IoT

Emerging technologies help smaller organisations compete against larger enterprises on a more level playing field. However, unless properly secured, they can open up significant threat vectors. The same research showed 26 per cent of all detected malware was mobile-based.

Cryptojacking

Modern cryptojacking attacks have risen 38 per cent, and can disable existing security solutions, exposing networks to attack from other sources. (2)

Encrypted traffic exploits

SMBs tend to assume that encrypted traffic is secure. However, encryption alone isn't enough and there has been an increase in the Pushdo botnet that is used to spread DDoS attacks across networks leveraging SSL-encrypted traffic. (3)

Ilan Rubin said, "SMBs should work with an expert security partner to ensure they're aware of the threat landscape and how they can protect themselves as risks continue to expand and worsen. They should also be aware that there are now suitably priced and scaled security solutions available that address the key threats facing SMBs."