Wavelink
Global Technology | Local Knowledge

MEDIA ALERT

Securing wireless networks in the Internet of Things (IoT) era

Organisations must make strategic changes to effectively secure wired and wireless LANs while supporting business applications for use on mobile and desktop devices alike. This means taking a 'mobile-first' mentality, according to Wavelink.

Ilan Rubin, managing director, Wavelink, said, "IT organisations face constant change, which only seems to be speeding up with technology transformations such as the Internet of Things (IoT), anything-as-a-service (XaaS), and artificial intelligence. Security has always been important but it has become more complicated to secure wireless networks in the face of these new technologies.

Deploying ad hoc security is no longer good enough; enterprise networks need a secure access architecture for end-to-end protection."

Wavelink has identified three key steps for IT teams looking to improve security:

1. Review access layer security
Mobile workers use multiple devices to access mission-critical applications. The addition of IoT devices introduces new security challenges, with unsecured wireless devices being connected to networks. The nature of IoT devices means that, if they're hacked, the consequences can be significant, resulting in equipment failure, financial losses, and even personal injury. The burden is on the network to keep these devices secure.

2. Consider new access layer defence strategies
Most organisations already have basic defences in place, and should add intrusion prevention and application control for maximum protection. Defence strategies should include policies that cover all devices across all environments, mitigating the risk of users unintentionally creating openings for attacks. Technologically, companies should have multiple layers of defence, such as internal network segmentation, which makes it difficult for attackers to spread widely across the network including:

• Wireless intrusion protection (WIP) systems to safeguard against rogue devices, unauthorised access, and ad hoc networks.
• Next-generation firewalls (NGFW) to fight advanced threats and respond to new cybercriminal tactics.
• Visibility and control tools to enable configuration and management via an integrated, end-to-end security strategy.
• Continuous scanning for malware to prevent access to malicious websites, end-point integrity checking and controlling application usage.

3. Select a secure WLAN solution
Companies need to implement multiple layers of defence against the increasingly sophisticated and persistent threats facing organisations. The security strategy should include an integrated wireless solution where control and security are combined in a single portfolio. All network components should be included: wireless; switching; and security.

Ilan Rubin said, "Companies should look for the most flexible WLAN options to mix and match deployment models for different use cases, locations, and IT resources. The solution you choose needs to match your network and organisational structure, delivering the functionality and access you need without sacrificing protection. An integrated, end-to-end solution is more secure, scalable, and cost-effective than piecemeal solutions.

"Additionally, IT administrators need a single pane of glass view now more than ever to simplify the

deployment and management of enterprise networks, applications, and devices.”

About Wavelink
Wavelink specialises in the supply, marketing and support of a range of leading edge Enterprise Mobility and UC Solutions. Wavelink distributes a range of products from Spectralink, Fortinet, Extreme Networks, COBS, Digium, Polycom and Purple WiFi. For more information please contact Wavelink on 1300 147 000.