Wireless becomes key integrated component of enterprise systems

Wireless networks have traditionally been viewed and managed as an 'add-on' to the corporate network, but new security threats demand that they now be integrated into the heart of the enterprise, says Fortinet.

The traditional approach to enterprise wireless was to treat it as an independent system and little more than an access point to enterprise systems, secured by user authentication. But times have changed, says Paul Williams, Country Manager – Southern Africa at Fortinet.

"The traditional approach meant users had to log on again every time they changed location. Traditional solutions required multiple SSIDs and came with challenges such as latency, chatter and authentication and management complexity," he says. "Now, security is of paramount importance, but at the same time, users are increasingly mobile. They want seamless connectivity as they move across various locations in the enterprise, or around large educational campuses. Hot desking is on the increase and enterprise users expect their profiles to move with them, without needing to disconnect and reconnect as they move from place to place."

In addition, growing global information security threats demand more granular management and control of the enterprise wireless infrastructure. "Enterprises and large organisations today have to create 'stickiness' behind the Wi-Fi network," says Williams. "The network must do more than just accept a user name and password – it must allow for user, device and even application authentication, support extended connectivity via a single SSID, and enable seamless management and control as an integrated component of the larger enterprise network."

Fortinet's Infrastructure Wireless portfolio, launched late last year, is the company's next generation solution to wireless network security and management. The cyber security leader now brings to market intelligent enterprise wireless solutions set to address the connectivity and mobile workforce challenges faced by enterprises today.

"We have broadened our solutions portfolio for the enterprise Wi-Fi market with integrated and intelligent secure wireless solutions, which address the challenges of latency, chatter and authentication complexity," Williams says.

"Our intelligent enterprise wireless solutions offer enhanced visibility with management from single pane of glass, certain cost savings through an implementation time reduction of up to one-third, and improved ease of use. South African large distribution warehouses, education faculties and large enterprises are seeing a compelling case for the intelligent enterprise wireless solutions," he says.

Large enterprises seeking integrated, enhanced security and improved productivity are now looking to advanced, intelligent enterprise wireless solutions to support their mobile workforces, he says.

Likewise educational institutions and schools are taking the advanced enterprise wireless approach, both to secure their systems and to support digitised education strategies.

Not only do Fortinet Infrastructure Wireless solutions extend the full force of enterprise security across the wireless network, they also support resource management and audit, allow for instant identification and blocking of rogue devices, and even support control of internet access by certain users and devices, at certain times.

Fortinet Infrastructure Wireless solutions form part of the Fortinet Security Fabric architecture, which integrates all network security components and allows them to react to threats in a more cohesive, proactive way.

For more information: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SG-SAA-Enterprise-Network.pdf

/ENDS.