Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

How to find out if your healthcare data is safe

With more personal health-related information being stored digitally, cybercriminals see healthcare systems as a potentially-lucrative target to attack. Healthcare organisations need to keep this sensitive data safe by assessing the threat landscape and the organisation's own security posture, according to Wavelink.

Ilan Rubin, managing director, Wavelink, said, "Data security isn't a new topic but people are becoming more acutely aware of the intensely private data being stored by healthcare organisations specifically. It's important for healthcare providers to assure customers that their data is, indeed, safe and secure."

There are three key actions for healthcare providers to ensure data is secure:

1. Create a culture of security awareness

Patient data tends to be constantly in use, which puts it at risk from user error and general carelessness as well as hacks via phishing scams or external devices. It's therefore essential to train healthcare and administrative staff to be aware of cybersecurity.

Ilan Rubin said, "Human nature makes people feel invulnerable, which leads to complacency. IT teams need to make sure everyone in the organisation practices good digital hygiene. This means leading by example, regularly scheduling data training sessions to keep everyone aware of the latest threats, holding random inspections to make sure everyone is complying with policies, and recognising success while remediating failure. Combined, these actions will help instil a security-conscious culture in the organisation."

2. Choose the right data security solutions

Having the right cybersecurity solutions in place can help deter, detect, and prevent threats. Healthcare organisations should start with a cyber threat assessment to understand the specific risks the organisation faces. Then, they need to validate the network's current security accuracy, analyse traffic across the environment and monitor network performance.

Ilan Rubin said, "Understanding the current position lets organisations decide what they need to do to address any vulnerabilities or gaps. Healthcare businesses should go through this assessment and investment process regularly because threats are always evolving."

3. Ensure security tools and policies support healthcare technology transformation

Technologies like the Internet of Things (IoT) are likely to dramatically affect the healthcare industry and it's essential to ensure the IT network can support new technologies securely. Connecting both wireless and wired devices to the network creates new potential entry points for cybercriminals, so IT teams need to protect them against the next wave of attacks.

Ilan Rubin said, "Healthcare organisations should consider a security solution that hosts a centralised architecture and an established advanced threat protection framework that can be accessed and managed in one place. Next-generation security solutions, such as those delivered by our vendor Fortinet, can help keep healthcare data protected and let providers expand new patient care delivery models leveraging new technologies."