Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

How to effectively address security challenges in a digital healthcare world

Like most other industries, healthcare has gone digital, making it a key target for cybercriminals looking to obtain sensitive personal information or make money through ransomware attacks. It's therefore imperative for healthcare organisations to maintain organisation-wide security through up-to-date and automated models, according to Wavelink.

The average cost for each stolen or lost record for Australian organisations is $139. Healthcare is the most expensive industry for data breaches globally, costing more than 2.5 times the global average across industries. Australian organisations currently take more than five months on average to detect an incident. (1)

Hugo Hutchinson, Wavelink's national business development manager for Fortinet, said, "Healthcare organisations need to be aware of their responsibilities to protect patients' privacy and they need to stay on top of the threat landscape so they can take the most appropriate steps to protect the organisation. It's therefore helpful to talk about the 'security fabric', which is a multi-layered approach that can include firewalls, cloud security, advanced threat protection, application security, access management, network operations centres, and security operations centres.

"Organisations should consider the fabric model because it delivers end-to-end control of the entire network even as it changes, as opposed to point solutions that can quickly become obsolete. The fabric approach speeds up threat analysis and response because it doesn't require a central management system. In fact, it integrates and shares information among external solutions."

The number of people and devices that need to access the network in a healthcare organisation can be high, making it hard to keep track of who is being given access to what parts of the network. Employees, patients, and visitors are all likely to use their own devices to access network services, along with the organisation's owned devices. Managing all of these disparate endpoints is therefore challenging.

Hugo Hutchinson said, "Best practice is to enforce access policies for all users and devices. This requires micro-segmentation of the network using internal network security firewalls so people can only get into the parts of the network that they're authorised to access. Using a fabric approach, healthcare organisations can exert even more specific access control with the agility to change as the organisation's needs change."

While it's essential to have strong security policies and processes, it's equally important that these don't hinder the organisation from providing excellent patient care. This means applications need to perform as expected or better, without being compromised by slow packet processing, content inspection, or policy management processing. A fabric approach speeds these processes up so users don't notice any difference in application performance.

This can be enhanced with automated security processes that eliminate the need for human intervention into security incidents, saving time and keeping networks up and running.

Advanced threat protection is key to minimising the risk of a successful cyberattack. This can take the form of sandboxing, which creates an isolated, secure environment to validate incoming threats then shares threat information with the security community to disrupt zero-day threats.

Hugo Hutchinson said, "Threats are emerging and evolving too fast for manual processes to keep up. Organisations can't expect to adequately fight the growing threats just by throwing more resources at

them; automation is the only answer. It's faster and less error-prone than humans, and it's better at prioritising threats so organisations don't spend time fighting every apparent threat.

"An automated system means security staff can work on minimising vulnerabilities and educating staff to help reduce the impact of human error on the organisation's security."

Reference:

(1) 2017 Ponemon Cost of Data Breach report