Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Why businesses must take a risk management approach to supply chain security

Organisations that use supply chains need to be aware of the cybersecurity risks created by vulnerabilities in upstream or downstream partners. Often, the lack of security is unintentional. A supplier may unknowingly leave security gaps in information, which is then incorporated into the organisations' systems and may be exploited by malicious hackers. It's essential for organisations to work closely with their supply chain partners to overcome these challenges, and to secure the supply chain, according to Wavelink, distributor of Fortinet security solutions.

Ilan Rubin, managing director, Wavelink, said, "CISOs and other leaders responsible for security can be forgiven for being frustrated by their limited control over supply chain activities. Supply chains tend to be dynamic, highly complex and fluid. And, with no easy way to predict where an attack might come from, this makes the job of securing the organisation even harder."

This challenge is equally confounding for small and large businesses. While small organisations don't tend to have the required resources to conduct due diligence throughout the supply chain, large organisations tend to have such disparate and complex supply chains that conducting due diligence is similarly challenging.

However, the more complex the supply chain, the more important it is to have a strong security foundation. And, even though CISOs can't necessarily control all the actions of supply chain partners, they're still responsible for securing the organisation, so they must pay careful attention to the supply chain.

CISOs should start by creating a risk management plan pertaining to the supply chain before determining what areas to focus on and where some risk may be acceptable. Characterising risk based on its consequences is a useful way of determining what is acceptable and what must be mitigated. Organisations can then start to plan their security measures.

Ilan Rubin said, "Organisations should protect information based on its value. This means it can segment its assets to protect the crown jewels more effectively and without wasting resources. This approach can also restrict the scope or spread of compromised supply chain systems.

"Open up a conversation with all partners about supply chain risks and security best practices to ensure that everyone in the supply chain is working towards the same goal of security. This can help overcome factors such as human error, which is often a significant contributor to data breaches. Just by being aware of the need for security best practices, organisations can reduce the risk of people inadvertently creating vulnerabilities.

"While mitigating the risks across the supply chain can seem overwhelmingly difficult, it is essential to take a risk management approach that minimises the dangers. This might involve incorporating a security fabric approach, which delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises."