



A self-healing network starts with a self-healing partnership.

Written by Juha Saarinen
– iTnews

To efficiently and securely transform your network, embrace self-healing AI.

The architecture of the typical corporate network has changed completely over the past few years, and rapidly too, thanks to cloud computing, mobility and remote working.

Essentially, many organisations now operate a hybrid-everything environment which meets their business needs, but which also poses the risk of increased management and monitoring burden due to added complexity and lack of end-to-end visibility.

What if you could make the networks that underpin the hybrid-everything environment self-healing, using artificial intelligence and machine learning?

“Typically, we detect something, then you diagnose and respond to disruptions,” NEC Australia’s National Portfolio Manager Pankit Mehta said.

“What if you can do that without human intervention,” Mehta said, defining how far the self-healing network concept goes.

Here, Cisco’s Catalyst Centre network management tool can be used to provide insights, automate common tasks, predict and act on failures, and monitor performance.

A three-dimensional map in Cisco’s Catalyst Centre provides a visualisation of the workspace, for wireless network analysis.

This 3D Wireless Analyser models walls, obstacles and building materials that can hinder WiFi signal propagation, manage access points to ensure they’re not interfering with each other and detect problems and provide resolutions suggestions for them.

With Cisco Catalyst Centre, admins can plan ahead and set up simulations to work out how to get the best possible coverage from the smallest number of access points, which saves both time and money.

When problems happen, in literally mission-critical works like in hospitals, the management system can be substantially faster to resolve issues by itself, automatically, without the lengthy intervention of staffers that need to diagnose faults first.

“Rather than human intervention where a support technician looks at diagnostics, wastes their time on it and more, self-healing is a concept where the system itself would detect that the device’s faulty,” Mehta explained.

“The system would then order a new one. It can even ask for the device to be shipped because it logs a ticket that is actioned. The device is then shipped the next morning when it’s business hours, somebody comes in, and swaps out the faulty device for a working one,” he said.



A setup like that is substantially less manual than a support staffer getting a pager buzz in the middle of the night, or waiting until the next morning to identify the problem.

With artificial intelligence and machine learning, a self-healing network can reduce downtime, improve reliability, save on costs and be more secure, Mehta said.

Thanks to ML, security on self-healing networks can accurately categorise observations of threats without explicit programming and act to keep users safe. By constantly monitoring networks for anomalies, the AI can detect events out of the ordinary, like unknown malware, insider threats and policy violations.

The Cisco systems NEC deploy use AI to provide safe browsing for users, predicting where the “bad neighbourhoods” on the Internet are and stop connections to malicious websites. Endpoint malware detection, which can be existing and new malicious code, can also be detected with AI/ML, even in encrypted traffic through algorithms that find patterns associated with hidden threats.

The challenges for organisations is that while the self-healing concept is not a tough sell at all as it’s very easy to demonstrate the benefits of that approach, it is very hard to integrate AI/ML into legacy networks.

“There is a lot of dependency on vendors delivering hardware that is compatible,” Mehta said.

“Regulatory compliance is another consideration. If you play with the device to make it compatible or something, it would void the warranty. This could lead to support for the device being dropped, which is not what any customer wants,” Mehta said.

So-called “forklift upgrades” with device replacement are usually necessary for organisations to ensure the best compatibility and support for AI/ML technology, Mehta said. And, there’s a time for when that can happen.

“Typically that sort of discussion happens when the customer is near the refresh cycle,” he said.

“Obviously there are discussions prior to that to give them a taste of why it's going to be better for them, but I think the serious discussion where they get an idea on what that cost would look like and so on is best done near a refresh cycle, and we’ve seen a high adoption rate.

“I don't see any customer saying no to it. I think the majority of the customers are keen, it's the fastest growing segment for us and the majority of the customers want that,” Mehta added.

NEC

