



HPE aruba
networking

HPE Aruba Networking Central with AI Ops

Do you really know what's on your network?

HPE 
GreenLake



Known endpoint clients are just the beginning

An increasing reliance on IoT (Internet of Things) for business efficiency, automation, and digital transformation comes with risks due to an expanding attack surface that's difficult to control. IT teams need better visibility and profiling information that can be used for automated risk-based segmentation—for the known endpoints connected to the network as well as the unknown clients. It's impossible to keep up without help.

Unknown clients and their unforeseeable concerns

The endpoints connected to your network often lead to connectivity and security issues, which then lead to help desk calls. For simplicity, unknown clients are sometimes given broad access privileges so as not to hamper the user experience. While ensuring a positive end user experience is admirable, it leaves your network open to a variety of issues that include internal and external attacks.

In addition to security concerns, IT teams often lack information about the type and amount of traffic generated by unknown clients. Problems are compounded as networks grow. In more distributed environments, it is very difficult to control what users are connecting onto the network and appropriately enforce usage policies.

Automated and accurate client insights are critical.

HPE Aruba Networking Central with AI-powered network and security insights

Luckily there's help. We include ML-based classification of traditional endpoints and IoT devices that goes beyond basic profiling. Our algorithms use dynamic comparisons and MAC range classification to determine what type of endpoints clients are connected. In the likely event that unknown clients are found, you can easily create a simple enforcement rule that limits what they can and cannot reach.

What makes HPE Aruba Networking Central unique? We are the only vendor to build in this level of AI-powered client visibility and accuracy into a cloud-based network management, inventory, and troubleshooting solution. No extra appliances, cost, or management burden.

When it comes to your network, why guess? HPE Aruba Networking delivers full-service network to client AI networking security features that give you the ability to build a better network. An AI networking feature set that you can use to optimize, as well as troubleshoot network and security issues before they turn into help desk and user experience problems—all from a single dashboard.



A real-life example

Without accurate client visibility, IT teams sometimes run into unexpected issues during a network refresh. They often find a greater number of known and unknown endpoints and applications being used, all of which are using more bandwidth than expected. This was the case for an IT team at a large retailer customer with over 5,500 sites. They were concerned that unexpected client and traffic variances would hamper their weekly roll out of new HPE Aruba Networking EdgeConnect SD-Branch Gateways and APs across 100 stores.

Would everything work or would they run into new bandwidth and security issues?

To make it easy on users, known and unknown endpoint clients were often given broad access privileges as IT found it difficult to differentiate between customer endpoints and sales and building-oriented IoT devices. Not only was this a network configuration issue, but it carried over into firewall rules and access policies as well. Outdated and manual methods of identifying endpoint clients were no longer going to work.

Fortunately, their timing was perfect. As part of the new infrastructure roll out, the customer also deployed HPE Aruba Networking Central Cloud. Their new management software has AI-powered Client Insights visibility and classification built-in. No need for a separate collector, third-party software, and extra management interface. Now each Wi-Fi or wired endpoint that connects is dynamically profiled and placed into a category of known clients to simplify the assignment of access privileges. The end result is better visibility for network and security purposes.

The magic is the ML techniques used to help identify endpoint clients with unknown characteristics. The IT team now has over a 95% confidence level that they know the type of endpoints coming into their stores and their intended use. The visibility allows them to create access policies 60% faster, while directly improving network security and application performance.

Summary

When it comes to digital transformation, rolling out new services, and effectively meeting your secure networking objectives, inline telemetry, cloud-based management, and automation with granular visibility are the future. AI-powered Client Insights along with other AI networking tools included in HPE Aruba Networking Central are just one step in delivering the best user experience possible.

HPE Aruba Networking AIOps. Data from millions of devices. Expertise you can trust.

www.arubanetworks.com/AIOps

Make the right purchase decision.
Contact our presales specialists.



Contact us

Visit ArubaNetworks.com

