aruba
a Hewlett Packard
Enterprise company

ARUBA AIOPS USE CASES

AI-powered IoT profiling at the Edge for Hospitality

INTRODUCTION

The last few years have seen an unprecedented growth in IoT adoption across industries. As IoT clients are not fundamentally trustworthy, they can become the “Achilles heel” of an organization. If not identified and profiled, broad access privileges can result in security breaches and harmful implications, including erosion of customer loyalty. Complete client visibility is essential. After all, you can’t protect what you can’t see!

CHALLENGE

IoT clients are collectively the eyes and ears of every hyper-aware facility. With the large influx and variety of these clients, traditional techniques that require collectors and agents for identification and profiling are no longer scalable. Since many IoT clients are built on common Windows or Linux software, it is difficult for IT teams to accurately identify and apply appropriate policies and access privileges. Legacy solutions also lack the ability to analyse client attributes such as traffic destination, protocols and communication frequency that can help pinpoint the identity and role of endpoints — forcing organizations to manage multiple tools that lack integration.

This can cause IT teams to incorrectly identify and assign policies using manual and siloed tools that are unable to share data for granular enforcement. The result is poor user experience, increased cost and complexity, and operational inefficiency.

SOLUTION

In today’s world, accurate classification and profiling of endpoints requires AI and machine learning (ML) to eliminate blind-spots and improve the overall security posture of an organization. To help, Aruba has included AI-powered Client Insights within Aruba Central at no additional cost, providing customers with a comprehensive view of the network, endpoints and traffic generated with a single solution. This enables organizations to use the data provided by their networks to respond to security and network challenges more efficiently.

Client Insights offers profiling accuracy of up to 99% with a success rate that delivers fewer than 5% of “unknowns”. The key is that Client Insights natively uses telemetry gathered from Aruba APs, switches, and gateways without the need for physical collectors that add complexity.

Our continuously re-trained ML models have access to over 120K customer sites and 200M+ clients to ensure that older as well as newer devices are being accurately identified.

Client Insights also lets IT teams tag and group similar devices for end-to-end policy assignment which has led to time savings and automated workflows thereby improving efficiency and generating better end-user experiences.

A REAL-LIFE EXAMPLE:

Digital transformation in the hospitality industry requires IT to support superior guest experiences. Guests expect seamless connectivity with smart, immersive, and personalized experiences. Imagine a scenario where you have an important business meeting and hotel Wi-Fi issues result in sub-optimal video and audio call quality. You'll probably stay elsewhere the next time.

As a consumer-centric business where user-experience plays a pivotal role, a large chain with 6000+ hotels across the globe required a better way to configure and monitor a plethora of IoT and other unknown clients connected to their network. Most of their customers are families staying for leisure where many bring wired gaming devices.

For wireless BYOD, guests could use a captive portal and easily onboard themselves. But most gaming devices do not support captive portal login and a manual and cumbersome process that required IT intervention was required. The MAC address of these devices had to be provided to the hotel's IT team prior to granting them connectivity.

This process led to a 15% increase in helpdesk calls on an average. Approximately 1000 hours yearly was spent on identifying, onboarding, and assigning policies for all type of gaming devices brought in by customers, thus making the process unscalable and error prone.

With Client Insights, the IT Team was able to automatically profile, identify the applications accessed and destination ports of these gaming devices, allowing them to bypass the captive portal and manual intervention by IT. The attributes such as applications accessed, communication frequency and traffic destination helped the IT team set appropriate policies, identify anomalous behaviour and quarantine malicious devices if required.

By taking a holistic approach where Client Insights and Network Insights work together, they were able to collectively save approximately half a million dollars, eliminate the 15% increase in helpdesk tickets and reduce the time spent to resolve network issues by up-to 90%.

SUMMARY

User experience, loyalty and trust directly translate to revenue for any industry. The objective is to create a zero-trust defensive framework with a comprehensive view of endpoint, application, and network performance. Organizations should not only support managed and unmanaged endpoints but ensure that IT teams have the required visibility to onboard these devices in a simple and secure manner. To experience the best of both worlds, AI-powered Client insights offers the most granular visibility and accurate profiling on wired, wireless and WAN networks.

Aruba AIOps. Data from millions of devices. Expertise you can trust. Powered by Aruba ESP.

www.arubanetworks.com/AIOps

aruba
a Hewlett Packard Enterprise company

Contact Us