

EXECUTIVE BRIEF

IDENTIFY, CONNECT AND PROTECT MOBILE AND IOT AT THE EDGE

INTRODUCTION

The sheer number of IoT devices connecting to enterprise networks creates challenges for IT as they balance the benefits of smart buildings with the risk of onboarding lots of unknown devices to their environment, without having the right set of tools to automatically identify, profile, authenticate, and apply policies to those devices.

Aruba's latest announcement tackles these challenges with a 4-step approach to IoT connectivity at the edge: Identifying what's on the network, connecting mobile and IoT devices with intelligent switches, protecting the network with industry-leading policy management, and innovating via our partner ecosystem to provide end-to-end security.

IOT BRINGS CHALLENGES

The explosion of mobile devices and the move to smart buildings brings significant challenges to IT and business leaders.

Lack of visibility—do you really know what's on your network?

Security starts with understanding what's on the network—unmanaged smartphones, rogue endpoints, IoT devices. These all increase the attack surface and threaten enterprise security. The ability to see what's on a network gives IT a better understanding of how their network is being used and by what. IT must be able to identify and profile every device that is connecting to the network, regardless of where it's connecting from. This becomes more challenging as unknown wireless and wired IoT devices flood our networks. All devices need to be profiled and assessed upon connectivity, assigned to a category, with access automatically granted or denied based on device type, ownership status, or operating system.

Wired is the new worry.

For organizations in the enterprise and industrial space, the number of expected wired IoT devices can range from 35% to over 50% depending on the vertical—motion detectors, medical equipment, process controllers on the factory floor, to name a few. In the past, network access control (NAC) discussions mostly centered on how to secure the wireless network because that's how most devices were connecting. Secure, per session connections became a requirement as wireless eavesdropping and unknown users could establish access from anywhere within range of an access point and unsecure SSID.

The heavy focus on securing wireless networks meant that wired networks were left unprotected as switches sat behind locked doors and the perception was that they didn't exhibit the same vulnerabilities as wireless. Unfortunately, as wired networks grew, consistency across many switches wavered, leaving ports wide open and accessible by anyone. Ports in conference rooms and printer areas are a classic example where "hit or miss" security exists. With many IoT devices connecting via wired, it's time for the same level of attention to be given to securing the wired infrastructure.

Traditional wired infrastructures were not optimized for IoT

In legacy switching environments, the workforce was not mobile and IoT was not a thing yet (no pun intended!). Assets lived behind the firewall and IT just had to make sure that the perimeter stayed strong. Now enter IoT—the wired infrastructure needs to be as smart as the wireless one — today's switches need to have security and smart network management integrated so that all of these devices can connect securely and seamlessly.

Protecting the network requires automated workflows

With the thousands of unknown mobile and IoT devices connecting to an enterprise network on a daily basis, it's impossible to manually assign and enforce policies that account for each device. The whole process must be automated to reduce risk with minimal hands-on effort from IT. Static devices and the infrastructure itself should also be profiled and automatically checked to look for suspicious changes. If a device is acting suspicious, it should be automatically quarantined until the threat is assessed.

It's expensive to stay ahead of the hackers

It seems that we hear about massive data breaches on an almost daily basis. It's expensive and time-consuming for companies to invest in security and it's almost impossible to keep ahead of the hackers by innovating alone. Aruba's partner ecosystem is designed to bring together best-of-breed security partners to provide an end-to-end security solution.

ARUBA'S BLUEPRINT FOR SECURE IOT CONNECTIVITY AT THE EDGE

1. Identify and profile unknown devices on multi-vendor wired and wireless networks

Given that network security starts with knowing what's on the network, it is essential for organizations to be able to identify and profile all devices. Aruba's ClearPass family offers a unique advantage versus the competition as real-time, agentless profiling can be acquired as a standalone appliance or within a comprehensive policy enforcement solution.

Both solutions allow you to continuously identify endpoints, and network devices on non-AAA or AAA enabled wired and wireless networks — whether via dynamic or static IP addresses. Comprehensive dashboard visuals make it easy to see the total number of endpoints, and the number by category, family and device type.

The new Aruba ClearPass Universal Profiler is a standalone virtual appliance that can be deployed and running in minutes, and is designed for those organizations that are not ready for a complete NAC solution, or for remote or restricted areas where NAC has not been deployed. The Universal Profiler is a simple and cost effective way to identify and profile what's on the network.

Aruba ClearPass Policy Manager is a virtual or physical appliance that includes comprehensive profiling, non-AAA and AAA wired and wireless policy enforcement, guest access, BYOD onboarding, endpoint assessment capabilities, reporting, and built-in third party security and user experience oriented solution integration.

2. Connect IoT devices with automated intelligence

The move to smart buildings means that today's businesses need a smarter wired infrastructure. The latest enhancements in ArubaOS-Switch are designed to power and secure the intelligent edge, optimizing for mobile and IoT devices. These enhancements enable unified role-based access across wireless and wired networks with the ability to identify and assign roles to connected IoT devices in order to prioritize business critical applications and secure the network.

The Aruba layer 3 switches are also capable of user-based and port-based wired traffic tunneling to a Mobility Controller so that policies can be applied, advanced services can be extended and traffic can be encrypted to secure the LAN. In order to meet the demand for the rapid growth in IoT and connected devices in distributed enterprises, the cost-effective Aruba 2540 (as well as the other Aruba switches) support Zero Touch Provisioning and optional cloud-based management to allow enterprises to simplify and slash network deployment and management costs.

3. Protect the network with smart policies

Once you have device visibility, automatic policy enforcement comes into play. Aruba ClearPass Policy Manager can help you see what's on your network and then enforce policies and automated workflows across multi-vendor wired and wireless infrastructures. ClearPass delivers profiling, policy enforcement, guest access, BYOD onboarding, and more to offer IT-offload, enhanced threat protection, and a seamless user experience. And with a new focus on securing the wired infrastructure, the OnConnect feature uses existing switch protocols, helping you lock down wired ports in vulnerable places like conference rooms, IP phones, and in printer areas.

4. Speed up innovation to improve security at the edge

Aruba's technology ecosystem includes industry-leading security solutions that integrate with ClearPass Exchange to ensure end-to-end security at the edge and core. Our latest partnerships focus on IoT security:

- Niara uses known traffic patterns associated with device types to identify suspicious behavior and then asks ClearPass to remove the device from the network.
- Attivo allows IT to create "fake virtual" IoT devices where people try to use the fake devices to attack a network. Once the virtual device is seen performing unwanted behavior, they ask ClearPass to pull devices off of the network.

CONCLUSION

As organizations increasingly embrace IoT into mainstream operations, the onboarding and management of IoT devices becomes critical to success. Companies need a strategy to securely connect mobile and IoT devices at the edge, to extract the value and efficiencies associated with smart buildings while keeping the network and corporate assets safe. Aruba's 4-step approach to IoT connectivity tackles the challenges of identifying what's on the network, connecting devices via smart wired and wireless infrastructures, protecting the network with automated policy management, and using our partner ecosystem to boost end-to-end security to keep ahead of the potential risks.