SOLUTION OVERVIEW

ACCESS POINTS AS IOT PLATFORMS

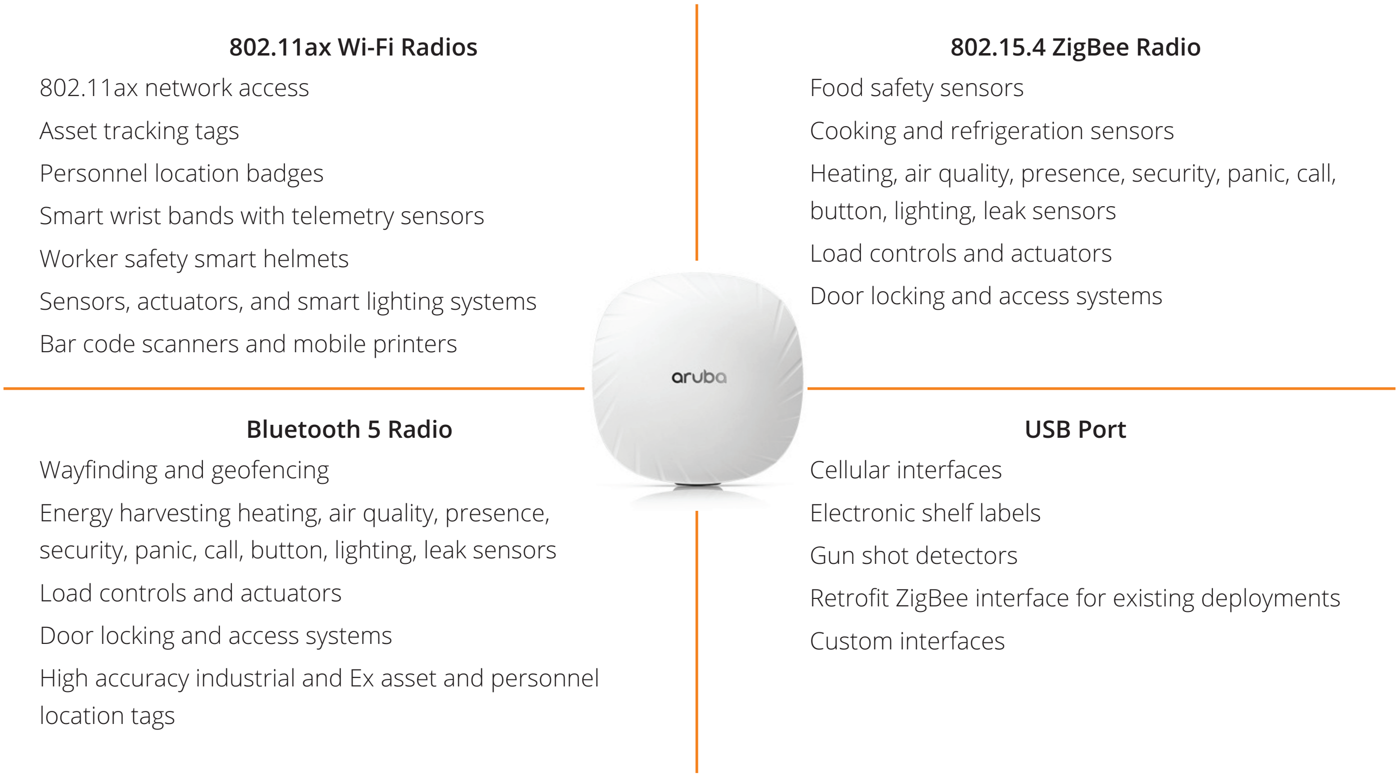
Bridging IT and OT networks

EVOLUTION OF THE PLATFORM

The introduction of Wi-Fi 6 (802.11ax) has expanded the role of an access point (AP) to encompass not only secure Wi-Fi connectivity, but also enhanced IoT capabilities that span Wi-Fi 6, Bluetooth 5, 802.15.4 (Zigbee), and third party functionality via USB. Taken together, new use cases such as wayfinding, geofencing, push notifications, and asset tracking transform Aruba APs into secure, multi-purpose communication hubs that are both network access on-ramps and full-fledged Internet of Things (IoT) platforms.

THE ARUBA ADVANTAGE

- Multiple IoT radios and flexible USB port address broad range of IoT applications
- Ideal positioning and coverage for IoT RF and IR devices
- Maximizes battery life of IoT devices
- Indoor, outdoor, and ATEX Zone 1 options
- Reduces reliance on stand-alone IoT gateways
- Minimizes or eliminates the complexity of mesh networks
- Tunneling, dynamic segmentation, policy management, and anomaly analytics enhance IoT security



802.11ax Wi-Fi Radios

802.11ax network access

Asset tracking tags

Personnel location badges

Smart wrist bands with telemetry sensors

Worker safety smart helmets

Sensors, actuators, and smart lighting systems

Bar code scanners and mobile printers

802.15.4 ZigBee Radio

Food safety sensors

Cooking and refrigeration sensors

Heating, air quality, presence, security, panic, call, button, lighting, leak sensors

Load controls and actuators

Door locking and access systems

Bluetooth 5 Radio

Wayfinding and geofencing

Energy harvesting heating, air quality, presence, security, panic, call, button, lighting, leak sensors

Load controls and actuators

Door locking and access systems

High accuracy industrial and Ex asset and personnel location tags

USB Port

Cellular interfaces

Electronic shelf labels

Gun shot detectors

Retrofit ZigBee interface for existing deployments

Custom interfaces

Figure 1: Aruba Wi-Fi 6 Access Point as an IoT Platform

All manner of low-voltage building systems - including comfort, intrusion detection, energy management, access control, personnel and asset tracking, man-down, call button, leak detection, and even gunshot monitoring systems - can now reliably and securely communicate via Aruba Wi-Fi 6 APs.

IDEAL VANTAGE

From their unique deployments on ceilings, walls, and even under seats, APs have an unobstructed, bird's-eye view of all nearby devices that are ideal for wireless communications.

Bit rates fall proportionately with distance, so to deliver a high- speed user experience Wi-Fi 6 APs are typically spaced at 12-15 meter intervals in open areas, and often one per room.

This spacing provides optimal coverage for energy-harvesting and battery-operated low power RF IoT devices.

Many ceiling-mounted IoT devices need a local power source, ideally with battery back-up, but powered outlets are not typically found in ceiling plenums, nor are UPS devices.

Aruba APs provide a simple solution to the IoT power issue: a USB port provides a convenient source of both power and high-speed data without new cable runs or equipment.

For Wi-Fi based, battery-operated devices, Aruba's Wi-Fi 6 APs support both Target Wait Time (TWT) and 20MHz channel IoT devices. TWT maximizes the sleep time of IoT devices up to several days before a check-in, extending battery life up to 10x longer than previous Wi-Fi technologies. With wake-up time negotiated between the device and AP, TWT delivers a more deterministic, power efficient operating mode. 20MHz operation allows for lower power operation, further extending battery life. And with the ability to support 1,000 IoT devices per radio, the APs can scale to IoT deployments of any size.

Access points are available in wide-temperature IP-66/67 outdoor variations, and with partner-provided polycarbonate ATEX Zone 1 enclosures for outdoor and hazardous location (hazloc) environments. So regardless of the IoT deployment mode – indoor, outdoor, or hazardous location – Aruba has you covered.

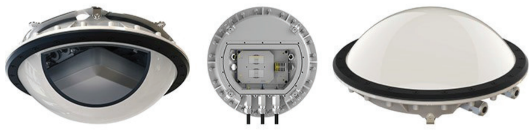


Figure 2: Bartec Polycarbonate ATEX Zone 1 Enclosures for Hazardous IoT Environments

LESS COMPLEX, MORE RELIABLE

Wi-Fi 6 APs eliminate the need for gateways by communicating directly with IoT devices, and bidirectionally tunneling the data to target applications. Eliminating these overlays reduces system complexity and cost, increases overall system reliability, and removes a typically vulnerable attack surface.

By communicating directly with IoT devices, the APs can also reduce the cluster size of IoT mesh networks, if not eliminate them altogether. Mesh backhaul multiplies the bandwidth consumed by every IoT transmission, an effect that is especially impactful in the congested 900MHz and 2.4GHz ISM bands.

Doing away with RF mesh networks, or allowing them to operate in smaller clusters, preserves bandwidth and minimizes the effect on other IoT devices operating on the same frequency. This has the added benefit of increasing the battery life of IoT devices, which don't need to retransmit backhaul packets as frequently, if at all.

ADDRESSING IOT SECURITY CHALLENGES

IoT devices are targeted for attack because they rarely have strong security built in, lack robust authentication, and store passwords in the clear due to price-constrained designs, limited compute capabilities, and design oversights. IoT devices are often located in public areas, and susceptible to probing, manipulation, and network breaches. It's no wonder that vigilantly asserting trust over IoT devices, and actively minimizing attack vectors, are top corporate priorities.

Funneling IoT traffic through Aruba APs and switches allows multiple active and passive security mechanisms to protect IoT devices and their traffic. Trusted Platform Modules in the APs store credentials so probing an access point won't yield authentication, authorization, or encryption details. IoT data are securely tunneled from the APs to Aruba on-premise, virtual, and cloud controllers, with no clear text conversion in the chain.

Role-based policy decisions and access rights segment traffic from the APs to target destinations without complex and static network configurations and VLANs. Aruba's built-in Policy Enforcement Firewall provides deep-packet inspection (DPI) to identify high-risk traffic. For example, a security camera can be limited to communicating only with network resources that are absolutely necessary to perform the function of capturing and storing video.

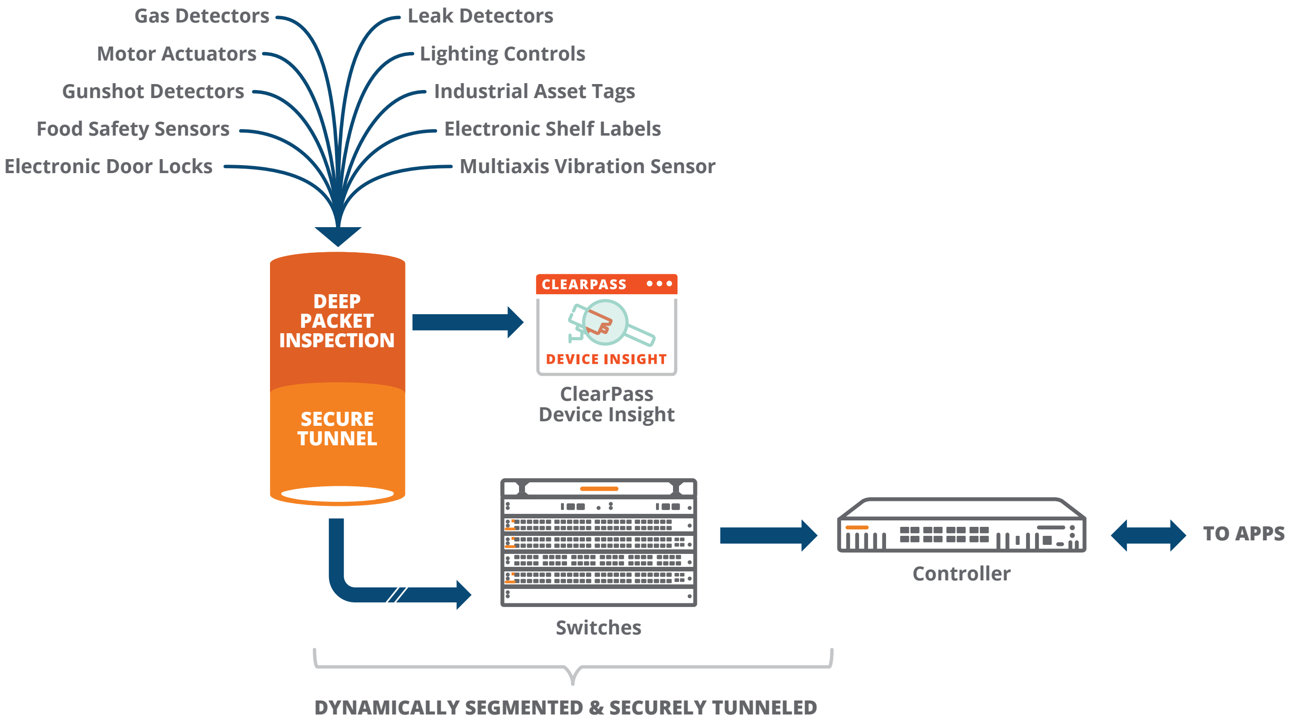


Figure 3: IoT Device Security Funnel

Aruba's ClearPass Device Insight fingerprints devices so they can automatically be assigned appropriate policies using Aruba's ClearPass Policy Manager. In the event that a device exhibits Indicators of Compromise (IoCs), access can be significantly restricted or the device can be quarantined from the network completely.

IoT vendors that bypass the security funnel, by using a LoRa network, put the enterprise at risk by routing traffic around these best-in-class protective mechanisms. Infected or compromised devices may simply go unnoticed as a result.

THE PLATFORM OF CHOICE

Gartner estimates that by roughly 2022 there won't be a noticeable difference between IT and IoT devices because of the widespread proliferation of IoT devices on IT infrastructure. Achieving more reliable and deterministic operation, with uniform security policies and visibility across both IT and IoT devices, requires a new approach to system implementation. Aruba's feature-rich Wi-Fi 6 Access Points are the platform of choice for that transformation.

Learn more about Aruba Access Points.

a Hewlett Packard
Enterprise company