WHITE PAPER

aruba
a Hewlett Packard Enterprise company

DESIGNING HYPER-AWARE RETAIL FACILITIES

SECURE INFRASTRUCTURE AND PARTNER SOLUTIONS FOR DIGITAL TRANSFORMATION IN RETAIL

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

At its core, the Internet of Things (IoT) is an amalgamation of machines in the physical world, logical representations of physical phenomena (such as temperature, flow, speed) acted upon by those machines, contextual data (identity, location, applications in use) generated by underlying network infrastructure, and applications that analyze, monitor, and act upon those data. Supplementing IoT data with contextual information enables applications to become cognizant – or "hyper-aware" – of, and responsive to, the occupants and their environment, service needs, security, and safety. The richer the set of data and context, the more adaptive the applications can become with the ultimate goal of driving revenue. In retail facilities, machines and applications are focused on understanding customer behavior, erasing the distinction between on-line and off-line shopping, improving human productivity, and maintaining health and safety.

Machines, applications, and interfaces are typically tailored to each IoT vertical application. However, the underlying network infrastructure can be designed more extensibly, using a common core set of services that can be applied across virtually any use case or vertical application.

Aruba's Edge Service Platform (ESP) is the first extensible infrastructure to combine information technology (IT), operational technology (OT), and IoT into a single framework with open interfaces and APIs. Third-party devices, applications, and services can use the open interfaces and APIs to plug vertical-specific systems into ESP without having to change the underlying infrastructure. This allows ESP customers to easily support changing IT, IoT, and OT requirements by plugging new systems into their existing Aruba infrastructure – no rip-and-replace needed.

ESP is built on three foundational services, and APIs provide access to technology partner devices and applications that need to access any or all of them:

- Unified infrastructure that encompasses wired and wireless networks, OT/IoT interfaces, wide area networks, and cellular networks;
- Zero trust security framework in which no user or device is granted entry or on-going access until proven trustworthy;
- Artificial intelligence for operations (AIOps) in which multiple AI and big data services are leveraged to continuously detect, monitor, isolate, and remediate issues impacting RUN excellence.

Aruba has built a broad ecosystem of retail technology partners whose products and services interface with ESP to understand customer behavior, enable omni-channel operations, and improve the operation of facilities.

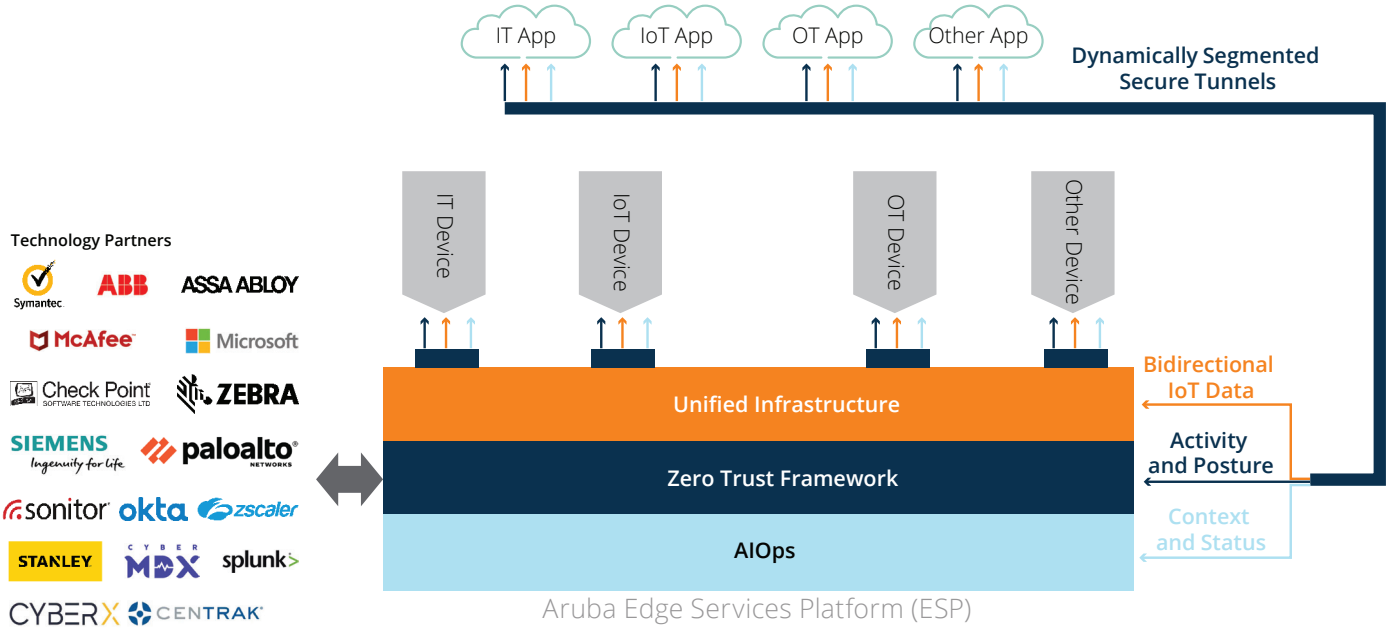


Figure 1: Aruba ESP And Technology Partner Ecosystem: The Foundation For Hyper-Aware Solutions

Solutions from Aruba and its technology partners span the retail market including brick-and-mortar stores, distribution centers, and warehouses in addition to corporate spaces used for business operations. Use cases and partners discussed in this white paper include:

- Improved Shopper Experiences
  - Self-service Shopping and Smart Checkout (Zebra)
  - Understanding Customer Behavior for Layout Optimization and Targeted Marketing (Aislelabs, Kiana, Skyfii, Wavespot)
- Operational Efficiency
  - Dynamic Pricing with Electronic Shelf Labels (Hanshow, SES-imagotag, SoluM)
  - Increasing Inventory Accuracy and Reducing Inventory Shrinkage (Wiliot, Zebra)
  - Enhancing the Reliability and Quality of Mobile Staff Communications (Ascom, Spectralink, Theatro, Zebra)
  - Migrating From Break-Fix To Proactive Maintenance (ABB)
- Connectivity and Security
  - Physical Distance Monitoring and Contact Tracing (AiRISTA Flow, AisleLabs, CohuHD, CXapp, Kiana, SkyFii)
  - Vaping and Air Quality Monitoring (IP video)
  - Gunshot Detection (AmberBox)
  - Context-Aware, Real-Time Integrated Emergency Response and Notification (Meridian and CriticalArc, Patrocinium)
  - Securely Sharing Retail Wireless Networks Without Losing Control (Aruba MultiZone)
  - Seamless 5G To Wi-Fi Roaming Without Distributed Antenna Systems (AirPass)
  - Connecting and Protecting Remote Stores and Workers (VIA, RAPs, SD-Branch)

Information on ESP can be found at https://www.arubanetworks.com/solutions/aruba-esp/. Information on Aruba's technology partners can be found at https://www.arubanetworks.com/partners/programs/.

INTRODUCTION

What is hyper-aware retail, and why is the Internet of Things (IoT) relevant to it? Hyper-aware retail defines an instrumented facility in which applications are cognizant of the contextual status of the environment, occupants, energy consumption, service needs, security, and safety. IoT is collectively the eyes and ears of a retail organization, and generates logical representations of physical data, i.e., temperature, air quality, product on shelves, and occupancy, among many others. These data are supplemented with contextual information generated by the retail's data network, i.e., identity, location, and applications in use. The combination of data and context enables retail facilities to become cognizant of, and responsive to, the occupants and their environment. The richer the set of data and context, the more adaptive the organization can become. Some retail environments have only limited cognizance, while others are fully instrumented and hyper-aware.

Before the advent of interconnected networks, retail systems operated autonomously from each other, with independent point of sale systems, inventory management systems, telephone, fire alarm, security, closed circuit television (CCTV), power management, lighting, and heating/ventilation/air conditioning/refrigeration (HVACR). The protocols, communication infrastructure, and even the means of powering each system were tailored to the specific application: telephony for line-powered handsets; fire alarms to line-powered sensors and long battery life; security for high speed, multi-drop sensors; video for analog signaling over coaxial cable; and so on.

The move to omni-channel – where shoppers have a unified experience across mobile, web, and brick-and-mortar stores is one of the evolutions that has driven the move to digital connectivity. Stores that were exclusively brick and mortar have to compete with on-line rivals. It is through the capture and use of in-store data that retailers will to close this gap. The recent worldwide pandemic and associated stay-at-home and social distancing orders have further accelerated this trend.

In some cases, local regulations have mandated system isolation, fire alarms being a case in point. In other instances, manufacturers have wanted their devices to be isolated because it locks customers into lucrative service contracts. Regardless of the reason, many systems remain isolated and unable to share edge data.

The challenge is that cognitively-aware retail applications need access to edge data to deduct status and infer occupant needs to deliver relevant shopper experiences. For example, an automated push-marketing system needs identity, past purchase history, loyalty club status, and location frequency, recency, and dwell time to know what constitutes a relevant offer and when/how to push it. Trusting IoT systems enough to share context and data is highly problematic.

IoT devices are fundamentally untrustworthy, making them the 'Achilles heel' of retail security. The reason is simple. The engineers who design IoT devices are typically trained on process reliability and application-specific architectures, and their objective is to make products work reliably for as long as possible. Cybersecurity expertise sits with information technology (IT) engineers. Adhering strictly to a zero trust framework, IoT devices should not be allowed on a network unless and until trust can be asserted to the same standard as it is with IT devices.

Addressing the shortcomings of IoT device security isn't a trivial task. The diversity of installed legacy devices is vast; many have been in service for years and predate the advent of modern cybersecurity. Replacing legacy devices is often technically and economically unviable, not to mention highly disruption to on-going operations. Many new IoT devices also lack sound cybersecurity features. For this reason, many CISOs will not permit IoT devices or gateways on their networks, a testament to the scope of the problem.

The goal should be to create a zero trust defensive framework in which no device or user is trusted until proven otherwise. The framework should leverage contextual information from a multitude of sources to scrutinize user and device security posture before and after they connect. Doing so helps overcome the limitations of fixed security perimeters tied to physical boundaries, which break down in the face of IoT devices that can connect and work from practically anywhere.

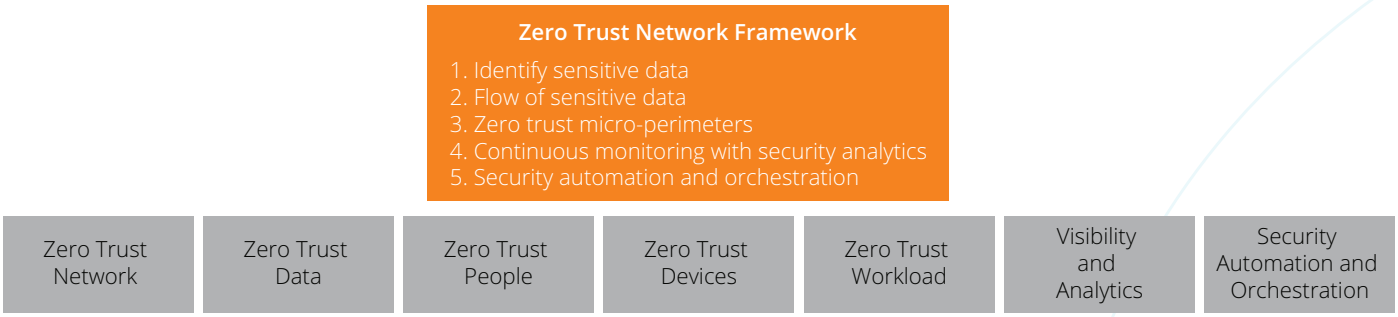


Figure 2: Zero Trust Framework

IoT security should include the layered protective mechanisms in accordance with a zero trust framework:

- Authenticating source/destination devices and monitoring traffic patterns;
- Encrypting data packets using commercial and, where applicable, government encryption standards;
- Micro-segmenting traffic inside secure tunnels to ensure devices communicate only with their intended applications;
- Fingerprinting IoT devices to determine if they are trusted, untrusted or unknown, and then applying appropriate roles and context-based policies that control access and network services;
- Inspecting north-south traffic with application firewalls and malware detection systems to monitor and manage behavior;
- Leveraging enterprise mobility management (EMM), mobile application management (MAM) and mobile device management (MDM) systems to monitor behavior and protect other devices in the event of a policy breach; and
- Relying on AI-based analytics to continuously look for anomalous behavior even after trust has been asserted.

Legacy IoT devices can be identified as known or unknown upon connecting to the network using their MAC address in an external or internal database. The profiling data should flag if a device changes its mode of operation or masquerades as another IoT device – a common issue with MAC-based authentication - and then automatically modify the device's authorization privileges. For example, if a connected smart TV tries to masquerade as a Point of Sale (PoS) device, network access should be immediately denied.

Mitigating IoT security risks requires a blended approach that includes methods taken from mobile, cloud, automation, and physical security. The sheer breadth of IoT solutions mandates an array of embedded trust, device identity, secure credential, and real-time visibility solutions. New and unfamiliar cybersecurity risks include: IoT solutions can change the state of a digital environment, in addition to generating data, and this variability of state requires a new view of cybersecurity; IoT environments include unattended endpoints – locally and in remote sites - that can be both physically probed and logically attacked; and machine-to-machine (M2M) authentication works in newer IoT devices but not in many legacy devices, creating trust gaps between generations of devices and gateways.

The brick-and-mortar retail market has been profoundly challenged by on-line retail competition, and the recent pandemic has only further accelerated the challenges. With the need and incredible responsibility to protect customers' payment method information, cybersecurity has to underpin all retail systems. At the same time, location services play an essential role in many retail applications, including staff and product tracking. Yet neither cybersecurity nor location-based services are core skills of many retail vendors – both have long been the province of IT. And then there's analytics, a family of highly specialized tools that help retailers secure and monetize collected data, which is yet another province of IT.

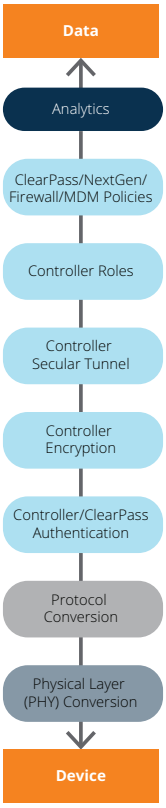


Figure 3: IoT Protection Mechanisms

Bridging the divide between IT and automation vendors is paramount to the successful implementation of a zero trust framework. Aruba's policy enforcement firewall and encryption, working in concert with secure tunneling and the ClearPass Policy Manager, can protect IoT systems and secure the network edge. However, policies are only as effective as the information used to build them, and that must be based on a deep understanding of automation processes and procedures underpinning retail operations. Applying a collaborative systems approach to the problem will help identify the IoT threat vectors and the security technologies needed for remediation.

Transforming untrusted IoT devices into trusted data must underpin strategic goals - like increasing basket size – if retailers are to avoid unacceptable risks in the process. On that note, it's important to understand how a retailer's strategic goals align with digital business transformation, and the central role played by hyper-awareness across front- and back-of-store operations.

BUSINESS TRANSFORMATION ENABLED

Some years ago the head of the Industrial Engineering Department of Yale University said, "If I had only one hour to solve a problem, I would spend up to two-thirds of that hour attempting to define what the problem is."1 In the same vein, a woodsman was once asked, "What would you do if you had just five minutes to chop down a tree?" He answered, "I would spend the first two and a half minutes sharpening my axe."[2] Regardless of your industry or task, it's important to be prepared, carefully defining your objectives and selecting the tools needed to achieve them.

Sadly, this lesson is often overlooked when it comes to retail IoT projects. Whether it's the allure - or misunderstanding - of the IoT concept, fear of being left behind by competitors, or pressure to do something new, companies frequently rush headfirst into projects without clearly defining objectives, value propositions, or the suitability of tools. The result is a high rate of failure, and disillusionment among customers.

Originally intended to describe an ecosystem of interconnected machines, the phrase "Internet of Things" has been taken literally to mean connecting all devices to the Internet. The overarching objective of IoT is not to connect every device to the Internet. IoT devices are vessels for context and data, and the objective is to tap only relevant information and devices. In retail, that relevance is simply to delight customer and drive sales. Very often this involves using IoT to collect relevant data to accomplish these goals.

How does one determine what is or is not relevant information? Relevance is established by a chain that stretches from the enterprise's strategic goals, to business objectives designed to achieve those goals, to what Gartner[3] calls "business moments" – transient, customer-related opportunities that can be dynamically exploited. A business moment is the point of convergence between the owner's strategic goals and relevant IoT context and data that when properly exploited will positively change reliability, performance, and/or safety.

These business moments must be carefully orchestrated, even if they appear spontaneous to the retail professional or customer. Success hinges on a second chain that stretches from relevant IoT context and data through the IoT architecture that accesses and conveys them to a target business moment. If the chain is poorly executed, say because the IoT architecture can't extract relevant information, then the business moment may pass without result, or could even trigger negative results to the detriment of the strategic goals.

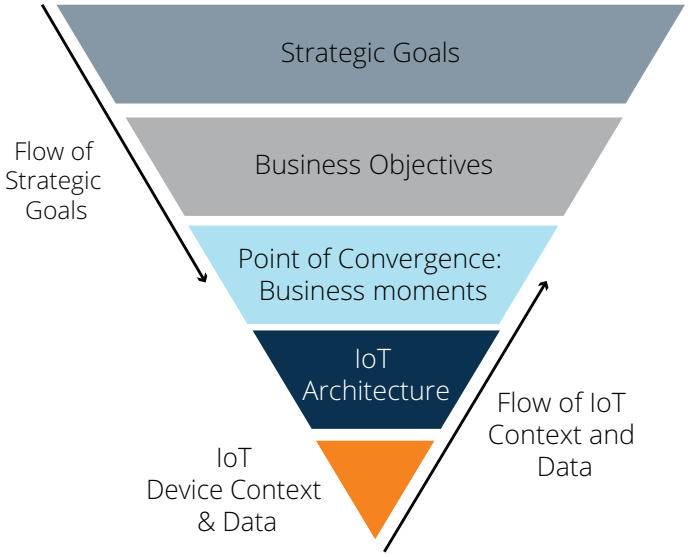


Figure 4: IoT Strategic Hierarchy

And so, we return full circle to the professor and the woodsman. The first order of business in any retail IoT project is to identify the strategic business goals to be achieved. Those should flow down into a series of specific objectives that rely on successfully delivered business moments. The IoT architecture is the tool by which relevant IoT context and data can be extracted and exploited to reorient behavior, attitudes, and actions in favor of the strategic goals.

Business goals and objectives inform the IoT architecture and relevant devices to tap, not the other way around. IoT solutions selected for eye candy appeal or hype alone will go wanting. Aruba's goal is to help customers identify relevant IoT data and context, define and successfully deliver business moments, and, in turn, attain their business objectives and strategic goals.

Where does one start this process? The first order of business in any retail project is to identify the customer's strategic goals and the associated business objectives that must be met. Those will inform the business moments for which the IoT architecture needs to extract relevant IoT data and context. Is the objective to enable new low touch guest services like "buy on-line pickup in store" (BOPIS)? Use data and analytics to drive in store product placement? Increase staff ability to communicate with each other and access real-time inventory data? Drive a loyal and more connected digital-relationship with customers via a branded mobile application? The answer(s) will impact the business moments that need to be delivered, and what constitute relevant data and context.

Business moments inform the IoT architecture, not the other way around. One-size-fits-all retail solutions are doomed to fail because they won't be tailored to deliver meaningful business moments.

This document presents IoT use cases that are relevant to a broad range of retail applications. Most of the use cases include at least one Aruba technology partner whose solution, used in concert with Aruba infrastructure, helps address strategic retail challenges.

RETAIL MARKET

According to McKinsey[4] the total economic impact of IoT in retail in 2025 should reach between $410B-$1.2T. The top identified areas include automated checkout ($150B-$380B) and real-time, in-store promotions ($89B-$348B). The reason these two areas are top priorities is because of the business benefits they drive: automated checkout typically yields a 40-88% reduction in check-out time, and a 75% reduction in cashier cost; and real-time, in-store promotions yield a 3-5% productivity improvement.

The breadth of retail initiatives mandates close attention to what a customer is trying to achieve. For example, is a point solution required to address a specific problem, i.e., increasing cybersecurity because of a recent breach? Or is an optimized system-level solution required, i.e., providing staff real-time inventory data when they need it?

Early adopters in retail environments could see share gains as well as cost reductions from leaner inventories, lower operating costs, and better use of floor space.[4]

Additionally, retail has other unique challenges that must be taken into account:

- Changing shopping habits as a result of the global pandemic;
- Inventory shrinkage;
- Growing numbers of cyber-attacks on retail organizations;
- Matching product with local demand to compete with on-line stores with ultrafast shipping options; and
- Customers' desire to shop from anywhere via multiple digital devices or in-store.

All must be balanced with the need and desire to increase sales by delighting the customer.

In every case, an extensible platform will be needed so customers can both build a broad range of services today while accommodating future requirements. While a platform is necessary, by itself it's insufficient to build a solution since no one vendor makes a universal set of end customer

solutions. Technology partners are an essential component of any use case.

Aruba has curated a world-class cohort of infrastructure, security, and location technology partners, the solutions of which have been validated interoperable with Aruba infrastructure. Common use cases that leverage solutions from Aruba and its technology partners to drive business outcomes are presented below.

SELF-SERVICE SHOPPING AND SMART CHECKOUT

Offering automated or self-service shopping together with smarter self-checkout have the potential to provide a dramatic improvement to the bottom line and is an effective way to increase customer loyalty through improved shopper experiences. Using a store-provided handheld scanner to check products as they are placed in the cart avoids the need to unpack a cart, scan items, and then bag them. Instead the shopper only needs to bag the items once, reducing queue times by 40 to 80 percent[4], lowering staff costs by up to 5 percent[4], and speeding the overall shopping experience.

Connected self-service devices and kiosks with integrated bar code scanning, touch screens, and printing can help brick-and-mortar stores compete today while serving as platforms on which to build tomorrow's shopping experiences.

ZEBRA

Zebra and Aruba have partnered to bridge the data quality and provenance divide thought a combination of technology integration, product interoperability, validated reference designs, direct support escalation, and joint innovation. The market leader in automatic information and data capture (AIDC), PoS, ruggedized mobile computer, and mobile printing solutions, Zebra is heralded for its ability to capture data reliably on the first pass over Aruba infrastructure, and deliver reliable connectivity over Aruba Wi-Fi to roaming staff and customers.

Zebra's handheld personal shopping devices, like the PS20, enable self-service checkout use cases by leveraging secure, wireless connectivity and location-aware context from Aruba infrastructure. PS20s can be attached to a cart or carried by a shopper. It allows customers to scan products as they select them as well as locate products and ensure that purchases do not exceed a shopper-defined budget. Personalized promotions and recipe options help to increase basket size.

Figure 5: Zebra Personal Shopper Mobile Device

In addition to self-scanning solutions, Zebra's MP7000 Bioptic Scanner includes an optional camera using computer vision to identify products and further enhance the checkout experience as well as reduce shrink. With product recognition and identification applications, the camera can identify items like produce, enabling a shortened picklist for simpler and faster checkouts. It also helps reduce self-checkout related losses by verifying that the scanned barcode matches the description of the product.

The MP7000 platform is extensible and can be enhanced with a customer-facing scanner to process loyalty reward cards, electronic coupons, and last-minute impulse purchases. These features reduce the burden on cashiers, accelerate checkout time, and enhance the overall customer experience.

Figure 6: Zebra MP7000 Add-On Scanner

Aruba and Zebra have taken the guesswork out of joint deployments by certifying the interoperable operation of both product sets, and by documenting reference designs across a range of retail applications. Joint systems go in faster and more reliably.

UNDERSTANDING CUSTOMER BEHAVIOR FOR LAYOUT OPTIMIZATION AND TARGETED MARKETING

Data from the location, movement, and behavior of shoppers can be used to optimize a store's physical layout to increase basket size. McKinsey estimates that layout optimization can lift productivity by 5 percent, driving $79B - $158B of added value in 20254. Understanding shopper behavior and high-traffic areas allows end caps to be fine-tuned, and marketing campaigns and advertising to be more precisely targeted and priced, based on empirical data.

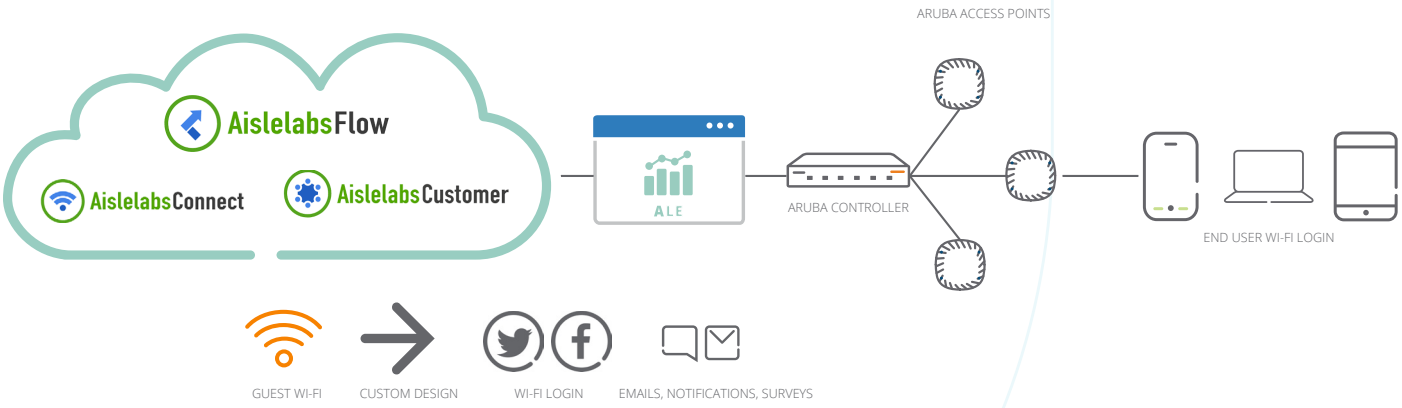
Aruba has partnered with a number of retail analytics partners that can use the network infrastructure and connected IoT devices like cameras, people counters, and other sensors to better understand shopper behavior.

Retailers can leverage data to personalize promotions and make them more relevant to shoppers. For example, identity and location can be collected from customers taking advantage of guest Wi-Fi offered by the retailer. Other contextual data can be collected from users who have signed into a branded retail app. Integrating identity, location, PoS data, people counter data, and smart camera data enables retailers to send real-time notifications to customers, dynamically manage in-store digital signage, and drive customized follow-ups post visit. McKinsey estimates that real-time personalized promotions can increase productivity in retail environments by 3 to 5 percent[4].

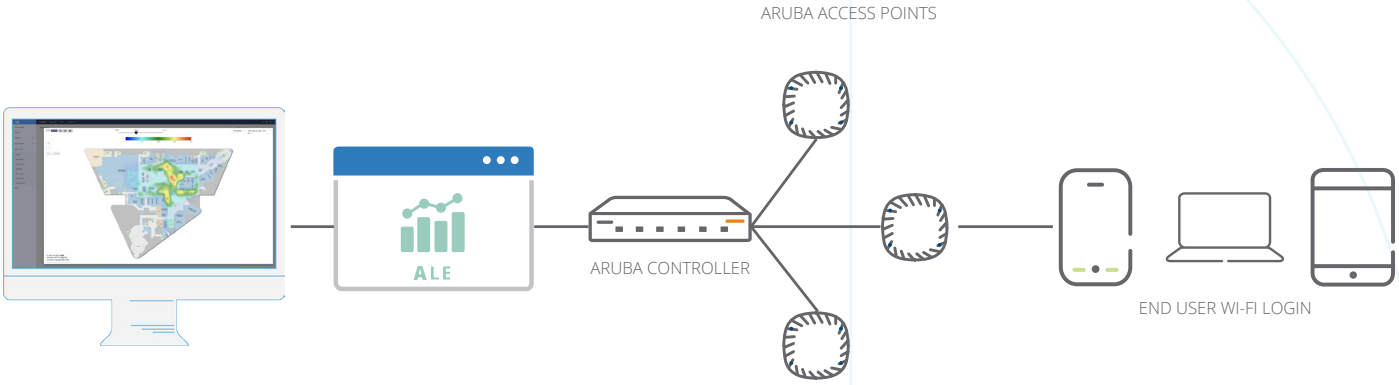
Aislelabs

Aislelabs is a Wi-Fi marketing and analytics company that provides location analytics and personalized marketing software. By combining the cloud-based Aislelabs product suite with enterprise-grade wireless access, retail stores can take advantage of existing infrastructure to understand who their customers are, how they behave within their space, and craft personalized messaging.

Aruba and Aislelabs have partnered to enable Wi-Fi marketing and location analytics for retail stores. Aruba wireless infrastructure has been certified interoperable with Aislelabs product suite including Aislelabs Flow, Aislelabs Connect, and Aislelabs Customer Hub. The joint solution provides business value beyond simple connectivity to make data-driven marketing decisions using enterprise-grade customer databases.



Skyfii's vision is to improve visitor experience by understanding user behavior thru its Skyfii IO suite of integrated visitor analytics and engagement software for physical venues. By pairing intelligent software with data science and marketing services, Skyfii can deliver tangible business outcomes through timely communication with guests and visitors with relevance to each individual's personal preferences, behaviors, and physical location.

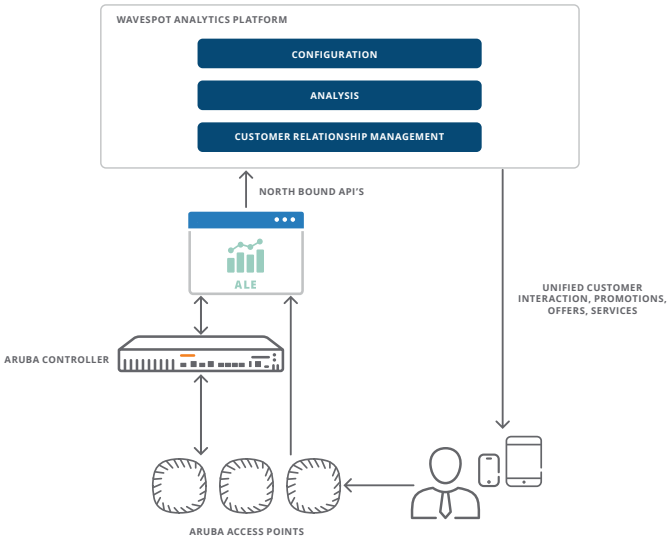


Skyfii IO pulls data and context from multiple network sources and aggregates it into a single system of record. Aruba ClearPass forwards guest profile and authentication data to SkyFii IO to enrich guest profile data when visitors access a venue's Wi-Fi network. Aruba's Analytics and Location Engine (ALE) forwards real-time location information, providing visibility into user behavior and space utilization. Using the Skyfii IO Insight application, retailers can generate a range of insightful, easy-to-understand reports that provide insights about the visitor experience. Skyfii IO Engage, a related application, creates highly targeted marketing messages based on location, behavior, and profile. Since Skyfii IO is a cloud-based SaaS platform, it can be integrated with an existing Aruba Wi-Fi network remotely without the need to install additional hardware on site.

Wavespot combines the ubiquity of Wi-Fi with the viral nature of social media marketing so retailers can offer free Wi-Fi to shoppers who log on using their Facebook, Twitter or other social identity. Powerful analytics offer insights into shopper behavior, empowering retailers to enhance their brand and build deeper relationships with customers.

Wavespot and Aruba have partnered to deliver location-based services to retailers, large public venues, and telecom providers. The joint solution leverages existing Aruba Wi-Fi 5 and Wi-Fi 6 access points – as well as ALE and Aruba's AirWave Management Platform - to generate analytics based on location and Web behavior.

The Wavespot Social CRM tool suite allows retailers to better understand shopper preferences, and ultimately expand their customer base, by leveraging the power of social media connections, targeted e-mails, and redeemable coupons.



The use of the Aruba infrastructure on-site avoids the deployment and management expense required for operating a separate overlay network. Typical spacing requirements of access points that meet today's mobility and unified communications demands also deliver reliable location accuracy throughout a store.

DYNAMIC PRICING WITH ELECTRONIC SHELF LABELS

Influencing customer behavior in real-time is a prime objective of retailers because it directly impacts basket size, sentiment, and loyalty. Long an elusive goal, behavioral impact is now achievable in no small part because of electronic shelf labels (ESLs), small e-ink displays that display information, receive signals such as near-field communications (NFC) from smart phones, and communicate wirelessly to back office systems.

ESLs provide bi-directional interactions between shoppers and real-time pricing, inventory, and advertising engines. Combined with knowledge of location and identity, ESLs allow stores to contextually adapt to, and influence, shopper behavior.

Robust ESL operation is business critical. Regulations mandate consistency between ESLs and point-of-sale system pricing. Additionally, targeted marketing programs only work if delivered to the right shoppers in the right context. These requirements put a spotlight on the reliability of ESLs and the infrastructure that supports them.

Hardwired ESLs would be prohibitively expensive, both because of the initial cost of pulling cables and rewiring during store churn. Deploying a dedicated ESL wireless network would similarly be expensive, and risks interfering with a store's RFID and Wi-Fi infrastructure. Leveraging a store's existing Wi-Fi access points for ESL communications is the most effective solution, however, the critical role of ESLs sets the bar high for the robustness of that wireless network.

Aruba's access points converge front- and back- of-store connectivity needs with high-speed wireless Internet access. With built-in radios for IoT and support for external USB adapters, Aruba access points can serve as platforms for a broad range of IoT devices, including ESLs.

Hanshow is a leading provider of electronic shelf labels and omni-channel digital store solutions based in Shanghai, China. Hanshow and Aruba have partnered to enable Hanshow ESLs to communicate with a Hanshow gateway server via Aruba's Wi-Fi 5 and Wi-Fi 6 access points. Equipped with a Hanshow USB adapter, an Aruba access point will securely, transparently, and bi-directionally transport ESL-related data between ESL tags within range and the gateway server. No additional infrastructure is required, eliminating the need for dedicated ESL gateways in the store.

The USB adapter automatically obtains an IP address from the Aruba access point, and then works just like a wired client to stream information to and from the ESL tags. The access point serves as a transparent pass-through, securely transporting tag data without otherwise altering, filtering, or otherwise processing the payloads.

SES-imagotag is a specialist in electronic shelf labeling systems and physical retail solutions. Founded in 1992, the company is headquartered in France and owned by Chinese electronics manufacturer BOE Technology.

A global leader in Electronic Shelf Labels and Retail IoT Cloud solutions, SES Imagotag and Aruba have partnered to ensure that ESLs can be economically, reliably, and securely deployed over a retailer's network. This includes applications spanning from convenience stores to hypermarkets to big box retailers. Access points secure communications between the ESLs and the back-office applications.

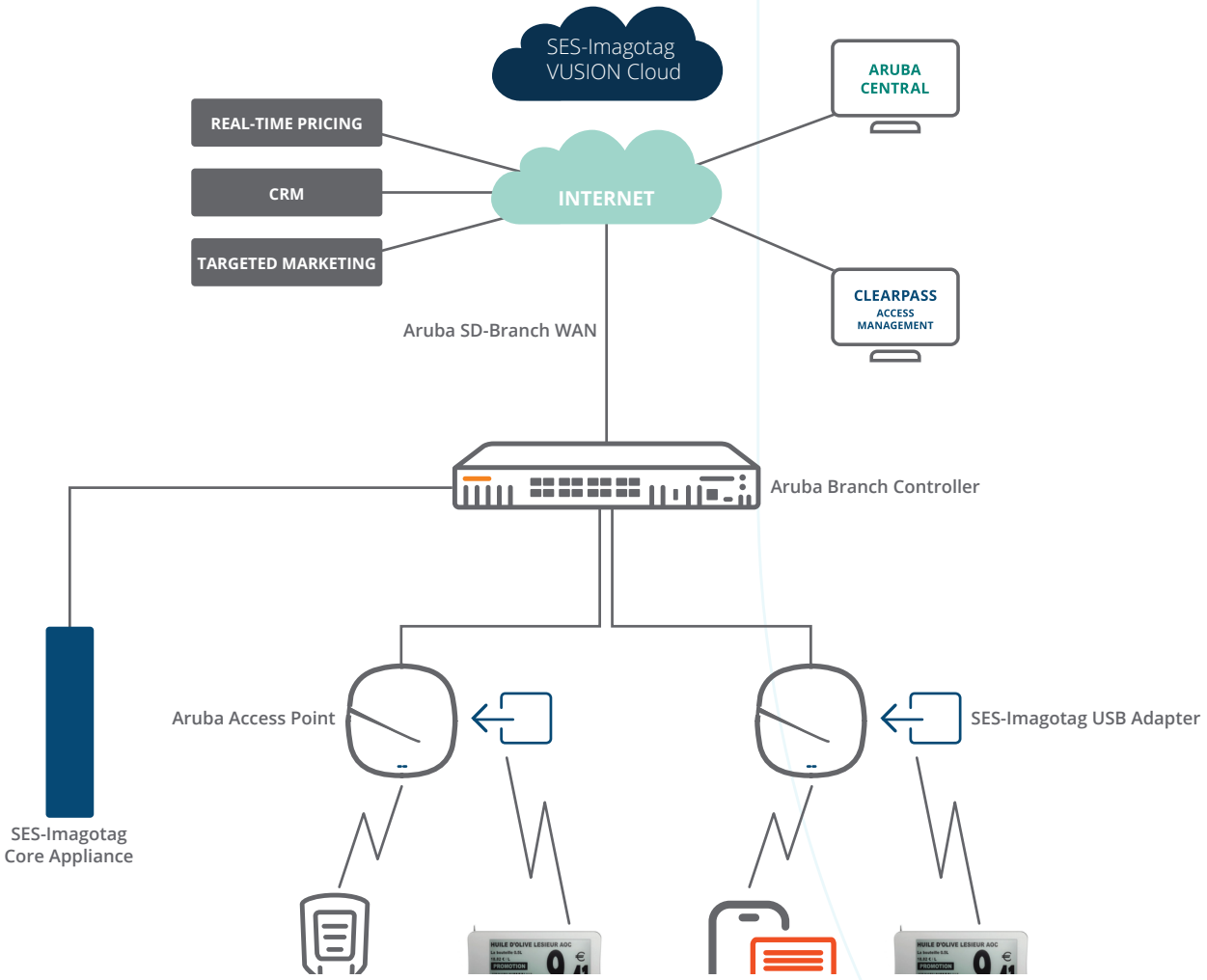


Figure 7: SES-imagotag System Running Over Aruba Infrastructure

ESL communications are handled by an SES-imagotag Retail IoT Connector inserted into the access point's USB port. Access points communicate through secure tunnels to SES-imagotag's VUSION Retail IoT Cloud platform. Dynamic IoT traffic segmentation is maintained throughout the Aruba switching infrastructure, protecting the tags against attack, and the rest of the network against compromised devices.

Set-up is simple and requires selecting "SES-imagotag" from a drop-down menu on the access point configuration page, and then entering the IP address of the SES-imagotag Core Appliance. Aruba switches, in conjunction with ClearPass, automatically set-up secure connections with access points without VLANs and independent of the switch port into which they are connected. This feature simplifies the initial deployment, and minimizes opportunities for miswiring during adds, moves, and changes over the life of the deployment.

SoluM (originally Samsung Electro-Mechanics), one of the world's largest ESL providers, and Aruba have partnered to ensure that ESLs can be economically, reliably, and securely deployed. The joint solution works in conjunction with Aruba access points and is designed for applications of all sizes - from branch stores to big box retailers. In addition, the solution can be applicable to various areas such as desk tags for smart offices, name tags for lockers, signage for meeting rooms and so on.

Figure 8: Examples of SoluM electronic shelf labels

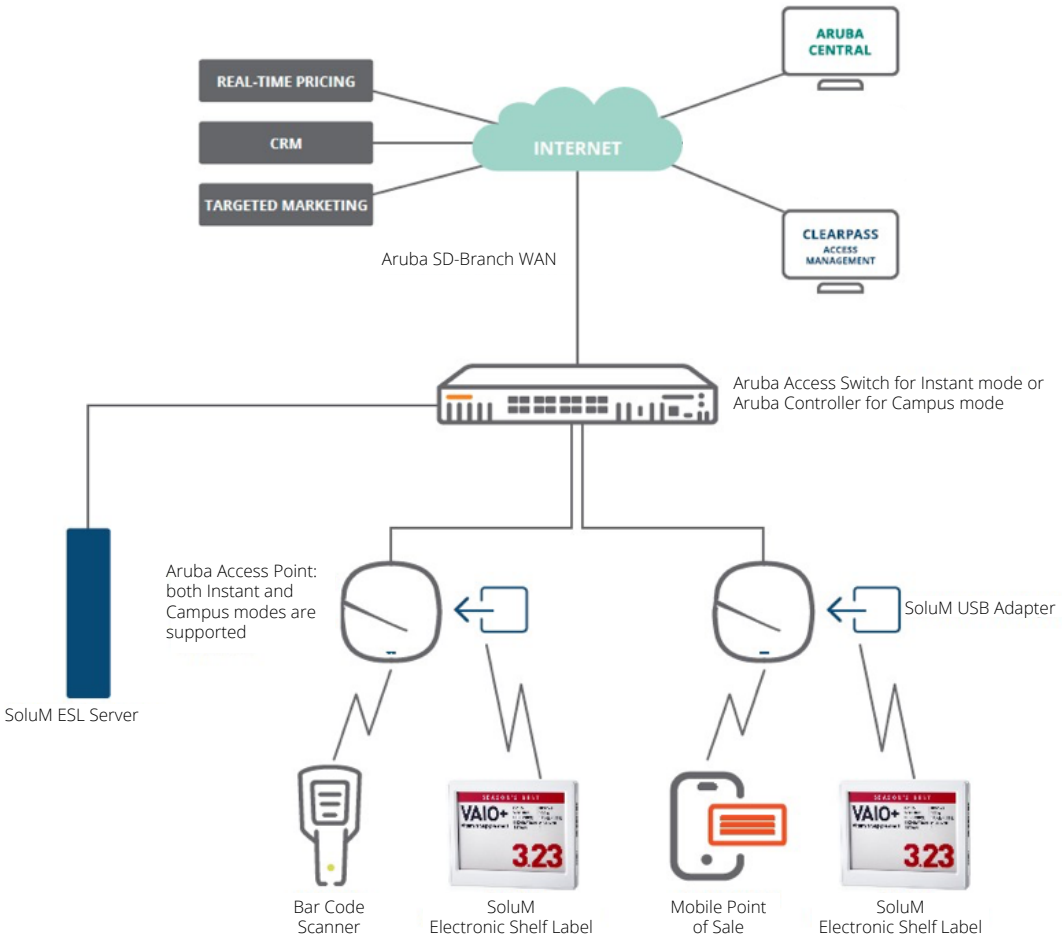


Figure 9: SoluM System Running Over Aruba Infrastructure

INCREASING INVENTORY ACCURACY AND REDUCING INVENTORY SHRINKAGE

Inventory shrinkage is the difference in count between what should be in inventory and what is actually available. Shrinkage can be caused by shoplifting, theft, vendor fraud, and mismanaged logistics. Shrinkage impacts a retailer's bottom line and imperils newly popularized services like buy on-line, pickup in store (BOPIS). It's difficult to deliver satisfying experiences to customers if inventory counts are inaccurate. If a customer purchases a product on-line and finds after traveling to the store to pick it up that the product is unavailable, both the sale and, in many cases, the customer could be lost.

Radio frequency identification (RFID) is commonly used to automate inventory collection, increase the efficiency of inventory counts, and reduce shrinkage. Tagging products with inexpensive RFID labels helps automate and improve the accuracy of inventory tracking. The distance over which RFID tags can be read has been steadily rising, and unlink bar or QR codes, an RFID reading device does not need to be in line-of-sight with the tag to be read. RFID encompasses a variety of RF frequency range and technologies, and some – like Bluetooth Low Energy – enable active tags that continuously broadcast for real-time inventory collection and location monitoring.

Video analytics, incorporated into cameras or run separately on servers, can also help prevent shrinkage. Analytics can be used to detect shoplifting, theft, and logistics errors. Shrinkage can be further controlled by combining RFID with video analytics.

Assuming that these measures could reduce losses by the equivalent of 1 percent of the cost of goods sold (on average, shrinkage costs stores 1.3 percent of revenue or $182 billion globally), the value to the global retail industry could be $23 billion to $92 billion per year in 2025.4

Aruba has partnered with leading asset tracking vendors to help customers address inventory accuracy and shrinkage.

Wiliot manufactures Bluetooth-based, intelligent stickers and tags powered using energy harvesting technology. The small, low-cost tags harvest RF energy from the air, sense the status of the item on which they're mounted (presence, temperature, movement), and broadcast status over an encrypted Bluetooth packet. The encrypted Bluetooth transmissions are recognized by Aruba Wi-Fi 5 and Wi-Fi 6 access points, which forward them to the Wiliot cloud for decryption and processing.

Retailers equipped with Aruba Wi-Fi can use the stickers and tags to monitor inventory levels, handling (i.e., that products are never stored outside specified temperature ranges), expiration date management, and in-store user experiences (i.e., changing digital signage when a tagged particular product is picked up). Retailers can also use Wiliot tags to implement new edge analytics initiatives, e.g., continuous cold chain monitoring or observing how many times a product was picked up before a customer added it to his or her cart.

Zebra is a market leader in AIDC, PoS, ruggedized mobile computer, and mobile printing solutions. Zebra's retail RFID and Bluetooth-based asset tracking solutions can automate and improve the accuracy of inventory counts and help reduce shrinkage by tracking the location of items in real-time.

Zebra offers a full line of mobile and fixed RFID readers that can connect to the Aruba network via Wi-Fi or wired Power-over-Ethernet connections. Providing visibility into the location of products as they move through warehouses and stores helps avoid miscounts and misplacement of inventory, speeding workflows and preventing shortfalls that could impact revenue.

Figure 10: Zebra Wi-Fi Enabled RFID Reader

Data from Zebra RFID readers, Bluetooth asset tags, mobile devices, and the Workforce Connect application can all be transported via Aruba infrastructure to the location-aware Zebra Savanna platform. Savanna uses AI and analytics to flag anomalies that impact workflows and inventory shrinkage. Shrinkage and theft can be further reduced by using products like the MP7000. Embedded cameras in the MP7000 detect anomalies like price tags that are mismatched with the product being scanned, say due to substitution of a price tag from less expensive merchandise. Given the tight margins under which retailers operate, lowering shrinkage and theft can have a significant impact on the bottom line.

ENHANCING THE RELIABILITY AND QUAILTY OF MOBILE STAFF COMMUNICATIONS

As organizations have migrated to mobile devices, network access has shifted from wired Ethernet to Wi-Fi. Providing the quality of service (QoS), bandwidth, and management tools necessary to deliver secure, toll-quality voice and jitter-free video at scale over Wi-Fi to mobile devices requires sophisticated wireless infrastructure. Aruba's AI-based application and device fingerprinting enable the system to detect the types of traffic flows, and the devices from which they originate. The network can then be dynamically conditioned to deliver QoS - on an application-by-application, device-by-device basis - as needed to deliver highly reliable voice, video, and other multimedia services. The result is a superb user experience in which staff can roam while staying connected with each other, anywhere in the facility.

Besides high-quality voice, secure text messaging is a popular means by which staff securely communicate. Secure texts can be sent mobile within the facility without the risks of using standard texting applications on personal devices.

These services are delivered over the same Aruba Wi-Fi infrastructure that is used for mobile IoT telemetry, IT devices, and OT facility operations systems. Converging all services under Aruba's extensible ESP platform yields considerable cost savings, enables IT to deliver uniform security and visibility from end-to-end, and allows additional services to be added on without ripping-and-replacing infrastructure. As will be discussed elsewhere in this paper, Aruba's AirPass technology allows cellular users to seamlessly handoff voice and data between cellular and Wi-Fi networks. In many instances this eliminates the need for expensive distributed antenna systems while offering high connection speeds, better audio quality, and fewer coverage dead spots.

Aruba has partnered with the leading mobile staff communication vendors the solutions of which span a broad range of applications and wearable and handheld Wi-Fi enabled mobile devices. Properly implementing these applications and services requires a different way of architecting wired and wireless infrastructure to achieve application prioritization, QoS, and actionable monitoring and diagnostics.

Application Prioritization

Wi-Fi bandwidth is a limited and shared commodity, so it's important that business-critical applications can be prioritized over social media and lesser priority apps. Aruba's deep packet inspection engine automatically identifies

thousands of different mobile applications on launch. When a business-critical application is recognized, the network will automatically establish a bandwidth contract to reserve sufficient bandwidth for proper operation. Non-critical applications are given bandwidth prioritization to deliver the best possible experience needed without compromising performance.

QoS

Retail productivity applications utilize end-to-end encryption to protect confidentiality and privacy. This unfortunately breaks QoS mechanisms on typical wired and wireless networks as they are unable to differentiate between non-critical and latency-sensitive traffic. Mis-tagged traffic is subject to jitter and delays.

Aruba has addressed this issue by developing a heuristics feature that can identify latency-sensitive traffic without decrypting it. The heuristics feature is a standard component of Aruba's secure mobility infrastructure that correctly tags voice and video traffic, but also retags misidentified traffic originating from non-Aruba network infrastructure.

Monitoring & Diagnostics

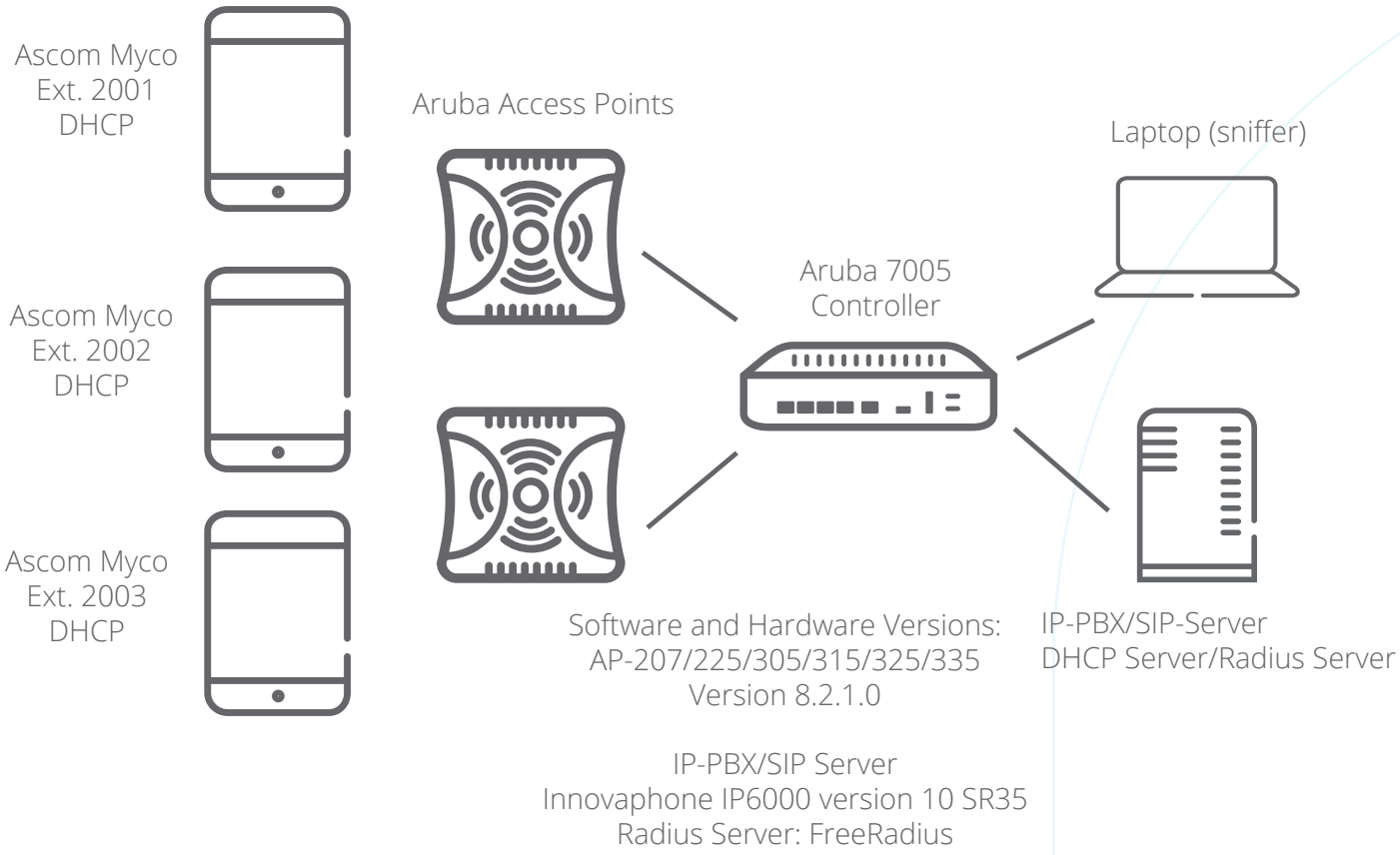
Cutting the cord on wired phones impacts the selection of monitoring tools. In-line tools can used to monitor wired IP phones call performance and diagnose the source of problems. Wireless phones, however, require different tools that provide end-to-end call performance visibility, and variably sized payload and dynamic port data, to isolate the root cause and remediate issues while calls are in flight. If IT cannot correlate poor call Mean Opinion Scores (MOS) to specific network, server, client, or client peripheral issues, then root cause analysis becomes highly challenging.

To address this issue, Aruba has developed a method to pull data directly from Wi-Fi access points, switches, remote VPN links and controller that is a combination of unified communications and network infrastructure performance data – no external probes required. Monitored data include R-value, jitter, delay, packet loss, Wi-Fi access point-to-controller packet loss, caller/callee identity mapping to MAC and IP address, call status, voice or video call type, and client sessions active at the time of the call. These capabilities enable Aruba's management and operations solutions to display dropped calls, low MOS values, and performance degradation per user location and device. Aruba controllers and virtual controllers can then use these data to implement Call Admission Control (CAC) based on bandwidth and call count to boost available throughout, reduce dropped calls, minimize bandwidth oversubscription, and lower traffic congestion. The results is significantly improved user experiences with multimedia and latency-sensitive calls.

ascom

Aruba has partnered with Ascom to support their purpose-built mobile devices for retail staff communications. Ascom products such as the i62 and Myco handsets interoperate with Aruba Wi-Fi infrastructure to ensure association, authentication, and roaming functionality are robust for retail environments.

Ascom solutions make it easier for staff to communicate, coordinate and execute time-sensitive activities. Ascom devices help streamline staff workflows, support faster responses and deliver context-rich information to mobile personnel. The easy-to-use user interface for managing calls, alerts, photos, messages, scores, waveforms and other critical information is simple to learn without formal training. A true hot-swap battery helps ensure constant operation throughout long shifts.

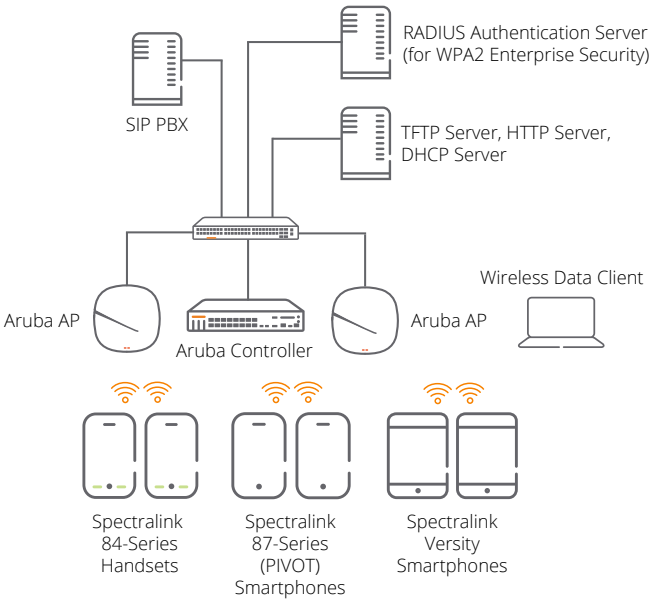


Ascom's certified interoperability with Aruba infrastructure helps staff stay connected while on the move in any retail environment.

Spectralink is a leader in the enterprise mobility market with a wireless solution portfolio optimized for mission-critical healthcare, retail, manufacturing and hospitality applications. Spectralink devices are known for superior voice quality, connectivity and enterprise-grade durability and reliability plus Spectralink has the only mobility solutions with native integration with Microsoft® Skype for Business®.

Spectralink's purpose-built devices are designed for retailers and include features like hot swappable batteries, fingerprint scanners, cameras, waterproof ratings, and built in Bluetooth and Wi-Fi.

Aruba is part of Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program which is designed to ensure interoperability and high performance between Spectralink 84-Series, 87-Series and Versity smartphone products with WLAN infrastructure.



Theatro, a leading provider of voice-controlled collaboration devices and apps, and Aruba have partnered to ensure that Theatro's smart devices and apps can be economically, reliably, and securely deployed over retail and enterprise networks spanning from specialty stores to the largest big box retailers.

Theatro's Intelligent Assistant solution consists of Communicators and the SaaS Conversational Platform. Communicators are Wi-Fi enabled, voice-controlled devices that connect workers with order management, human capital management, and task management enterprise applications using a simple conversational interface.

The joint solution uses Aruba access points already deployed on site as secure communications platforms between Communicators and the SaaS Conversational Platform. No additional gateways are required in either new or retrofit deployments.

The access points establish secure tunnels to the SaaS application. Dynamic segmentation is maintained through the Aruba switch fabric, protecting Communicators against attack, and the rest of the network against compromised devices.

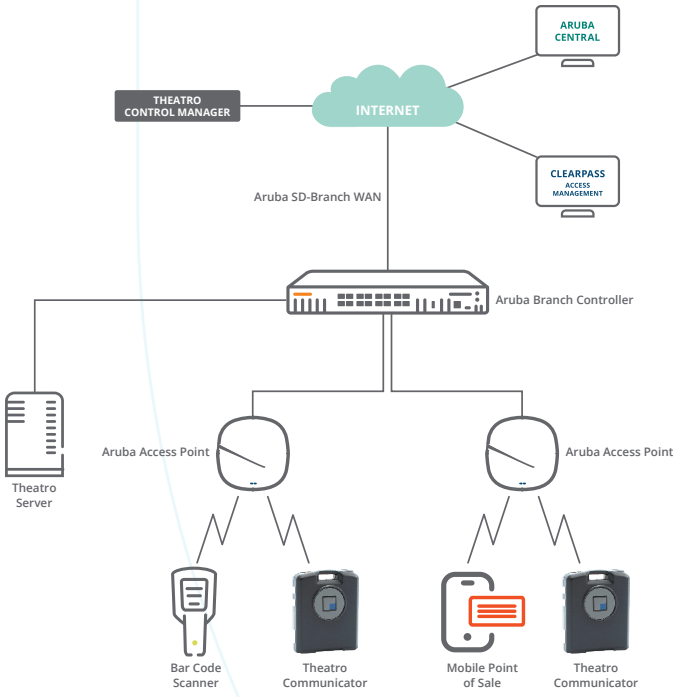


Figure 11: Representative Theatro Block Diagram

Locating, harvesting, and conveying relevant, trustworthy IoT data and context is easier said than done. Data must be captured with fidelity, over networks that reach wherever IoT devices are working or roaming. And cybersecurity must be implemented and enforced from source to C-Suite, from I/O to CMO.

It is on these last points that fractures typically appear in retail applications. Data input is often hit or miss. Voice communications with staff are unreliable, especially when roaming. Locating inventory, equipment, and staff members is challenging. End-to-end security is aspirational but rarely achieved, especially with IoT devices and systems.

Zebra's Workforce Connect solution provides a single platform for collaboration with workflows based on contextual data. This enables staff and associates to more efficiently do their job while only needing to carry one mobile device. It includes capabilities like push-to-talk and text messaging for one-to-one or one-to-many communications to ensure all staff members are informed.

Zebra and Aruba have partnered to ensure the secure and reliable operation of Zebra mobile devices, including those running Workforce Connect, over Aruba wireless networks. Aruba's deep packet inspection engine identifies and prioritizes latency sensitive Workforce Connect communications to deliver toll-quality voice to roaming devices across even the largest sites. Zebra barcode scanners are heralded for their ability to capture data reliably on the first pass, and Zebra printers and mobile computers offer unparalleled reliability and robust construction. Aruba ensures reliable service delivery to all Zebra devices when they operate and roam over Aruba Wi-Fi infrastructure, and secure dynamically-segmented communications over Aruba wired infrastructure.

Figure 12: Aruba-Zebra Integrated Voice and Data Capture

Aruba and Zebra have taken the guesswork out of joint deployments by certifying the interoperable operation of both product sets, and by documenting reference designs across a range of hospitality applications. Joint systems go in faster and more reliably.

MIGRATING FROM BREAK-FIX TO PROACTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep refrigeration, air conditioning, bakery ovens, and other plant and equipment running non-stop. Addressing maintenance proactively to minimize downtime, and maximize the utilization and performance of assets, can reduce maintenance costs by up to 40%. Spending on proactive and predictive maintenance is expected to hit $12.9 billion in the next two years.

Proactive maintenance is an essential tool in this quest. By instrumenting equipment, monitoring for degradation, and identifying potential problems in advance of failure, predictive maintenance can provide visibility into the performance of assets, ensure high availability, and maximize the returns on often substantial capital investments.

The challenge is that identifying the source of possible failures is not always a simple task. Sensor networks and gateways have traditionally been expensive to deploy and can have vulnerable attack surfaces that keep CISOs awake at night. COOs, in turn, fret whether innovative AI predictive maintenance solutions require resources beyond the means of operations teams. Based on these factors, juggling the high cost and security risks of asset performance monitoring solutions against the benefits of lower downtime and fewer disruptions is a challenging calculus.

An optimal solution is to leverage secure, robust IT infrastructure that is already deployed to capture machine status from proactive monitoring sensors. A dual-use network is more economical to deploy and can eliminate gateways and the security threat they pose.

ABB is a technology leader in industrial digital transformation of electrification, automation, motion, and robotics. Thru its ABB AbilityTM digital platform, ABB drives improvements in productivity, reliability, and efficiency.

The ABB Ability Smart Sensor is a battery-powered, multi-sensor device that monitors rotating machinery like motor drives, valves, and pumps for abnormal behavior indicative of pending failure. Status is communicated over a secure Bluetooth link, and analyzed by ABB's advanced algorithms. Operations engineers are automatically notified of out-of-normal conditions well before failure, allowing repairs to be performed before processes are impacted.

The Smart Sensor helps customers migrate from break/fix to proactive maintenance, a digital transformation that reduces downtime related to refrigeration and air conditioner failures, enhances asset utilization, and optimizes the scheduling of maintenance engineers. All of which ultimately boost efficiency and profitability.

ABB and Aruba have partnered to enable Aruba Wi-Fi 5 and Wi-Fi 6 multi-radio access points to securely collect and forward ABB AbilityTM Smart Sensor data to the ABB Ability Condition Monitoring application. Using Aruba zero trust infrastructure as a data collection platform provides uniform security and visibility across both IT and IoT domains. It eliminates the costs and security risks and costs associated with large fleets of gateways. Since gateways filter raw data streams that can be rich in visibility data, removing them has the added benefit of improving visibility all the way down to individual sensors.

The Aruba-ABB solution works with brownfield and greenfield deployments of any Aruba Wi-Fi 5 and Wi-Fi 6 access points equipped with a BLE radio and AOS 8.6 or later. This means that proactive maintenance monitoring can be retrofitted to existing Aruba WLAN deployments without adding additional IT gear or gateways.

The joint ABB-Aruba solution delivers the operational visibility and robustness demanded by COOs, without the expense of a dedicated wired sensor system. Wireless communication allows Ability Smart Sensor to be deployed anywhere without expensive conduit or enclosures. These savings extend throughout the lifecycle of a stores, refrigerated warehouses, and logistics facilities since adds, moves, and changes are easy and inexpensive.

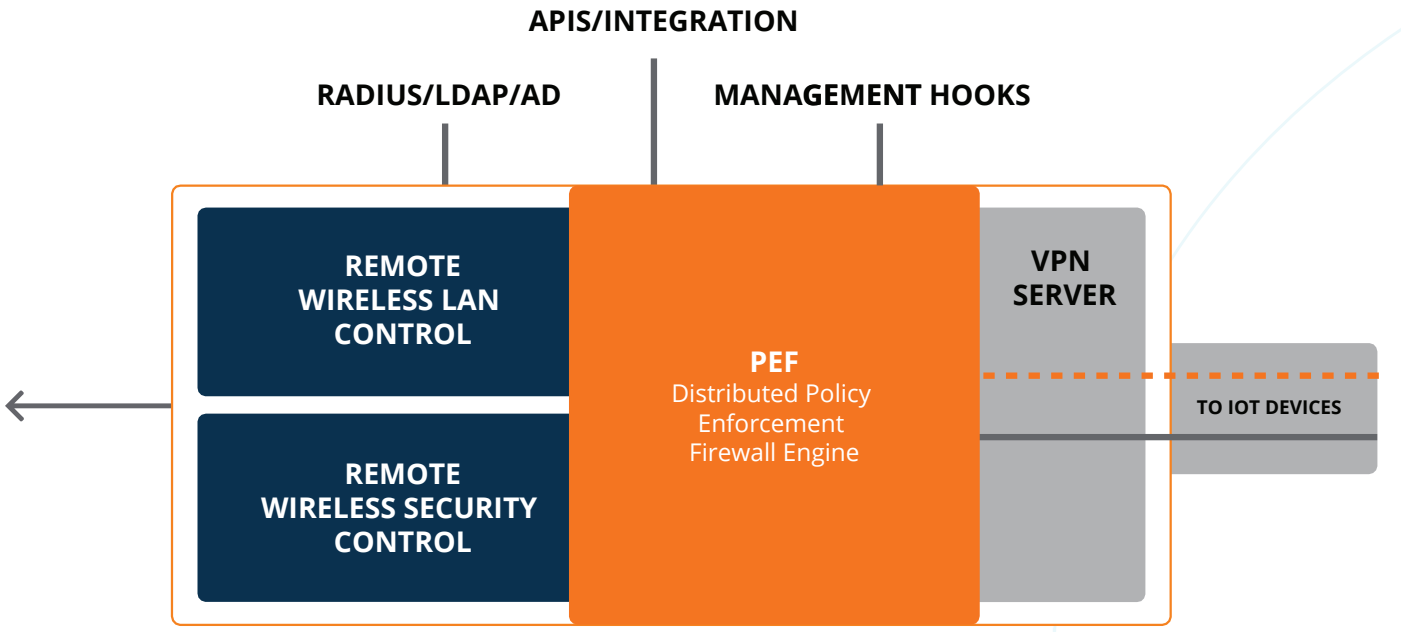


Figure 13: Aruba VPN Concentrator Controller

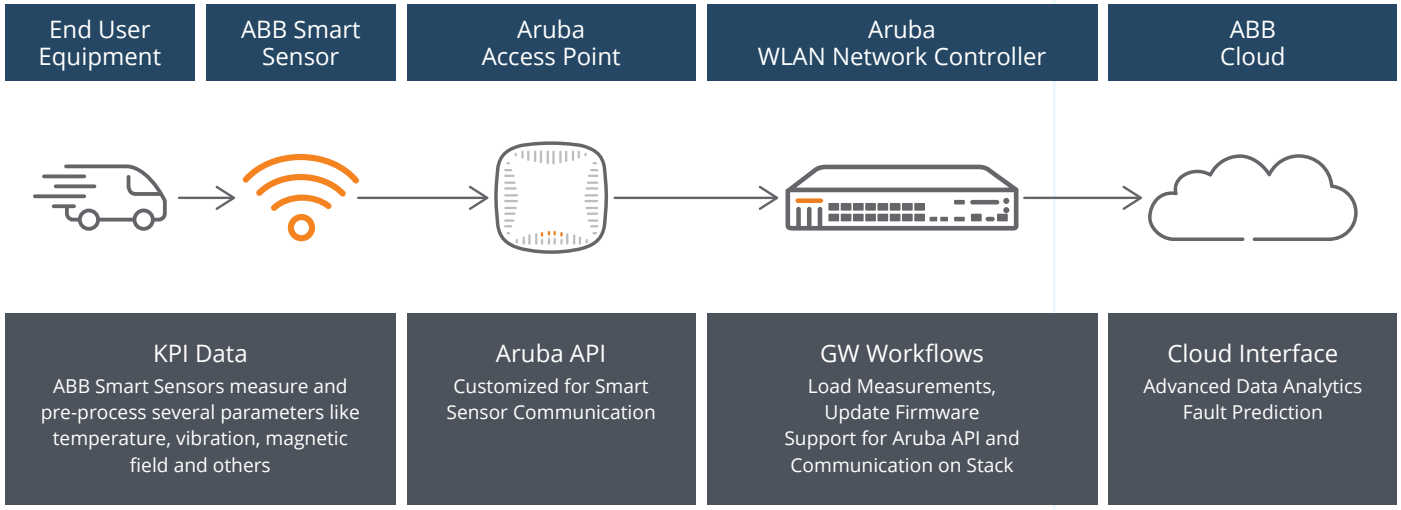


Figure 14: Aruba and ABB Integration Overview

The intersection between IT and plant operations has historically been a point of friction, but not so with the ABB-Aruba joint solution. Both companies are respected leaders in IoT and IT, respectively, and the joint integration allows data to flow reliably and securely between systems. Visibility and robust design address the uptime concerns of COOs, while I/O-to- application security and policy management check the box for CISOs. And the cost savings will cheer CFOs.

PHYSICAL DISTANCE MONITORING AND CONTACT TRACING

Workplace safety extends beyond physical and environmental hazards. Today, physical distance monitoring and contact tracing are essential for back-to-work and stay-healthy-at-work initiatives. Whether mandated by local regulations or company policies, maintaining safe distances from customers and infection control tracing are top of mind for facilities teams. While there is no single physical distance monitoring and contact tracing application that will work for all retail sites, real-time location services and identity stores have an essential role to play in every workplace infection control solution.

Aruba has teamed with multiple technology partners to deliver a broad range of physical distance monitoring and contact tracing solutions. The solutions fall into four categories:

- Physical distancing enforced by wearable tags or wristbands for situations in which a personally-owned device is not suitable;
- Application-based physical distancing solutions that run on personally-owned or company-issued devices;
- Presence detection systems that pick-up Wi-Fi signals from personally-owned or company-issued devices, but do not require an application; and
- Thermographic and facial recognition systems that monitor the temperature of individuals' heads, and can process dozens of people simultaneously.

AiRISTA FLOW

The AiRISTA Flow Social Distancing and Contact Tracing Solution uses a wireless tag worn by employees to help enforce guidelines for social distancing and automate contact tracing. The tags communicate with each other autonomously, without supervisory control, and trigger when they are closer than 2 meters apart. The user is signaled haptically and the devices forward the incident via Aruba access points to the AiRISTA Flow cloud-based software system.

Figure 15: AiRISTA Flow BLE Proximity Tags With Haptic Feedback

Aislelabs

Aislelabs provides a real-time footfall and occupancy monitoring to promote social distancing in large sites without the need to download an app or obtain opt-in approval. The solution uses personally-owned, Wi-Fi enabled smart phones or tablets, together with existing Aruba Wi-Fi infrastructure, to anonymously log the movement of people and area occupancy in an auditable database. Violation alerting is triggered based on programmable thresholds.

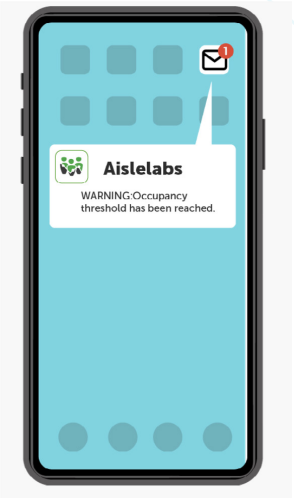


Figure 16: AisleLabs COVID-19 Social Distancing Solution

COHU | HD COSTAR

CohuHD's Thermographic System is an intelligent thermal imaging, radiometric detection, optical imaging, and facial recognition solution. The system automatically and simultaneously identifies the faces of more than thirty people within one second, reads forehead temperatures, and alerts when a reading is above normal. All measurements are recorded together with location for trend analysis. If a high temperature reading is detected the system can respond automatically using voice synthesis, triggered relay outputs, and access control interfaces. The camera uses a US Department of Commerce compliant SoC.

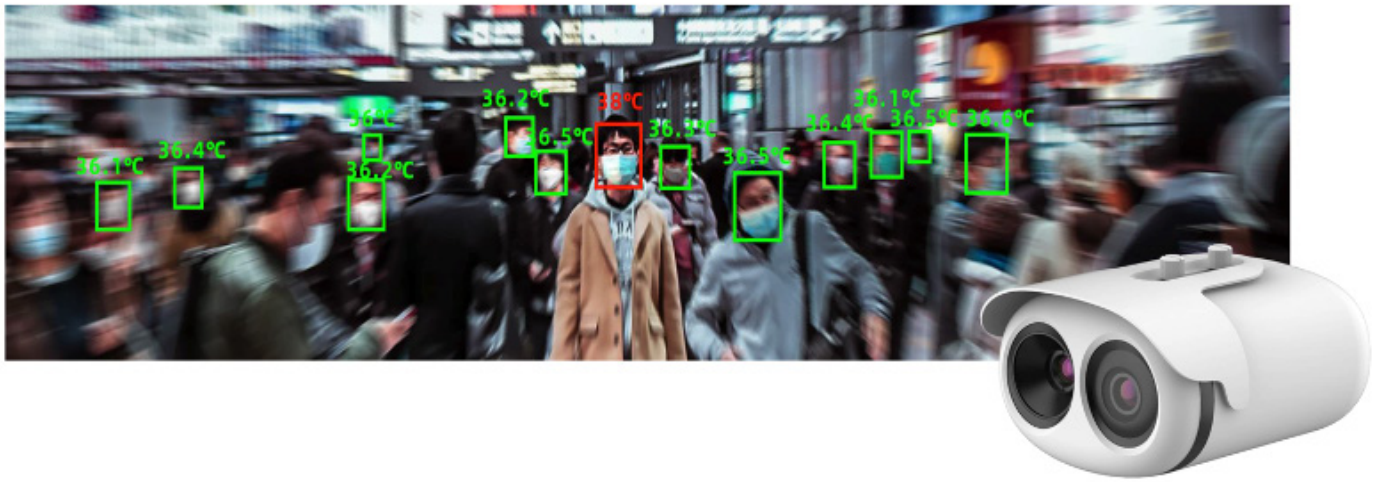


Figure 17: CohuHD Non-Contact Thermographic and Facial Recognition Camera

CX APP

The CxApp Touchless Application leverages Meridian BLE Beacons strategically placed around the facility, and the Meridian cloud service for location data. The mobile app sends notifications based on crowded times, vacant times, and total staff, customers, and guests per square foot/meter, all based on real-time occupancy within the environment.

Kiana

Kiana Analytics' Rapid Containment Application uses real-time location data, collected by existing Aruba access points from Wi-Fi enabled mobile phones and tablets, to identify the presence and movement of people. The application analyzes social transmission vectors, including locations and contact trees, to help mitigate spreading of communicable diseases.

Patrocinium™

The Patrocinium Safe Return Application leverages Meridian BLE Beacons, the Meridian cloud service for location data, and Patrocinium's ArcInsight analytics package. The application runs on personally-owned or corporate-issued smartphones and tablets, and automatically detects when other personnel are too close. The location and identity of the individuals are sent to the analytics application via Aruba Wi-Fi for contact tracing.

skyfii

OccupancyNow is an automated occupancy and social distancing management toolkit from SkyFii. The cloud-based solution uses real-time location data from existing Aruba infrastructure to maintain safe occupancy and social distancing guidelines, automatically alert staff when occupancy counts reach a set threshold and facilitate contact tracing via with Skyfii's analytics and communication tools. OccupancyNow also helps track whether routine cleaning and sanitization procedures are being performed.

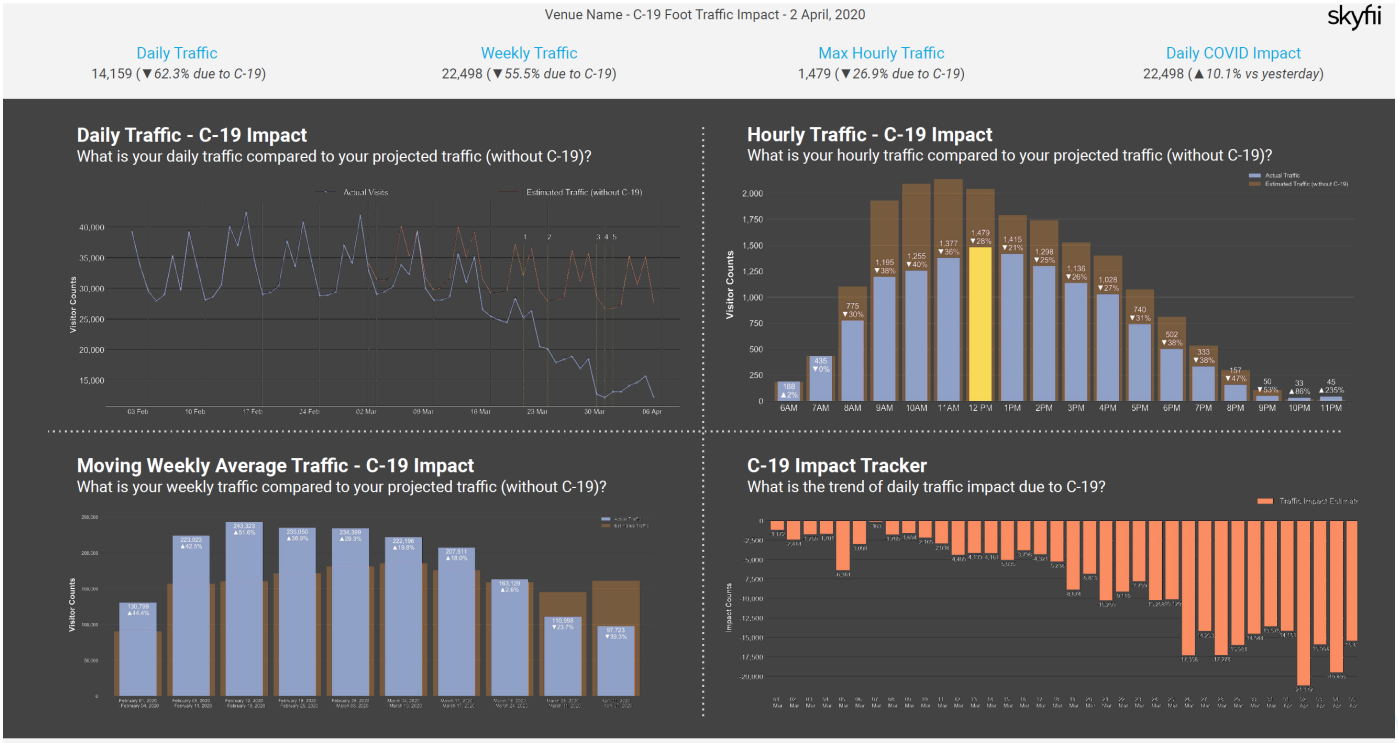


Figure 18: SkyFii OccupancyNow Dashboard

VAPING DETECTION AND AIR QUALITY MONITORING

In 2016 the U.S. Food and Drug Administration (FDA) mandated that electronic cigarettes (e-cigarette) products be regulated as tobacco products, and subsequently banned the sale of these products to minors. That same year a World Health Organization (WHO) report recommended that e-cigarettes be banned in indoor areas and wherever smoking is prohibited. Since then governments worldwide have enacted laws that prohibit e-cigarette usage (vaping) everywhere that smoking is banned.

The challenge has been how best to enforce no-vaping rules since the vapors can be difficult to detect. E-cigarette vapor contains ammonia, and the first vaping detection sensors simply detected when a preset level of ammonia was present and triggered an alarm. The problem is that many products contain ammonia, including body sprays, resulting in a high false alarm rate.

An alternate solution is to use two different sensors to detect ammonia and other chemicals present in e-cigarette vapors. Dual-trigger sensors have a much lower false alarm rate and raise confidence that a vaping alert is valid.

IP Video is a New York-based developer of smart building physical security sensors. Their HALO IoT Smart Sensor is a multi-function security and environmental monitoring devices that hosts chemical sensors, audio detection, and a voice synthesizer.

Figure 19: HALO Smart Sensor Powered By Aruba Switches And Pass-Through PoE Access Points

IP Video and Aruba have collaborated to enable plants to combat vaping through automated sensing and response. Powered by Aruba PoE pass-thru access points and PoE switches, HALO detects vaping and THC using dual-triggers to reduce false alarms. HALO incorporates multiple sensors so it can serve additional roles, too, i.e., detecting particulates, carbon dioxide, carbon monoxide, volatile organic compounds (VOCs), oxidizing agents, and ethanol. These features make HALO well suited to air quality monitoring applications. Audio monitoring enables HALO to detect gunshots and cries for help, while a voice synthesizer lets HALO respond to occupants with context-appropriate messages, i.e., in response to a verbal request for "help" HALO can respond that "help is on the way." Voice detection and response are processed locally, not in the cloud, to ensure that privacy is maintained. The joint solution is ideal for enforcing no vaping rules and monitoring for other signs of danger.

GUNSHOT DETECTION

One of the most dangerous situations faced by first responders is a live shooter inside a building. Without knowing the location of, and weapons used by, the shooter, first responders imperil themselves when they come on the scene. Situational awareness can save lives and speed apprehension of the perpetrator.

Emerging technologies for public safety sit at the cutting edge of the detection and mitigation of threatening situations, with gunshot detection being an essential element in that toolbox. Despite claims about sophisticated machine learning algorithms, older generation gunshot detection systems based on acoustic sensor arrays were notoriously prone to false alarms.

The most current generation of gunshot detection relies on multiple sensing mechanisms – muzzle flash, impulse, and pattern matching – to validate the presence, type, and even barrel length of discharged firearms. The result is fewer false alarms and more efficient routing of first responders to active shooter-involved incidents.

Installing a dedicated network to support gunshot detectors is not economically viable, and many CISOs will not permit such overlay networks. Additionally, battery-operated sensors on wireless networks, like LoRa, present cybersecurity risks by bypassing standard IT security monitoring tools. There are also maintenance issues associated with battery replacement.

Aruba's Wi-Fi 6 access points overcome these issues by providing a USB port that supplies power and data communications for gunshot detectors. Standard Aruba security mechanisms help protect against malicious or unintentional security breaches.

AMBERBOX Gunshot Detection

AmberBox, a leading provider of next-generation gunshot detectors, and Aruba have partnered to ensure that first responders can be reliably notified when an active incident is in process. Applications include building lobbies and publicly accessible spaces.

Figure 20: AmberBox Gunshot Detector

The joint solution works with Aruba Wi-Fi 6 (802.11ax) or Wi-Fi 5 (802.11ac) access points already deployed on-site, avoiding the need for a separate overlay network. AmberBox sensors interface with the access points' USB ports, which provide both power and data access. Sensor spacing matches the access point spacing required for voice applications. AmberBox sensors do not interfere with the access point's ability to deliver high performance voice, video, location, and telemetry.

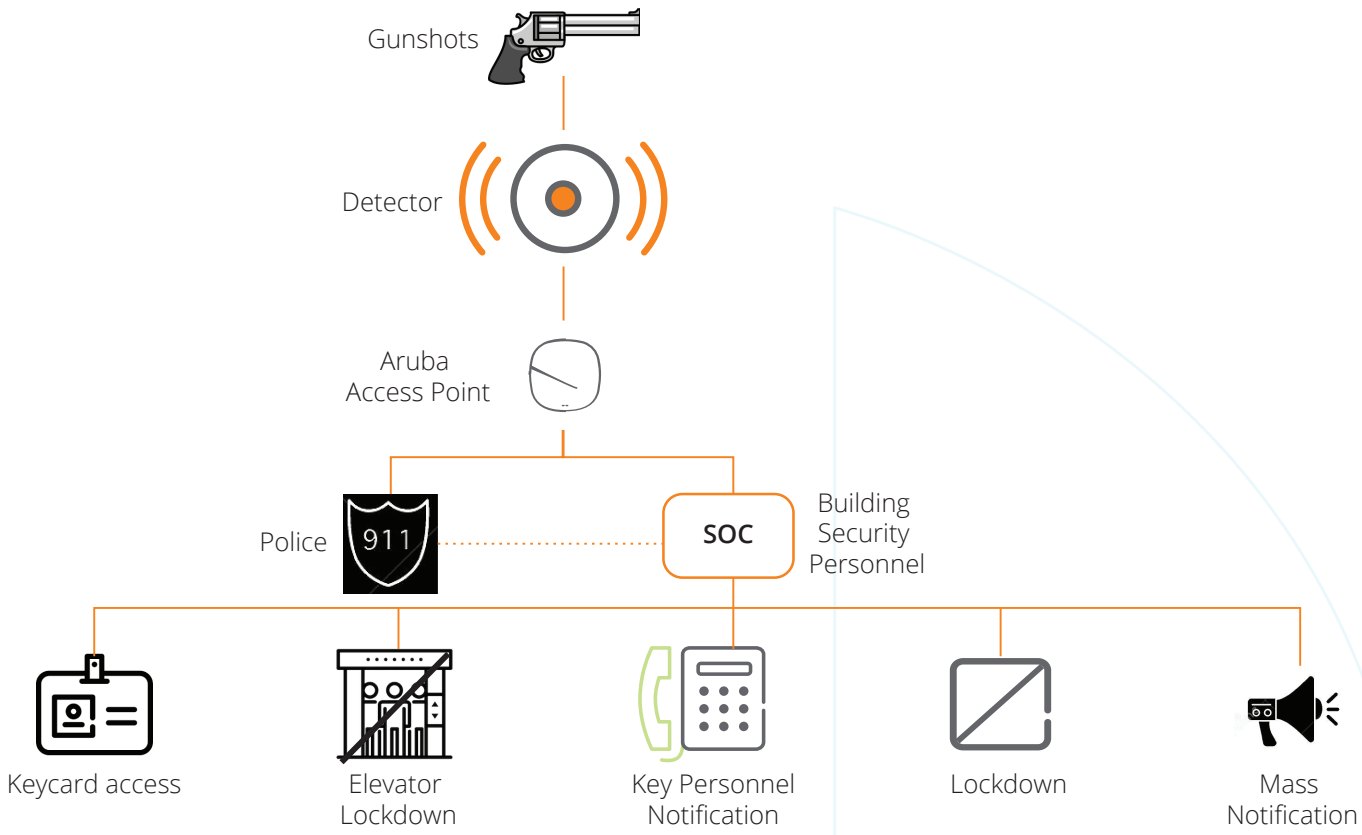


Figure 21: AmberBox Gunshot Detection And Notification System

The sensors use acoustic and infrared data to recognize when firearms are discharged. Within roughly 3.6 seconds, the sensor identifies the actual gunshot signature and relays an alert using the USB port. Access points use secure tunnels to relay data to the AmberBox monitoring application. Automatic alerts can then be sent to law enforcement via the AmberBox cloud-based e911-certified platform, with additional notifications to building security or other responding parties. A conference call line is automatically established to share information and coordinate efficiently.

AmberBox can also immediately activate facility security systems while alerting personnel with SMS, e-mail and call notification. Real-time shooter location tracking can be viewed through the Web or a mobile response platform.

Dynamic segmentation of IoT traffic is maintained throughout the Aruba infrastructure, protecting the rest of the network against compromised devices. Aruba switches automatically set-up secure connections with Aruba access points without the need for separate VLANs, regardless of the switch port into which they're connected. This feature simplifies the initial deployment of the access points, and minimizes opportunities for miswiring during adds, moves, and changes over the life of the deployment.

Key benefits of a jointly deployed solution include:

- Gunshot detectors can be placed where needed without new cabling or PoE injectors;
- No maintenance required, unlike with battery operated systems;
- Uses existing Aruba access points and leverages Aruba security mechanisms; and
- Supplements security solutions from Aruba and other partners including occupant safety monitoring, video surveillance, door locking controls, and wayfinding solutions.

Jointly deployed with AmberBox sensors, Aruba access points dramatically improve situational awareness so first responders know what they are facing on arrival.

CONTEXT-AWARE, REAL-TIME INTEGRATED EMERGENCY RESPONSE AND NOTIFICATION

Building security teams have an obligation to protect the wellbeing of people who work in, visit, or travel through their headquarter buildings, warehouses, stores, and other facilities. Posted evacuation plans and audio/visual alarms are often considered sufficient for this purpose, but in reality, they aren't. During an incident people need context-relevant information pushed to them to keep them safe under highly fluid circumstances.

Moreover, first responders need the ability to communicate in real-time with those in imminent danger, who need assistance exiting the facility, and who are in safe areas but don't know it. Active communication can often make the difference between a well-managed incident and a nightmare scenario.

criticalarc

CriticalArc is a global technology innovator and the creator of the distributed command and control solution, SafeZone®, which has been adopted by enterprises across the world. SafeZone fundamentally transforms the way organizations manage safety and security operations across multi-site organizations, by providing real-time situational awareness to maximize response and minimize the impacts of an incident.

Through a cloud service and dedicated applications for responders, Security and Emergency Directors and their teams have a real-time view of the location and status of all potential responders and assets at their disposal and the means with which to communicate critical information. This ensures the optimal response to any situation as it occurs.

In addition, having the SafeZone app enables an organization's staff to call for help or actively receive details about events near them. With a mobile app for Apple or Android, users can take advantage of the mobile device that they carry with them. If they see or are involved in an emergency situation, they can use their mobile device to notify applicable authorities.

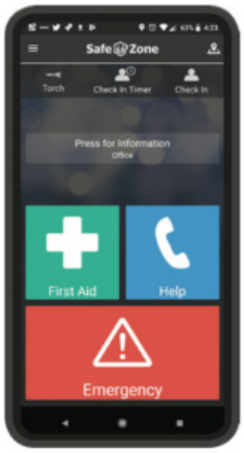


Figure 22: CriticalArc SafeZone Mobile App

If an employee is currently at a facility that is experiencing an event, based on their current location, the app can pro-actively notify them of the situation and provide them instructions on how to navigate to safety. Additionally, the SafeZone platform is SaaS-based, highly scalable, built on enterprise class infrastructure and can be operational within a month.

The SafeZone system allows security teams to define the protocols for how they respond. Often clients have different protocols for different situations, for example, in a chemistry lab. Accurately understanding which areas are occupied, and by whom, enables security teams to respond more effectively and save lives in the process.

Patrocinium™

Patrocinium, in partnership with Aruba, addresses integrated emergency response and notification by combining Meridian indoor location services with an innovative mobile app. The solution informs people of incidents and what actions should take based on danger in or near their specific location. Communication occurs in real time with tenants, visitors, and staff, and unique 4D graphics enables first responders to see where people are situated within buildings.

Figure 23: Meridian-Based Patrocinium Emergency Response Platform

All that is required for 4D support is a Meridian subscription and Aruba Beacons, standalone or embedded within Wi-Fi access points, throughout the facility. Patrocinium's app leverages Meridian's maps and indoor location, in addition to GPS, to provide a new level of visibility. Unlike GPS-only based location services that cannot differentiate between floors, Aruba's BLE indoor location incorporates that critical 4th dimension

Generic crisis management and emergency notification tools that use text, e-mail, social media, and audio/visual alarms to alert people of danger fall short because they can't isolate those in danger from other occupants or provide real-time situational awareness.

Working together, the Patrocinium Platform and Meridian location services fill this critical gap. Doing away with lists and opt-in workflows. Patrocinium instead uses patented software to automatically notify occupants when they are within a danger zone geofence without first signing up for alerts. To protect user privacy, Patrocinium's geofencing technology only visualizes individuals' locations when they are in or near danger or need assistance.

This event-triggered process generates an immediate, personalized flow of information to anyone at risk of being affected by an incident. Occupants are shown their location, relevant pushed updates, perimeters, and safe zones. If help is needed it's one button-push away. In essence, users become sensors for the security team.

Key benefits include:

- Situational awareness indoors so users can see their location relative to incidents, fire extinguishers, exits, and other safety-related data;
- Wayfinding guides users to stairwells, exits, and designated outdoor muster areas;
- A4D picture with longitude, latitude, floor number, and time gives first responders more details than they could obtain from just GPS;
- Exact location is presented when a user declares themselves safe/unsafe via the mobile app;
- Easily integrates into existing branded mobile apps - a dedicated app is not required;
- Responders can send specific information to targeted recipients; and
- Incident recording ensures that all relevant data are saved for digital auditing and reporting.

Patrocinium and Aruba have created an event-triggered process that generates an immediate, personalized flow of information to those affected by an incident. Employees and visitors can see their location relative to an incident, send and receive updates, and see perimeters and safe zones.

SECURELY SHARING RETAIL NETWORKS WITHOUT LOSING CONTROL

Retail wireless network access is typically tightly controlled out of concern that critical services and devices, such as staff Wi-Fi calling, or PoS data transfers could be negatively impacted by wireless users. Payment Card International (PCI) and related compliance rules dictate minimum network security standards, and failure to comply can result in heavy fines. That said, growing demands for mobile device wireless access to enhance worker efficiency, productivity and safety increase pressure to open up wireless networks and avoid the cost and RF interference of parallel networks. IT, facilities, and compliance organizations are struggling to find a mutually acceptable solution.

Several years ago, the US Department of Defense (DOD) encountered a very similar situation. There was pressure to use one common network to support secret (SIPR) and non-secret (NIPR) traffic. These distinct traffic flows were managed by different groups, each of which needed total control over who access to the traffic they manage. Security was paramount, and there could be no sharing of data across groups or unauthorized network access within a group.

Aruba solved the issue by developing MultiZone, a networking solution that allows each of up to five groups to define authentication, access, operation, and management rules applicable to, and enforced within, their unique "Zone." One Aruba controller is assigned to the Primary Zone, managed by IT, which handles access points and RF settings, and directs access points to authenticate to Data Zone controllers. Separate Data Zone controllers handle authentication, access, operation, and management rules for the SIPR and NIPR groups. MultiZone supports up to five Data Zones.

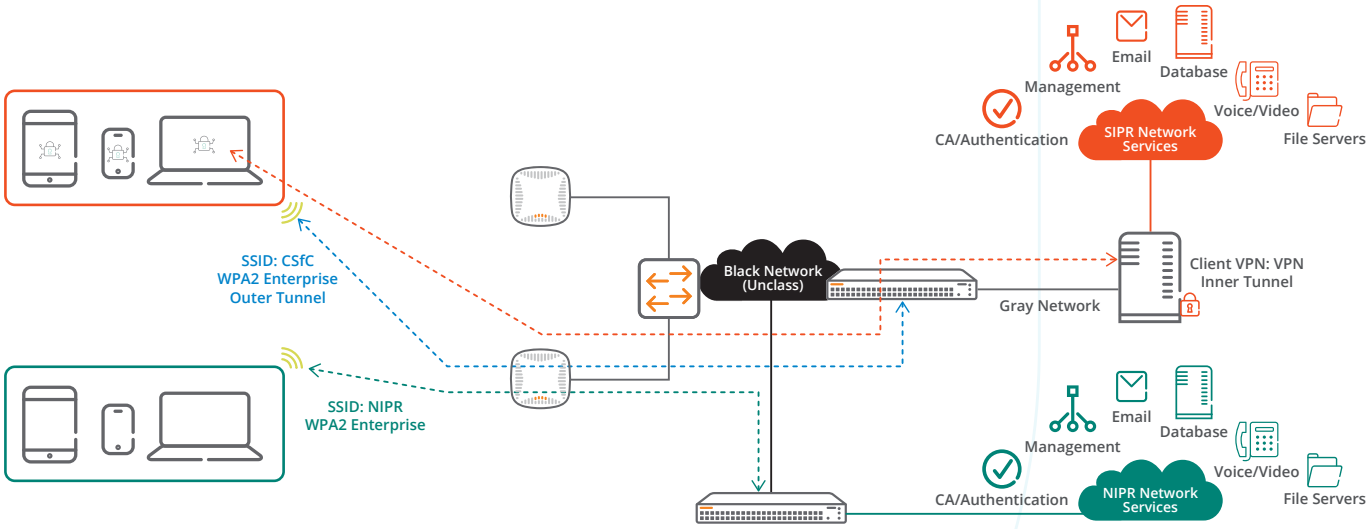


Figure 24: Aruba Multizone Solution

The multi-tenancy design of MultiZone is ideal for retail applications. Separate Data Zones can be allocated to the groups managing, say, building and refrigeration controls, inventory auditors, shoppers, and of course corporate services. Each group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services.

In a MultiZone system IT manages the overall infrastructure through the Primary Zone but cannot access Data Zone traffic. Uniform visibility and security can be achieved while simultaneously respecting the access control rights of Data Zone owners.

SEAMLESS 5G TO WI-FI 6 ROAMING WITHOUT DISTRIBUTED ANTENNA SYSTEMS

If you can't connect with people and machines inside a store or warehouse, then you can't extract or share information. The prevalence of low-emission glass, energy-efficient construction materials, and evolving building codes have made indoor wireless coverage from outdoor cellular networks a recurring challenge. This results in inconsistent experiences for mobile users and devices as they roam in and out of stores and warehouses. These problems are compounded with high-speed 5G, which operates at higher frequencies that do not penetrate indoors as far as 3G or 4G cellular.

For decades, indoor cellular issues have been addressed by deploying distributed antenna systems (DAS). This expensive infrastructure operates as extended antennas for one or more cellular carriers. More recently, indoor small cell (also called "femtocell") networks have been deployed by individual mobile network operators (MNOs). Unlike DAS, a separate layer of equipment is required for each MNO. Both DAS and small cells are complex, very costly, and are rarely cost effective for facilities with less than 200,000 ft2 (20,000 m2) - the bulk of commercial properties worldwide.

Over 150 MNOs in nearly 50 countries have embraced Wi-Fi Calling. This service leverages the existing Wi-Fi network, which when properly designed provides pervasive coverage throughout a building. 5G includes support for Wi-Fi 6 integration as a radio access network (RAN), so building owners do not need to choose between 5G and Wi-Fi 6: Wi-Fi Calling and other services can be performed over both. For this reason, wireless LANs are the premier and most economical onramps for indoor cellular devices.

Aruba Air Pass is the industry's first seamless cellular roaming solution designed to unify enterprise and mobile network experiences. The service enables smart building 5G initiatives - including visitor and IoT device on-boarding and roaming - to be accomplished with enterprise-class security over Wi-Fi 6 without the high cost of a DAS or issues with inconsistent cellular connectivity.

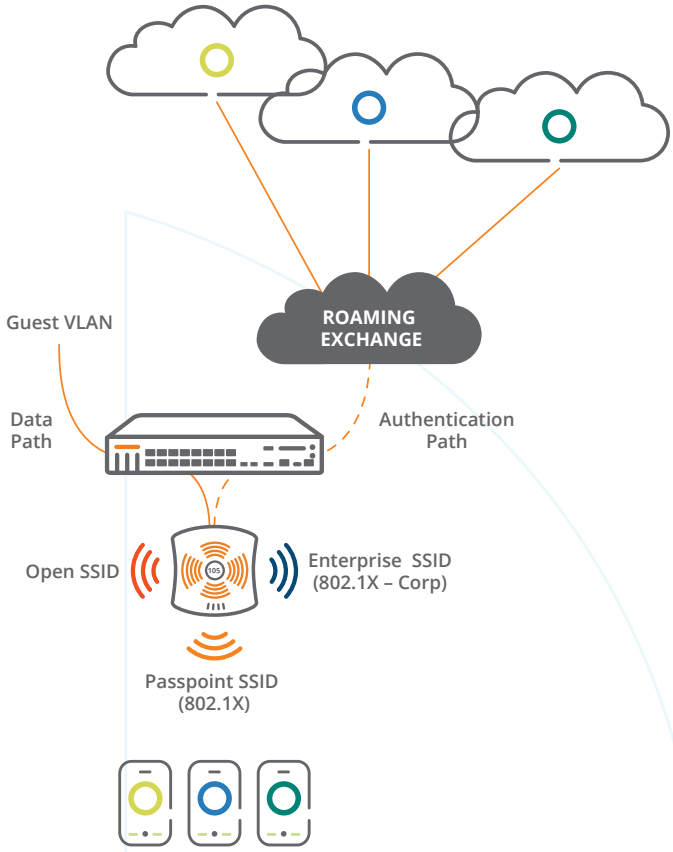


Figure 25: Aruba AirPass System Architecture

Air Pass uses pre-negotiated agreements with MNOs that support the Wi-Fi CERTIFIED Passpoint standard to automatically gain network access using cellular SIM credentials for authentication. No captive portals, usernames, or passwords are required. Aruba ClearPass provide high security network access control so that public and private resources remain secure and separate. Mobile subscribers, and Passpoint-capable IoT devices, can then roam between the cellular and Wi-Fi networks in compliance with IT security standards.

Air Pass is managed by Aruba Central, a massively scalable cloud-based network operations, assurance, and security platform. Aruba Central simplifies the deployment, management, and orchestration of wireless, wired, and SD-WAN environments. This includes delivering 5G and Wi-Fi 6 to the network and customer edge, complete with built-in and third-party services.

IoT devices are increasingly accessing cloud services to support applications like digital twins and augmented or virtual reality. Air Pass leverages Air Slice for SLA-grade application assurance by dynamically allocating radio resources such as time, frequency, and spatial streams to specified users, devices, and applications.

Reliably connecting people and IoT devices inside a building is essential for context-aware engagement, safety, and security. Air Pass marks an end to a dependence on expensive DAS systems. It also overcomes connectivity, security, and convenience issues associated with indoor cellular coverage gaps, insecure open wireless networks, manually hunting for Wi-Fi networks, and the inconvenience of navigating captive portals. Secure connectivity is assured regardless of where people and IoT devices work or roam.

CONNECTING AND PROTECTING REMOTE STORES AND WORKERS

Industry analysts have long opined that the rise of smart machines, cognitive technologies, and algorithmic business models will be more influential than labor arbitrage in driving profitability and enhancing productivity. Smart machines will accomplish this by classifying content, finding patterns, and extrapolating generalizations from those patterns. There is no denying the central role of IoT on the journey by retailers to run their businesses more efficiently, productively, and profitably. The underpinnings of IoT are the sensors, actuators, and related control systems that for decades have been running stores, warehouses, and corporate offices.

Large, geographically-distributed retailers can have buildings and stores spread across a broad areas, and depending on the location it could be unattended for large parts of the day or night. Remote sites are particularly at risk of break-ins and cyber-attacks because of the vulnerability of IoT devices running inside them, and the complexity of setting up and managing secure remote access solutions.

Virtual private network (VPN) access has historically been essential for security and vexing to set up: the labor savings that come from centralized VPN management are often offset by the complexity of system configuration and modifications. Additionally, VPNs don't protect endpoints or data at rest, and need to be supplemented with firewalls, intrusion protection systems, and other endpoint defenses. These solutions can be difficult to integrate with IoT devices and confusing for users because the remote access methods – like VPN authentication – differ from those used at corporate facilities.

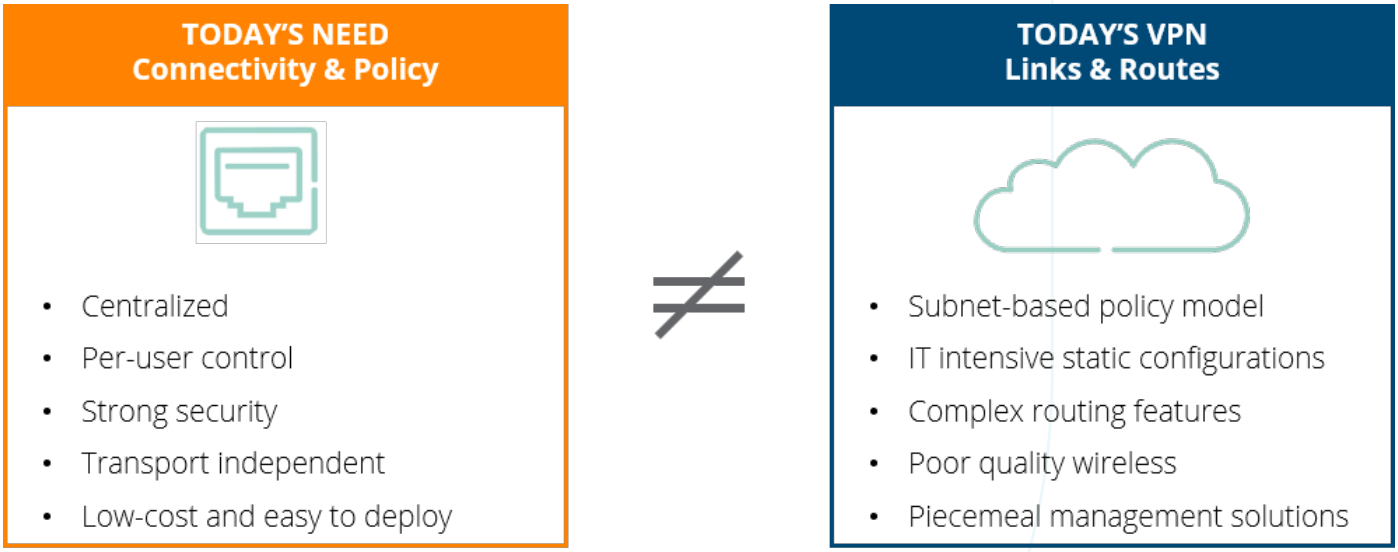


Figure 26: Limitations Of Traditional VPNs

Aruba addresses these issues by simplifying remote site access and connectivity to IoT devices. Solutions are tailored to the type and number of IoT devices on site.

If the remote site uses a standalone IoT refrigeration, lighting, or other controller running Linux, Windows, iOS, MacOS, or Android operating systems, Aruba's VIA VPN Client application can be used. VIA can also be used by field engineers and contractors using ruggedized laptops or tablets. VIA scans and selects the best Ethernet or broadband connection from the IoT device to the main building network. Unlike traditional VPN clients, VIA offers a zero- touch experience and automatically connects to an Aruba VPN concentrator controller on which it has been whitelisted.

Retailers on military bases can run the VIA Suite B VPN client. The client is a hybrid IPsec/SSL VPN, which when used in conjunction with an Aruba VPN concentrator controller running the Aruba OS Advanced Cryptography (ACR) module, ACR supports elliptic curve cryptography validated for classified information.

VIA sets up a secure, encrypted tunnel to an Aruba VPN concentrator controller at the retailer's operations center. The controller r terminates the VPN tunnels, manages identity assignment, centralizes encryption, and runs Aruba's unique role-based firewall. Every IoT device and field support laptop/tablet is assigned a unique identity by the role-based firewall to regulate how and when the device connects to and uses the network. Identity follows the devices, regardless of how or where they connect to the VPN network.

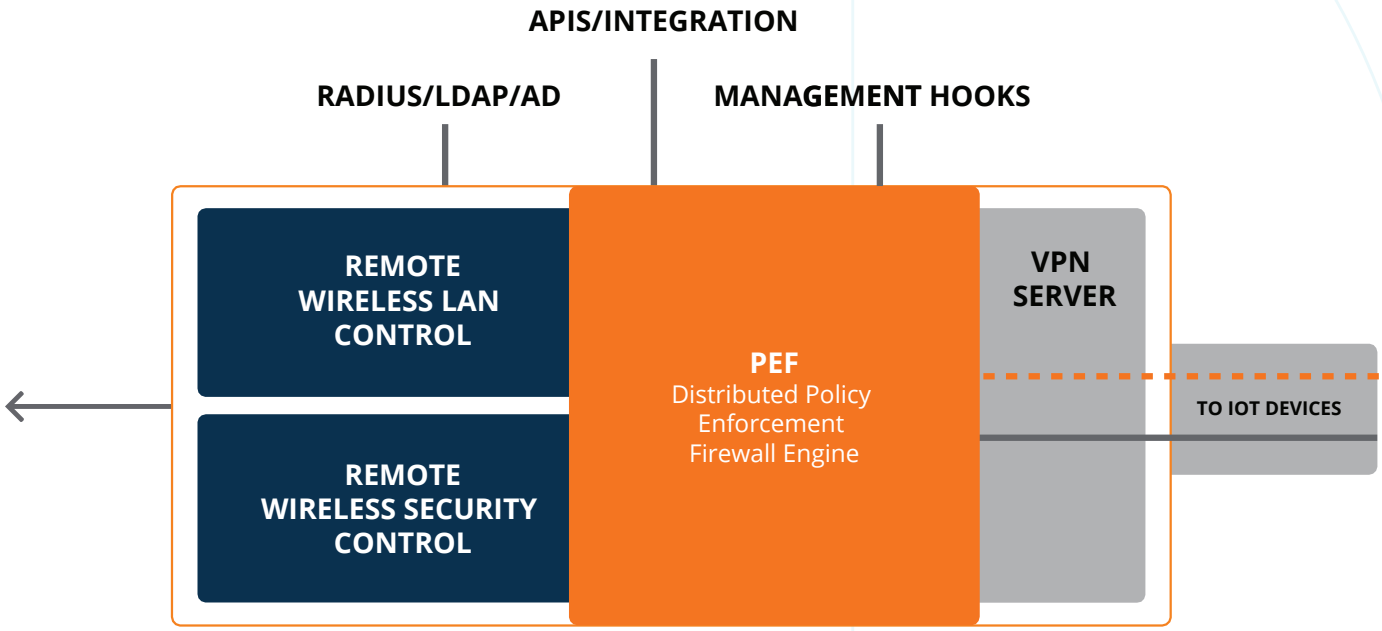


Figure 27: Aruba VPN Concentrator Controller

IoT device MAC addresses can be spoofed, so the identity of headless devices needs to be supplemented by the controller with strong authentication protocols (like 802.1x) and role-based contextual data. These data include location, time of day, day of week, and current security posture, and are used to provide more granular role-based access control.

A role is applied during the authentication process, before the device has network access, using Active Directory, RADIUS, LDAP, or comparable data. Unlike simple Access Control Lists (ACLs), Aruba's stateful role-based firewall will actually track upper-layer flows to ensure that unauthorized traffic can't bypass access control. For example, a packet claiming to be part of an established Telnet session would be blocked unless there was an actual established Telnet session underway.

Many remote sites have multiple IoT devices, devices that cannot run a VIA client, and/or need a secure local Ethernet and/or Wi-Fi network. In these instances, a Remote Access Point (RAP) can be used to provide secure remote connectivity to Ethernet or Wi-Fi based IoT devices using a broadband WAN and/or cellular connection. Like VIA, a RAP uses a zero touch mechanism to set up a secure, encrypted tunnel with an Aruba VPN concentrator controller at the plant or data center. Stores on military bases can use Suite B on TAA-compliant RAPs. Unlike VIA, RAPs include local Ethernet ports, Wi-Fi access, and the option to plug-in a cellular modem for primary or redundant back-up wide area communications.

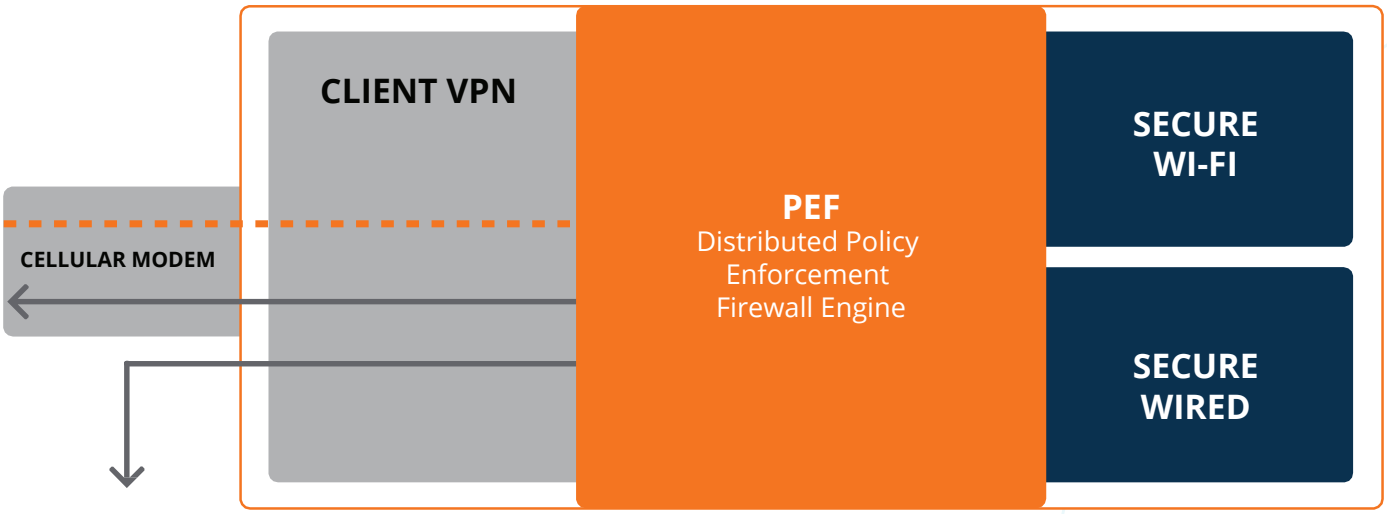


Figure 28: Aruba Remote Access Point

A side benefit of role-based access is that controls are available to optimize the bandwidth utilization of Wi-Fi enabled devices. Since Wi-Fi is a shared medium, significant benefits accrue from limiting the maximum amount of bandwidth consumption for some devices and guaranteeing a minimum bandwidth level for others. These mechanisms help limit the impact of denial of service attacks while allowing critical IoT devices to continue operating.

IoT devices and field support laptops/tablets are authenticated, and data encrypted, without any client software or manual intervention. The result is high security connectivity with remote IoT sites and users that is easily configured, requires no user training, and delivers a plug-and-play IoT monitoring experience.

An example remote monitoring application is shown below. In this case the objective is to remotely supervise an air conditioning chiller that has I/O information of value to facility management and energy optimization applications. The chiller has an available Ethernet port but lacks modern security features or VPN support. The Ethernet port is connected to a RAP, which establishes a secure IPsec tunnel via Internet broadband with a cellular back-up. Chiller I/O data are streamed thru the tunnel to the retailer's IoT application. RAP updates are pushed automatically from time to time, and no manual or local intervention

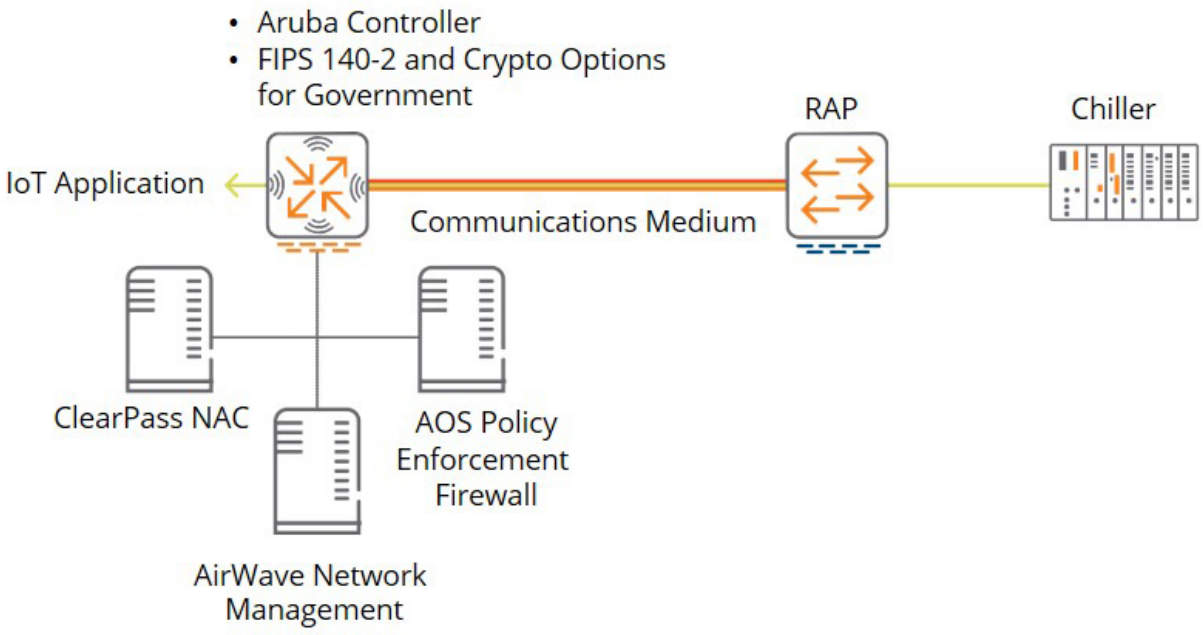


Figure 29: Remote Chiller Monitoring

For sites than need secure, high-bandwidth connectivity with back-up communication paths with service level agreements, a software defined WAN may be appropriate.

Larger remote sites may benefit from a wide area network (WAN) connection. Traditional WAN infrastructure is complex, and on a large scale can require hundreds of routers, firewalls, and network security systems. Provisioning and maintaining Multiprotocol Label Switching (MPLS) and other dedicated WAN links is time consuming and can require expensive on-site configuration and maintenance. Direct Internet Access (DIA) services are less expensive than MPLS, however, best path selection for applications requires probing paths and mapping flows.

Aruba's SD Branch solution addresses these issues by providing a central point for configuring routing and access control policies, and a simple means of pushing those policies to the remote sites. There is no on-premise management equipment to update or maintain. WAN management is orchestrated through the Aruba Central cloud, from which it's easy to distribute routes and build secure, scalable VPN tunnels on demand. Aruba Central can monitor where traffic enters and exits a remote site, regardless of uplink type, making it easy to manage WAN environments using public WAN connections.

To ensure uniform security, access policies dynamically follow IoT devices (such as replacement parts) and field support tools (like ruggedized laptops and tablets) as they move between stores and warehouses. High availability active/active and active/standby modes deliver full redundancy for sites that need it.

SD-WAN Gateways located at remote sites are designed to support multiple broadband, MPLS, or cellular links. Policy-based routing ensures that traffic can be routed across multiple private or public WAN uplinks based in the traffic type, link health, device profile, user role, and destination. Traffic can be routed over the best available uplink based on factors such as throughout, latency, jitter, and packet loss.

Regardless of whether you need to connect a small remote store or a large cold-storage warehouse, Aruba has you covered.

SUMMARY

The availability of IoT data and relevant context enables retailer to adapt to the environment and occupants. The richer the set of available data and context, the more adaptive the retailer's sites can become.

Key technology partners - working in concert with Aruba's ESP-based unified infrastructure, zero-trust security, and AI powered solutions - enable retailers to boost efficiency, productivity, reliability, safety, security, and profitability while ultimately driving profits and delighting customers.

Please contact us for more information on how we can help your retail store, warehouse, or distribution center make the digital transformation to hyper-awareness.

CITATIONS

[1]William H. Markle, "The Manufacturing Manager's Skills" in *The Manufacturing Man and His Job* by Robert E. Finley and Henry R. Ziobro, American Management Association, Inc., New York 1966

[2]C. R. Jaccard, "Objectives and Philosophy of Public Affairs Education" in *Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation*, Chicago, Illinois 1956

[3]A business moment is a transient set of context-sensitive interactions between people, business, and things that yield a negotiated result as opposed to a predetermined result, i.e., a personalized, targeted offer from a retailer based on location, time, and CRM data. See Frank Buytendijk, Digital Connectivism Tenet 4: *We Do Not Differentiate Between People and Things*, Gartner, 1 November 2016.

[4]McKinsey Global Institute, *Unlocking The Potential Of The Internet of Things*, June 2015

aruba
a Hewlett Packard Enterprise company

WP_DesigningHyper-AwareRetailFacilities_RVK_111820 a00107711enw

Contact Us **Share**