WHITE PAPER

aruba
a Hewlett Packard Enterprise company

DESIGNING HYPER-AWARE HEALTHCARE FACILITIES

SECURE INFRASTRUCTURE AND PARTNER SOLUTIONS FOR HEALTHCARE INSTITUTIONS INCLUDING ACUTE AND AMBULATORY CARE, CLINICS, ASSISTED LIVING, AND LONG-TERM CARE FACILITIES

TABLE OF CONTENTS

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 positive patient outcomes. In healthcare facilities, machines and applications are focused on optimizing human activity monitoring, organizational redesign, augmented reality, human productivity, and 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 healthcare technology partners whose products and services interface with ESP to address patient monitoring, healthcare operations, and facilities applications.

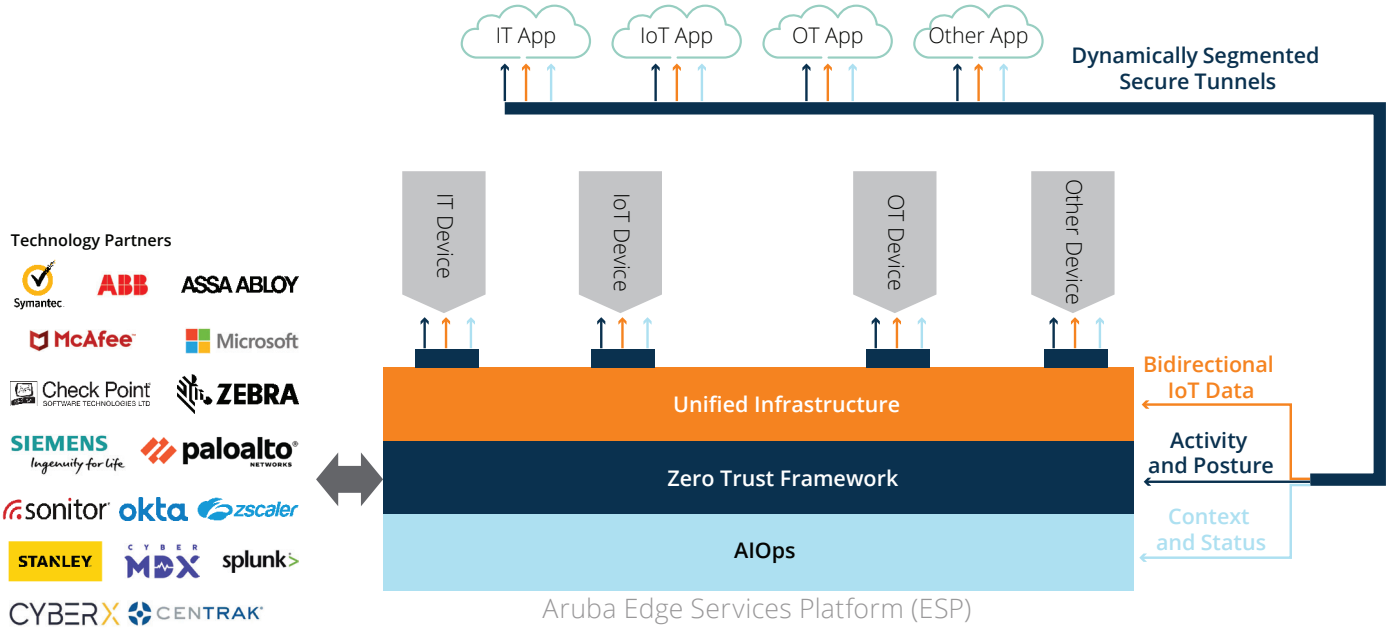


Figure 1: Aruba ESP And Technology Partner Ecosystem: The Foundation For Hyper-Aware Solutions

Solutions from Aruba and its technology partners span the healthcare market including clinical spaces, acute and ambulatory care, assisted living, and long-term care facilities in addition to non-clinical spaces used for business operations. Use cases and partners discussed in this white paper include:

- Monitoring and Treating Illness
  - Physical Distance Monitoring And Contact Tracing (AiRISTA Flow, AisleLabs, CohuHD, CXapp, Kiana, SkyFii)
  - Biomedical Device Connectivity (B Braun, Dräger, GE, Hill-Rom, Philips, Nihon Kohden)
  - Non-invasive Resident Monitoring (Tellus)
- Improving Wellness
  - Hand Hygiene Compliance to Reduce the Spread of Disease (AiRISTA Flow, CenTrak, Sonitor, Stanley)
  - Location-Aware Patient Engagement, Compliance, and Telemedicine (Emerge Interactive)
- Human Productivity Optimization
  - Measuring and Improving Patient Flow to Reduce Wait Times and Increase Revenue (Hypros, MySphera)
  - Improving Patient-Facing Staff Efficiency When Locating Biomedical Devices (AiRISTA Flow, CenTrak, Sonitor, Stanley)
  - Enhancing the Reliability and Quality of Mobile Staff Communications (Ascom, Mobile Heartbeat, Spectralink, Vocera, Zebra)
  - Automating Guest Network Access to Enhance Staff Efficiency (Aruba, Envoy)
  - Migrating From Break-Fix To Proactive Maintenance (ABB)
- Connectivity, Physical, and Cyber Security
  - Mobile Duress Alarms for Enhanced Staff and Physician Safety (AiRISTA Flow, CenTrak, Sonitor)
  - Vaping and Air Quality Monitoring (IP video)
  - Gunshot Detection (AmberBox)
  - Context-Aware, Real-Time Integrated Emergency Response and Notification (Meridian and Patrocinium)
  - Securely Sharing Healthcare Wireless Networks Without Losing Control (Aruba MultiZone)
  - Seamless 5G To Wi-Fi Roaming Without Distributed Antenna Systems (Air Pass)
  - Connecting and Protecting Remote Clinics and Workers (VIA, RAPs, SD-Branch)
  - Securing Healthcare Networks That Can't Protect Themselves (CyberMDX, Medigate)

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

Before the advent of interconnected networks, healthcare systems operated autonomously from each other, with independent patient recordkeeping systems, analog medical devices, and local applications for nurse call, 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 in patient rooms; and so on.

The move from paper patient records to local and then interconnected EHR systems is one of the evolutions that has driven the move to digital connectivity. Now biomedical device manufacturers can add features that will insert a patient's monitoring data directly into their digital record. Digitized copies of analog imaging can also be stored in a patient's digital records, eliminating the need for paper files and making the images more broadly accessible.

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 healthcare applications need access to edge data to deduct status and infer occupant needs. For example, an automated meeting room reservation system needs identity, presence, calendar, and location data to know when attendees are present so a meeting can start, and to infer when a room can be released due to non-use. Physical layer and protocol converters can address data exchange, however, trusting IoT systems enough to share context and data in a regulated healthcare environment is highly problematic.

IoT devices are fundamentally untrustworthy, making them the 'Achilles heel' of healthcare 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.

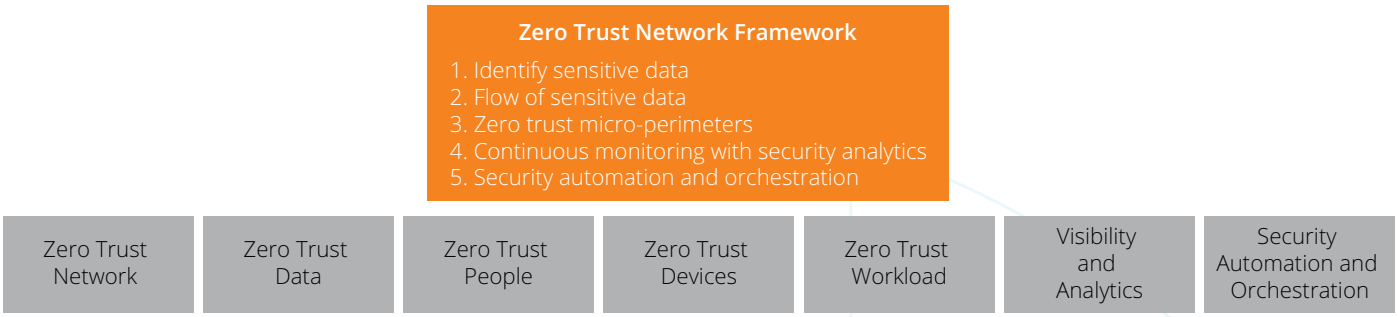


Figure 2: Zero Trust Framework

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 biomedical 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.

Due to its nature and long technology approval cycles, the healthcare market is very conservative, and the rate of technological change has been significantly slower than the consumer product industry. With the need and incredible responsibility to protect personal patient health information, cybersecurity has to underpin all healthcare systems. At the same time, location services play an essential role in many healthcare applications, including asset and patient tracking. Yet neither cybersecurity nor location-based services are core skills of many healthcare vendors – both have long been the province of IT. And then there's analytics, a family of highly specialized tools that help providers secure and monetize the data they collect, which is yet another province of IT.

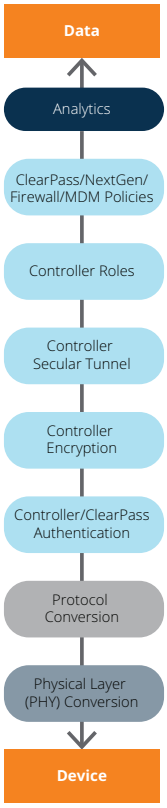


Figure 3: IoT Protection Mechanisms

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 healthcare 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 will allow the strategic healthcare business goals of providing better patient care without incurring unacceptable risk. Let's now examine how to align a company's strategic goals with the implementation of hyper-aware healthcare.

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 healthcare 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 healthcare, that relevance is typically determined on cost management and improving patient care and outcomes.

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 healthcare professional or patient. 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.

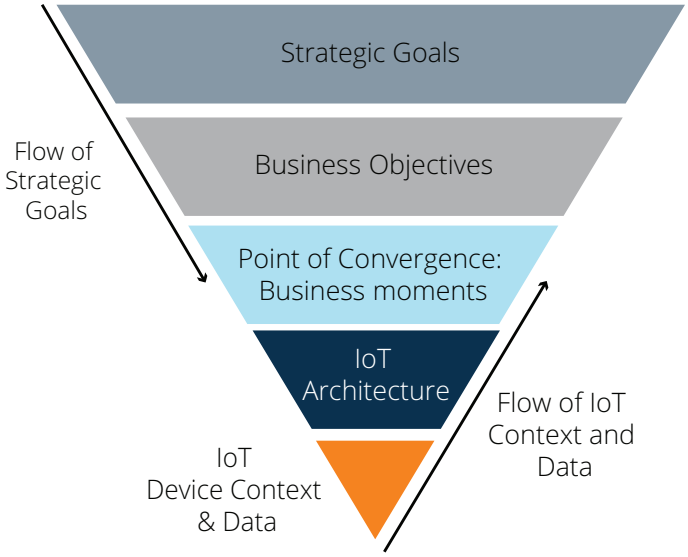


Figure 4: IoT Strategic Hierarchy

And so, we return full circle to the professor and the woodsman. The first order of business in any healthcare 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 healthcare 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 reduce patient wait times and/or improve patient flow? Enhance personal safety with social distancing and thermographic monitoring? Reduce the time spent searching for costly biomedical devices? Drive a loyal and more connected digital-relationship with patients via a branded mobile application? The answer(s) will impact the business moments that need to be delivered, and what constitutes relevant data and context.

Business moments inform the IoT architecture, not the other way around. One-size-fits-all healthcare 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 healthcare applications. Most of the use cases include at least one Aruba technology partner whose solution, used in concert with Aruba infrastructure, helps address strategic healthcare challenges.

HEALTHCARE MARKET

According to McKinsey4 the total economic impact of IoT in human health and wellness in 2025 should reach between $170B-$1.6T. The top identified areas include monitoring and treating illness ($171B-$1.0T) and improving wellness (up to $519B):

- Monitoring and treating illness – Up to 20% reduction in disease burden
- Improving wellness - $80-600 per year in wellness benefits per user

The breadth of healthcare 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., providing panic buttons to all staff members because of a recent event? Or is an optimized system-level solution required, i.e., migrating from hoarded biomedical devices to enabling staff to find the devices they need in real-time?

Where healthcare capacity is constrained in the developing world, IoT has the potential to expand the number of patients that physicians and other care providers can treat.[4]

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

- Local patient data privacy requirements;
- Challenges when medical staff want to use personally-owned devices (BYOD) to access patient records;
- Impact of migrating to electronic medical records (EHR);
- Growing numbers of cyber attacks on healthcare organizations;
- Using automation to address medical staff burnout;
- Zero downtime requirements; and
- Patients' desire to access care and information from anywhere via personally-owned digital devices.

All must be balanced with the need and desire to provide value-based care.

In every case, an extensible platform will be needed so customers can both build a broad range of services today and accommodate 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 improve patient care are presented below.

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 other workers 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 healthcare 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 5: 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.

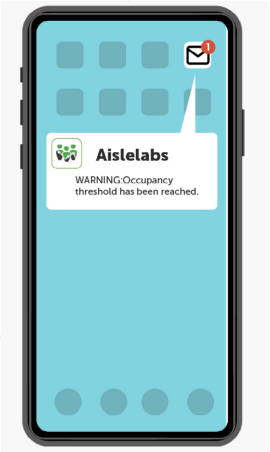


Figure 6: AisleLabs COVID-19 Social Distancing Solution

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.

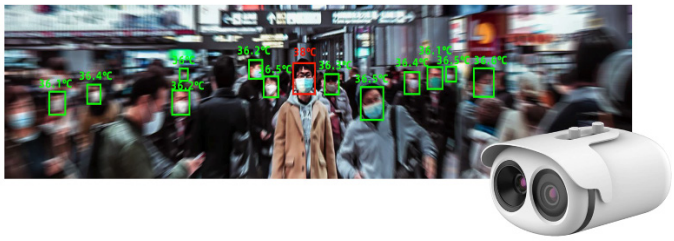


Figure 7: CohuHD Non-Contact Thermographic And Facial Recognition Camera

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 physicians, staff, patients, and guests per square foot/meter, all based on real-time occupancy within the environment.

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.

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.

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.

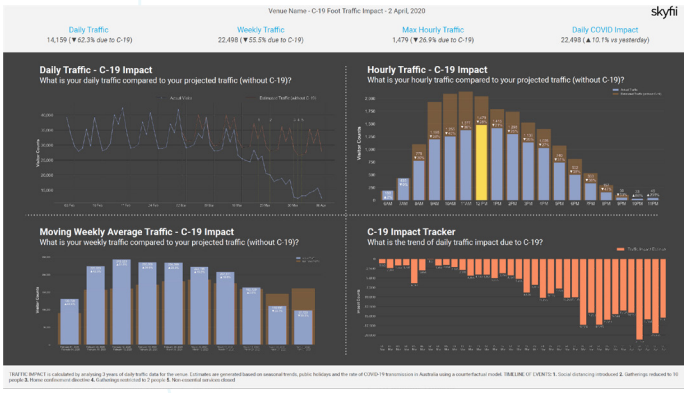


Figure 8: SkyFii OccupancyNow Dashboard

BIOMEDICAL DEVICE CONNECTIVITY

Using medical devices to monitor patients was one of the earliest IoT applications. The explosion of battery-operated mobile devices, network-connected data collection and recording systems, and compliance monitoring systems have driven up the number of biomedical devices connecting to wired and wireless networks. Many of these new devices can now directly insert monitoring data into a patient's EHR.

Biomedical devices include connected beds, infusion pumps, portable MRI, CAT scan, syringe pumps, pulse oximeters, heart rate monitors, to name just a few. These devices typically have very long-life operating lives, and many network-connected devices in use today use outdated communication and security standards that require special handling by the network infrastructure.

Aruba has partnered with these vendors to ensure that their devices will interoperate reliably and integrate with Aruba's zero trust framework. Features like Adaptive Radio Management (ARM) and deep-packet inspection ensure that the devices receive the quality of service they require in densely deployed healthcare settings. ARM uses infrastructure-based controls to optimize Wi-Fi client behavior, minimize interference, and enhance roaming. The result is more reliable, higher performance throughput and roaming mobile biomedical devices.

B. Braun Medical Inc., a leader in infusion therapy and pain management, develops, manufactures, and markets innovative medical products and services to the healthcare industry. Aruba securely connects B Braun infusion pumps via Wi-Fi to allow them to communicate with the B. Braun DoseTrac© infusion management software. Aruba APs can be used as IoT platforms without the need to install a parallel network. This allows healthcare facilities with B. Braun devices to leverage their investment in wired and wireless Aruba infrastructure while also benefiting from the security solutions that Aruba provides.

Dräger is a leading international company in the fields of medical and safety technology. Aruba securely connects Dräger patient monitoring equipment via Wi-Fi. Draeger developed the Infinity OneNet solution to enable patient monitoring information to be transmitted over the hospital's existing WLAN. This enables healthcare organizations to greatly reduce the management overhead of the networks, since they only need to support one system, instead of purchasing a dedicated system for patient monitoring alone.

Infinity OneNet works by guaranteeing bandwidth availability on the WLAN. Infinity OneNet is both a network architecture and a comprehensive suite of professional services that allows the existing network to provide patient monitoring in parallel with commercial and administrative applications.

Hillrom draws on a combined heritage of more than 450 years of innovation and excellence with Hillrom, Allen Medical, Liko, Mortara, Trumpf Medical, Voalte and Welch Allyn product brands, to provide solutions that enhance outcomes for patients and their caregivers.

The combination of Aruba's mobile-first networks and Hill-Rom patient monitors and central stations can transform any healthcare setting into a center of excellence. Hill-Rom provides a variety of patient monitoring systems, from the Propaq line designed for bedside, transport, or ambulatory use, to the Micropaq monitors designed for patient wear. All these devices are geared to collect patient health information and transmit it to the Acuity health monitoring station using the Wi-Fi network. The user-centric solution from Aruba ensures that the data collected from the various devices is secured and transmitted reliably to the monitoring station.

Most of the patient monitoring data carried across the WLAN network is delay and loss sensitive. The Aruba Wi-Fi infrastructure ensures that the traffic receives the right QoS level and is delivered reliably with low latency and loss.

GE Healthcare provides medical technologies, digital infrastructure, data analytics and decision support tools that help healthcare professionals diagnose, treat and monitor their patients. Aruba can securely connect to GE biomedical devices via wired or wireless. Aruba APs can be used as IoT platforms to collect imaging data without the need to install a parallel network. This allows healthcare facilities with GE solutions to leverage their investment in wired and wireless Aruba infrastructure while also benefiting from the security solutions that Aruba provides.

Nihon Kohden is Japan's leading maker of EEG, patient monitors, AED, and medical electronic equipment. Aruba can securely connect to Nihon Kohden biomedical devices via wired or wireless. Aruba APs can be used as IoT platforms to collect telemetry data without the need to install a parallel network. This allows healthcare facilities with Nihon Kohden biomedical devices to leverage their investment in wired and wireless Aruba infrastructure while also benefiting from the security solutions that Aruba provides.

Philips Healthcare provides wired and wireless diagnostic, patient monitoring, and imaging solutions across almost all areas of healthcare. Aruba can securely connect to Philips biomedical devices via wired or wireless. Aruba APs can be used as IoT platforms to collect telemetry data without the need to install a parallel network. This allows healthcare facilities with Philips biomedical devices to leverage their investment in wired and wireless Aruba infrastructure while also benefiting from the security solutions that Aruba provides.

NON-INVASIVE RESIDENT MONITORING

Non-invasive monitoring of at-risk patients is challenging both in healthcare facilities and at home. Bed sensors only provide data during occupancy, and don't provide fall detection or biometrics. Wearables need to be charged and can be easily misplaced or discarded by dementia patients. Camera-based vision solutions, including infrared cameras, can run afoul of privacy compliance requirements.

Recent advancements in IoT technology from Tellus, a venture-backed ArubaEdge technology partner, provides passive monitoring without wearables or invasive cameras. Actionable health data like fall detection, in-bed hours, in-room hours, wake-up detection, heart and breathing monitoring, and visitor detection help improve patient care and staff efficiency. Tellus' solutions can be used in hospitals, long-term care facilities, and assisted living units.

The Tellus solution consists of a compact microwave-based sensing and communication device to analyze reflections and uniquely-identifiable signatures indicative of heart, chest, and body movements. Real-time alerts can be automatically pushed to resident's own mobile device, while data destined for Tellus' cloud monitoring platform, passes over Aruba Wi-Fi infrastructure. Automated messaging enables staff to monitor more patients, without violating their privacy, and allows patients to sleep restfully without being awakened during the night to check vital signs.

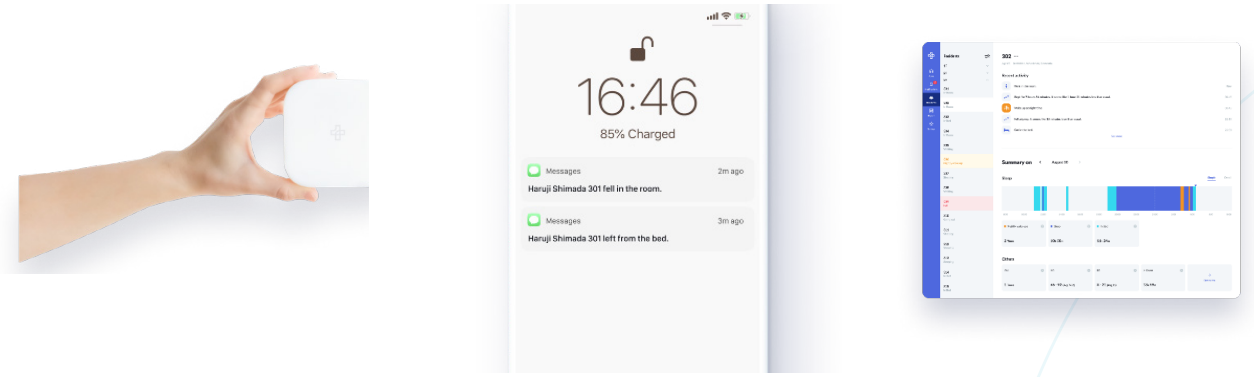


Figure 9: Tellus Non-Intrusive Vital Sign Monitoring Sensor, Mobile Application, And Web Portal

The Web monitoring application presents data to staff and physicians via a web portal. Cloud monitoring allows the system to scale massively while remaining cost-effective for local and remote telemetry applications. Reports show a 20% reduction in disease burden associated with using IoT for remote monitoring.

The Tellus solution is currently available in the Japanese market with world-wide availability in 2021.

HAND HYGIENE COMPLIANCE TO REDUCE THE SPREAD OF DISEASE

There is a direct correlation between hand hygiene and the spread of disease within a healthcare facility. On average, healthcare providers are only 50% compliant with hand wishing protocols. Healthcare organizations risk costly citations if audits or observations document improper hand hygiene. Accordingly, healthcare organizations are actively seeking technical means of enforcing compliance both to reduce the spread of disease and avoid citations.

Aruba has partnered with multiple hand hygiene solution vendors, all of which use transmitters in staff badges along with readers in hand washing stations. Their software platforms allow healthcare systems to determine baseline handwashing compliance and then drive staff to meet higher standards of care with the end result of reducing the spread of disease within their facility. Each of these solutions leverages the Aruba AP as an IoT platform to securely connect data generated at the point of care. AiRISTA Flow

AiRISTA FLOW

Unified Vision Solution (UVS) software with Hand Hygiene Compliance provides efficient compliance management of all caregivers within an organization. AiRISTA Flow B4n Personnel Tags and the BLE-based dispenser nodes, provide notification and recording of all gel and/or soap requirements for complete compliance. The Aruba APs receive hand washing data via Wi-Fi from the B4n personnel tags and securely transmit the data to the Unified Vision Solution.

CENTRAK®

CenTrak's electronic hand hygiene monitoring system captures 100% of hand hygiene events and is deployable as part of CenTrak's Enterprise Location Services™ platform in which data can be viewed at the hospital-, department-, or individual-level. Using 900 MHz, CenTrak staff badges communicate with dispensers to automatically collect hand washing compliance data. Then those data are securely sent via Wi-Fi over the Aruba infrastructure.

Sonitor's SenseCleanTM Hand Hygiene Modules containing low radio frequency (LF) transmitters that are seamlessly installed in GOJO® SMARTLINK™ dispensers. They capture 100% of hand hygiene events of staff wearing Sonitor badges as well as accurately track the number of dispenses from each device so that you know compliance activity in real-time. The data from the Sonitor badges are securely transmitted via Wi-Fi over the Aruba infrastructure.

Stanley Healthcare's solution (formerly known as AeroScout) leverages Aruba access points to relay information to Stanley's MobileView platform. MobileView is a comprehensive platform that allows healthcare organizations to track, manage, alert, and integrate with their clinical flows to improve care and increase efficiency. The hand hygiene dispenser incorporates an AeroScout LF exciter (EX3300 series) that is automatically activated when the caregivers uses the dispenser. This activates the caregiver's staff badge which securely sends the event to the MobileView software via the Aruba infrastructure.

LOCATION-AWARE PATIENT ENGAGEMENT, COMPLIANCE, AND TELEMEDICINE

For decades, medical records were stored as paper charts that needed to be retrieved on demand. Electronic Health Records (EHR) replaced paper charts with electronically stored records that could be retrieved by authorized personnel from any connected clinic within that healthcare system. The rise of mobile devices has prompted patients themselves to seek direct, self-service access to their own medical records via personally owned mobile devices and a healthcare provided-supplied app.

Healthcare systems are always on the lookout for ways to improve patient satisfaction scores (such as HCAHPS) because it drives a larger portion of variable payouts. Coupled with healthcare providers' desire to improve patient satisfaction using telemedicine, say for non-critical ailments when emergency room wait times are long, pressure has been growing to provide more experiences via mobile. However, app fatigue is a common complaint today because we are bombarded with requests to download separate apps for telemedicine, check test results, pay bills, and mobile check-in. From the patient's point of view, everything feels disconnected. One way to address this issue is by using a single app that serves as a "digital front door" to a healthcare system. Digital front door apps are high on the list of CIO/CTO's digital transformation plans, plus they provide an opportunity to build a branded, loyalty-driving relationship with patients.

Emerge Interactive is a digital product consulting firm dedicated to harnessing digital product transformation to improve their operations and customer experience. Aruba and Emerge Interactive have together enables a "couch-to-care" flow using a single mobile application branded for the healthcare provider. Aruba wireless infrastructure, APIs, and Meridian location services are key components in delivering the most relevant experiences via Emerge Interactive's mobile app.

Patient facing mobile OS and Android apps use the Bluetooth radios in Aruba access points to deliver wayfinding and location-based mobile check-in experiences. Allowing patients to navigate and check in with personally-owned own mobile devices reduces the risk of infection compared with public kiosks and interactions with hospital volunteers. It also improves on-time arrival rates, speeding workflows and maximizing total billable hours.

Experiences available with Emerge Interactive's couch-to-care flow include:

- Find a doctor and book an appointment from home, freeing staff from managing appointments ;
- Receive turn-by-turn directions to the optimal parking garage based on a patient's appointment time, saving time and lowering stress while improving on-time arrivals;
- Locating where a patient's car is parked and providing turn-by-turn walking directions through the healthcare facility;

- Mobile check-in upon arrival at the healthcare facility, saving staff from managing check-ins;
- Turn-by-turn navigation to an appointment , again, saving time and lowering stress while improving on-time arrivals;

Additional functions include bill paying, checking medical results via EHR integration, telemedicine from home or work, and chat bot engagement.

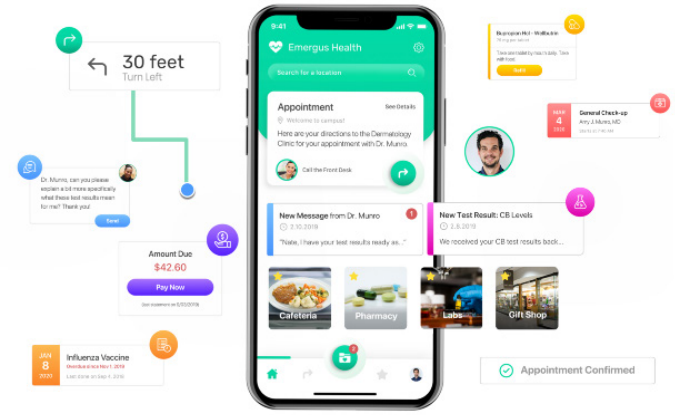


Figure 10: Engage Interactive Mobile App Integrated With Aruba Meridian Location Services

Aruba and Engage Interactive transform a patient's interaction with their healthcare provider, enabled a personally-owned device to deliver a more personalized, engaging experience will driving efficiencies, revenue, and higher customer satisfaction scores for the provider.

MEASURING AND IMPROVING PATIENT FLOW TO REDUCE WAIT TIMES AND INCREASE REVENUE

Before a provider can tackle workflow improvements that increase revenue via higher throughput, they first need to baseline patient flow. A challenge faced by virtually every provider today, measuring patient flow typically involves paper records and a clipboard, which is neither automated nor scalable. Instead, providers need to leverage automation to better find, understand, and remediate operational bottlenecks. Improved patient flow will increase revenue and patient throughput, while also reducing wait time and improving patient satisfaction.

Aruba has partnered with two companies – Hypros and MySphera – that use Aruba infrastructure as an IoT platform to monitor and report patient location.

HYPROS
INNOVATION IN TRACKING

Optimizing clinical workflows is essential to the timely delivery of care, best utilization of clinicians and capital equipment, and maximization of billable hours. Creating a contextually adaptive "connected clinic" that balances throughput speed with the availability of clinicians and diagnostics machines requires accurate location information on position, dwell time, and travel path.

Location data can be obtained by monitoring the movement of smart phones or other Wi-Fi or Bluetooth 5 enabled devices. Similarly, electronic tags affixed to assets or worn by people can also be readily located.

The challenge in clinical settings is that patients wouldn't typically download a locationing application, nor do they want their personal mobile phones to be monitored during visits. Clinicians, too, don't want their personal devices monitored, and work rules in many countries prohibit the observation of personnel on breaks or while undertaking personal matters.

Electronic tags could address the issue. Worn by patients and clinicians, tags wirelessly broadcast an ID number that identifies the person. RF tag monitoring infrastructure picks up the ID number and relays it to the workflow management system.

The issues with tags are that they typically require dedicated tag RF infrastructure, which is expensive to deploy and adds a new failure domain. Additionally, patients could inadvertently walk away with the tags, impacting workflow management and life cycle costs. Accordingly, operations teams typically prefer location data to be collected and managed thru a clinic's existing wireless infrastructure, using location devices (such as clipboards and tags affixed to wheelchairs) that will not leave the site.

HYPROS is a German, venture-backed technology company that produces clinical workflow management systems. The HYPROS location application works with BLE-based, location-enabled tags and clipboards, among others, to monitor the movement of patients and clinicians throughout the day. The system can identify bottlenecks, misalignments between actual and needed staffing, time and motion improvements, and patient and equipment scheduling improvements.

The HYPROS system includes three elements:

- HYPROS on-premises and cloud-based Tracking Tracing Infrastructure (HYPROS TTI) database that collects, stores, and processes location data;
- BLE Beacons, available in many form factors, that can be worn as tags, affixed to beds, or attached to clipboards and equipment;
- BLE data collection devices that track the movement of Beacons.

HYPROS and Aruba have partnered to provide location services that can be economically, reliably, and securely deployed over a hospital or clinic's existing Aruba mobility infrastructure. This is achieved by using the Aruba access points' internal BLE radios to collect BLE Beacon data and forward them to HYPROS TTI software for processing.

Aruba access points serve as secure communication platforms between the Beacons and TTI. Dynamic segmentation is maintained through the Aruba switch fabric, helping to protect the location system against attack, and the network against infected devices.

Aruba's 'colorless switch port" concept automatically establishes the correct secure connections with access points regardless of the switch port into which they're connected. This feature greatly simplifies system deployment, and reduces the chances of miswiring during network updates.

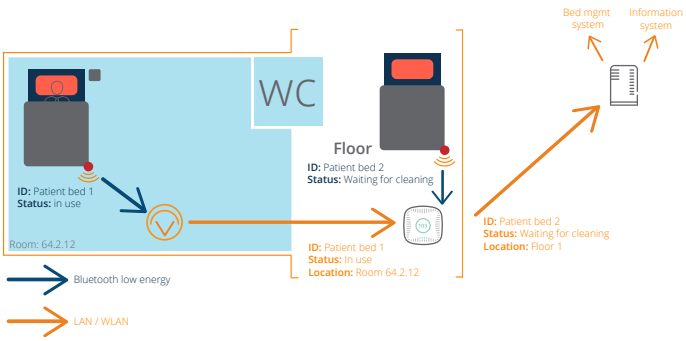


Figure 11: Aruba And Hypros Bed Workflow Management

Once deployed, the system updates TTI in real-time. Location data are both processed by HYPROS and can be shared with other clinical, operations, and finance applications using open APIs to further automate workflow management. Key benefits include: real-time location monitoring without significant investments in new infrastructure; shared location data and asset status via open APIs to optimize time-and-motion, maintenance, and asset storage processes; and data and workflow privacy thru end-to-end security.

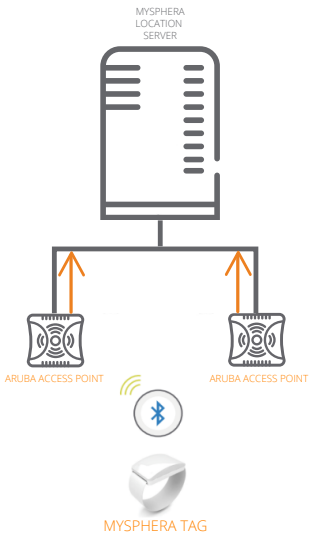
MySphera is a Spanish-based, healthcare IoT company focused on transforming healthcare systems though location and process visibility. They help optimize efficiencies, lower operating costs, increase reliability and safety, and improve patient outcomes.

Aruba and MySphera have partnered to tackle the challenge of clinical workflow optimization in hospitals, assisted living, and memory care units. The joint solution collects real-time location data from MySphera's wearable Bluetooth tags via 802.11ac (Wi-Fi 5) and Aruba 802.11ax (Wi-Fi 6) access points, and forward those data to MySphera workflow optimization software using secure tunnels and dynamic segmentation.

Aruba access points are ideally situated to collect real-time location data, with line-of-sight to MySphera wearable tags. The tags are alerted by proximity to staff smartphones and tablets, and trigger requests for patient-related tasks and workflows. Once entered, the information is viewable on MySphera's real-time dashboards and include:

- Occupation metrics
- Bed management and utilization rates
- Patient status
- Wait times

Staff are notified of the closest patient and next procedural step, and in turn can log when the patient has moved to the next clinical phase of care. Out-of-order or incorrect steps prompt automated alerts. Staff can enter updates in real-time, such as "in recovery," "in preparation," "equipment in use," and "equipment needs maintenance." This creates a fluid, orchestrated process to deliver and track care, enhancing efficiency and reducing the chances of errors.



Leveraging Aruba wireless infrastructure as an IoT platform to collect MySphera tag data lowers deployment costs, improves the utilization of staff and equipment, and enhances patient outcomes. Together, Aruba and MySphera enable healthcare organizations of any size optimize clinical workflows, improve surgical outcomes, boost equipment and room utilization rates, make faster fact-based decision-making, improve patient safety, and better manage staff and physician time.

IMPROVING PATIENT FACING STAFF EFFICIENCY WHEN FINDING BIOMEDICAL DEVICES

It is common for clinical staff to object that biomedical devices are in short supply when in fact they're readily available but have been sequestered in closets and cabinets. Studies show that nurses waste roughly one hour per shift trying to locate biomedical equipment, precious time that could otherwise be dedicated to essential services. Sequestering equipment creates false scarcity, yet is commonplace for many reasons: preference for a specific model or brand; a unit is known good or recently calibrated and therefore more reliable; and concern that if not sequestered a device may be unavailable when needed. Regardless of the reason, the consequence is the same: the cycle of scarcity forces healthcare providers to buy/rent more biomedical devices than is needed.

With an Aruba infrastructure-based asset tracking solution, devices can be located faster and more reliably. By reassuring staff that medical devices can be located when needed, sequestering behavior will change. Furthermore, fewer devices will be needed, and those that are purchases will be better utilized, lowering capital expenditures and life-cycle costs.

Aruba infrastructure supports a wide suite of IoT location-based services to help navigate sites (Where am I?), find staff and patients (Where are they?), and locate biomedical and other assets (Where is it?). Some of the services are based on Aruba applications, such as the Meridian location and asset tracking suite, while others leverage technology partner applications.

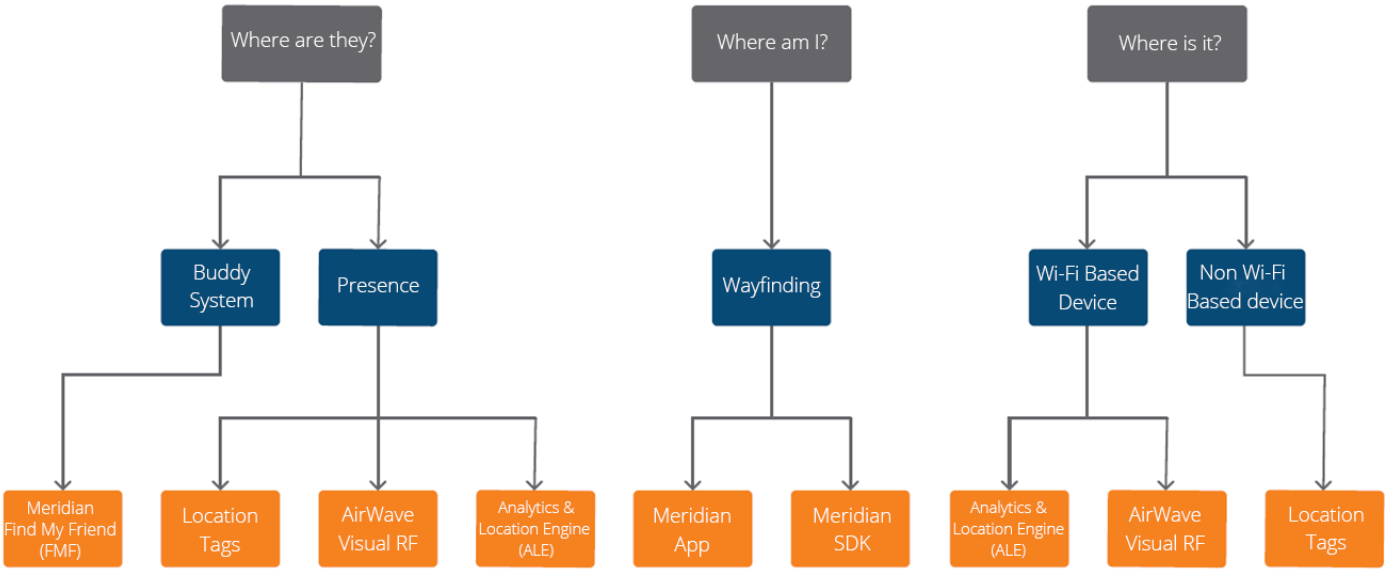


Figure 12: Aruba Location-Based Service Options

Aruba has partnered with leading healthcare asset tracking solution vendors that leverage Wi-Fi, Bluetooth, RF, infrared, and ultrasound for locationing depending on the clinical requirements. In every case the technology partner leverages existing Aruba infrastructure as an IoT platform to gather and/or transport location data.

AiRISTA Flow provides a variety of battery powered Wi-Fi asset tags that can leverage Aruba APs to transmit location data to their Unified Vision Solution (UVS) software. In addition to options for RF fingerprinting, the overall solution can leverage Aruba ALE (Analytics and Location Engine) to provide additional location data to UVS.

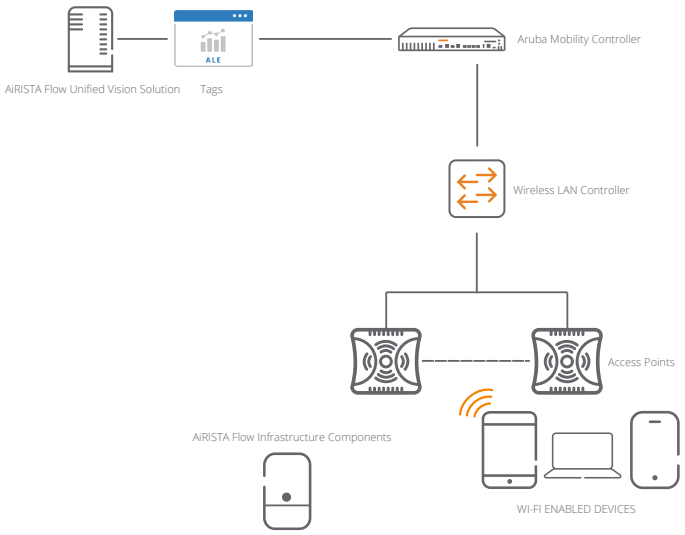


Figure 13: AiRISTA Flow and Aruba Wi-Fi system overview

CenTrak's solution uses a combination of Wi-Fi and infrared to provide solutions for various use case. When room level accuracy and certainty is required to make clinical decision, infrared is a preferred technology since it cannot penetrate walls like other RF signals can. The battery-operated infrastructure components (such as monitors or Virtual Walls™) are able to provide a unique location number and pinpoint any tagged assets in the room or zone that the healthcare facility has defined. They can be placed anywhere they are needed, including rooms, bays, nursing stations, hallway segments and other relevant workflow areas without the need for costly hardwiring. The solution also has the ability to leverage your Aruba Wi-Fi network to communicate location and condition information to authorized hospital personnel. For areas in the facility or use cases that don't require clinical grade location, Aruba ALE (Analytics and Location Engine) can be used to provide Wi-Fi-based location to the Centrak platform. This approach can help reduce the total cost of the entire solution by only focusing the clinical grade location solution where it is needed.

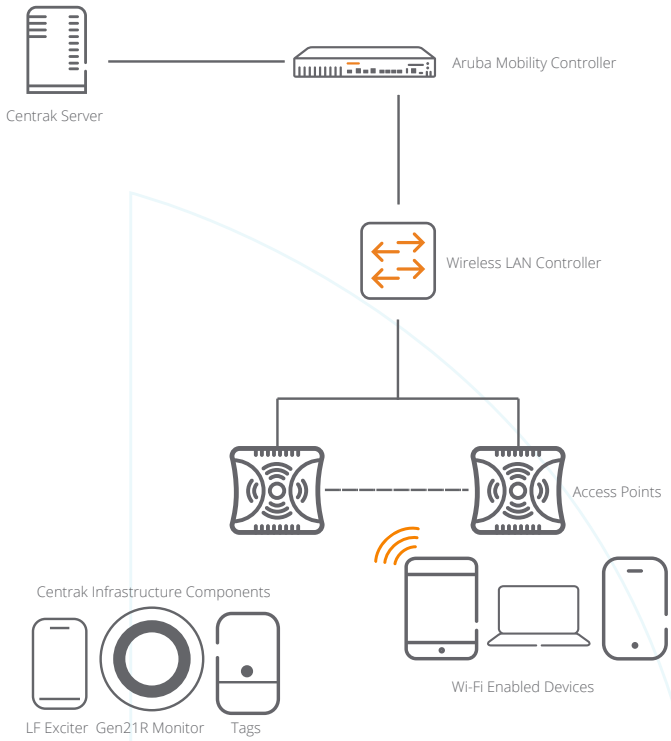


Figure 14: Centrak and Aruba Wi-Fi system overview

The Sonitor solution uses a combination of Wi-Fi and ultrasound to provide room level and even sub-room level accuracy for use cases that demand that level of accuracy. Quad-LTs (location transmitters) are wireless (PoE optional), multi-function, battery-operated devices that are mounted on ceilings or walls and are assigned unique identifications. These LTs transmit ultrasound signals that are synchronized by Sonitor gateways and are then picked up by tags/badges that also have a unique ID. When the tags/badges receive the location information from the LTs, they communicate that location via Aruba Wi-Fi to a server, providing the exact location of that tag at the exact moment the signal is received. Ultrasound LTs can combine both ultrasound and low frequency transmitters in a single unit and enhance positioning accuracy.

SenseVIEW is the Sonitor software program that provides customers with immediate, visual confirmation that their system is working optimally, and through unique mapping capabilities, pinpoints the exact location when a device is not performing. In addition, SenseVIEW displays tag and infrastructure signal strength and battery status information.

For areas in the facility or use cases that don't require room or sub-room level accuracy, Aruba ALE (Analytics and Location Engine) can be used to provide Wi-Fi-based location to the SenseVIEW platform. This approach can help reduce the total cost of the entire solution by only focusing the ultrasound solution where it is needed most.

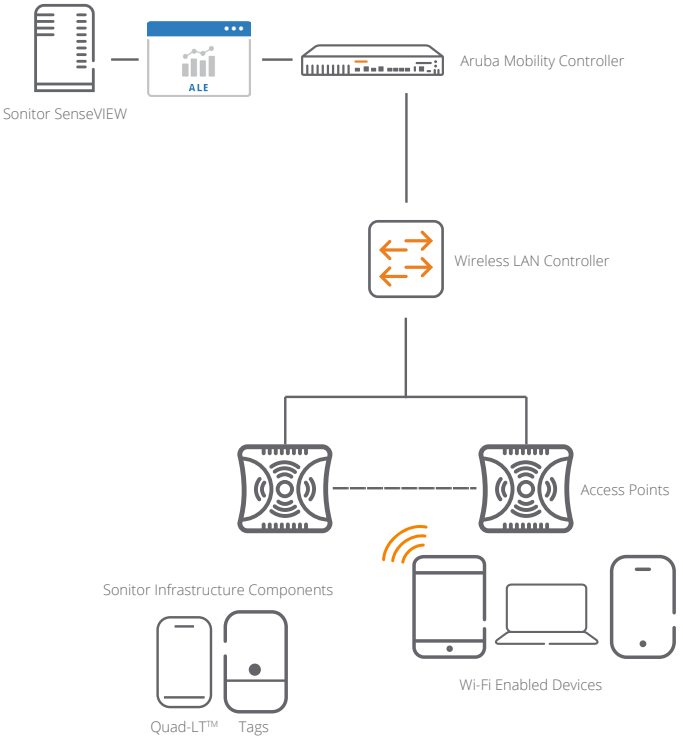


Figure 15: Sonitor and Aruba Wi-Fi system overview

Stanley Healthcare's solution (formerly known as AeroScout) leverages Aruba AP to relay information to their MobileView platform. MobileView is a comprehensive platform that allows healthcare organizations to track, manage, alert, and integrate with their clinical flows to improve care and increase efficiency. With a wide array of sensors and tags, the platform supports protecting infants, locating equipment and monitoring temperature conditions. Stanley RTLS tags transmit Wi-Fi packets that are recognized by Aruba APs and forwarded to MobileView. In addition, MobileView is integrated into Aruba AirWave to streamline the process of AP adds, moves, and changes.

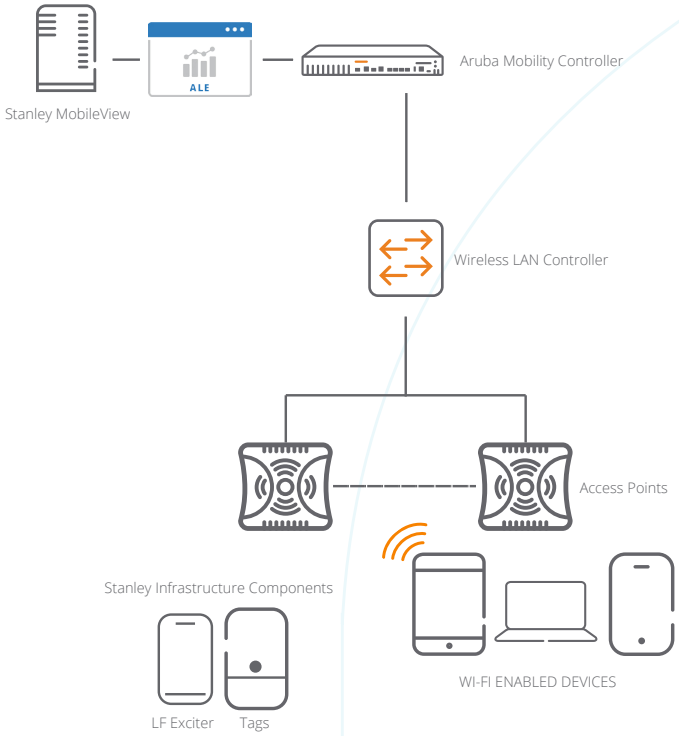


Figure 16: Stanley MobileView and Aruba Wi-Fi system overview

ENHANCING THE RELIABILITY AND QUALITY OF MOBILE STAFF COMMUNICATIONS

As organizations have migrated to mobile devices, network utilization has shifted away from wired Ethernet for edge access in favor of 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 physicians and 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 physicians and staff securely communicate. Secure texts can be sent mobile within the facility without the HIPAA compliance 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 Operational Technology (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, Quality of Service, 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.

Quality of Service (QoS)

Healthcare 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
- Client sessions active at the time of the call

This method allows Aruba's Central and AirWave 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. This results in a significantly improved user experience involving multimedia and latency-sensitive calls.

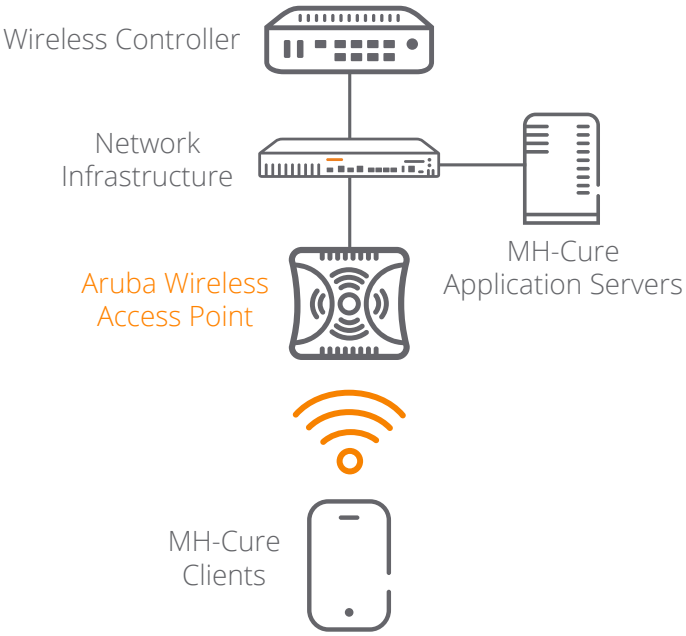
ascom

Aruba has partnered with Ascom to support their purpose-built mobile devices for clinical healthcare communications in hospitals and long-term care facilities. Ascom products such as the i62 handset are integrated with Aruba APs and Mobility controllers to ensure association, authentication, and roaming functionality are robust for healthcare environments.

Mobile Heartbeat®
UNIFIED CLINICAL COMMUNICATIONS

Aruba and Mobile Heartbeat have partnered to integrate Aruba secure wireless with MH-CURE. The result is a reliable clinical communications system that can operate in challenging environments in which cellular connectivity is not assured.

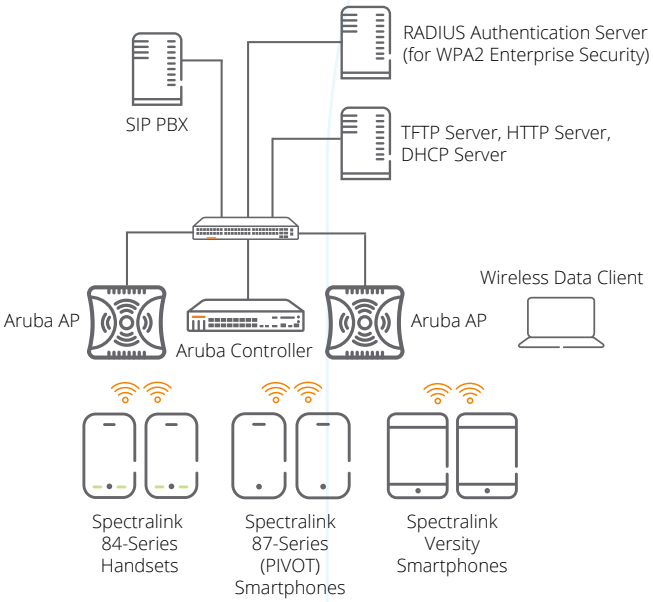
Ceiling mounted Aruba Wi-Fi access points are uniquely positioned to receive mobile device data from MH-CURE enabled mobile devices. As staff members move around the facility, they're automatically matched with the optimal access point to ensure a reliable application experience. Aruba's ClientMatch and patented RF optimization technology enhance the mobile roaming experience. ClientMatch continuously monitors the status of all clients connected to each access point, passing them to other access points, as needed, to optimize performance. Matching mobile clients to the optimal access point resolves roaming issues and improves the overall user experience.



spectralink

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.

The integration allows Spectralink devices to take advantage of Aruba's Adaptive Radio Management (ARM) and user profile functionality to ensure staff have the right access at the right time.



vocera

Aruba has partnered with Vocera to ensure their badge and smartbadge solutions perform optimally on Aruba infrastructure. Vocera software solutions also run on Spectralink and Zebra handheld smart devices.

The Vocera solution consists of wearable Vocera Communications Badges with integrated Wi-Fi radios and the Vocera Communications software server. VoIP call management and speech recognition engine functionality are incorporated in the Vocera Communications server software which runs on standard Windows servers. Through the use of optional modules, Vocera can interface with circuit PBX, alarm/alert, and nurse call systems. Medical staff can log into the system using voice commands and can call colleagues by

name or role (e.g. radiologists or charge nurses) by speaking into the badge. Vocera and Aruba support secure voice communication.

The solution supports fast roaming of Vocera badges which significantly improves call quality and reduces the occurrence of "dropped calls" due to latency. The Aruba network, with its unique awareness of the application layer, is able to recognize badges from their use of the Vocera VoIP protocol. This capability allows Aruba to ensure optimal load through call admission control of the voice badges.

Figure 17: Vocera device

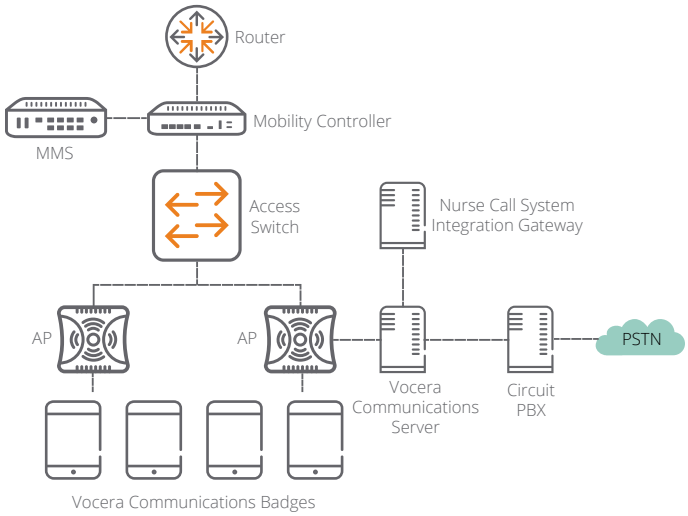


Figure 18: Aruba and Vocera Communications joint solution

ZEBRA

IoT is the digital raceway that transports data and context to mining engines, which alchemize them into insights to optimize operations, manage inventory, and improve user experiences. Information sources vary by industry but may include processes, systems, products, patients, customers, applications, and their environments. The veracity of these sources impacts the value of the insights, so validating the quality and provenance of information fed into the engines is paramount.

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 enforces from source to C-Suite, from I/O to CMO.

It is on these last points that fractures typically appear for healthcare institutions. Data input is often hit or miss. Voice communications with staff are unreliable, especially when roaming. Locating inventory, lab test results, biomedical devices, and wheelchairs is challenging. And end-to-end security is aspirational but rarely achieved, especially with IoT devices and systems.

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), point-of-sale (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 voice and video over Aruba Wi-Fi to roaming staff and physicians.

Aruba's deep packet inspection engine, supported by voice heuristics and intelligent Quality of Service tagging, bring toll quality audio to voice-enabled Zebra healthcare devices. Combined with Aruba's best-in-class Wi-Fi performance that means higher legibility, fewer drop-offs, and higher-speed coverage over large areas in a healthcare setting.

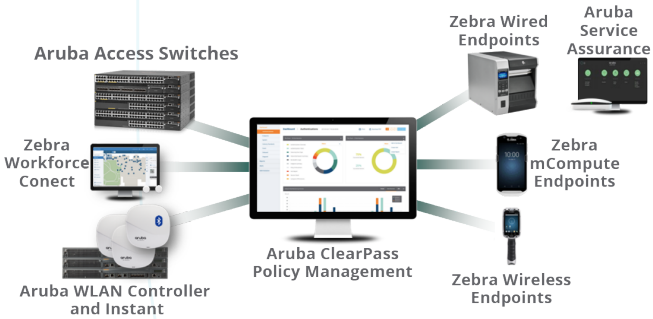


Figure 19: Aruba-Zebra Integrated Voice and Data Capture

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 healthcare applications. Joint systems go in faster and more reliably.

AUTOMATING GUEST ACCESS TO ENHANCE STAFF EFFICIENCY

Enhancing human productivity necessitates making devices and the environments in which they work more cognizant of, and automatically adaptive to, the needs of employees, guests, service personnel, and contractors. On-boarding guests on to healthcare networks has historically been challenging because of network security concerns. In some cases, access is simply refused, forcing visitors to use cellular networks that by-pass plant IT security and can't take advantage of on-site applications and servers. The trick is to both simplify guest access so it doesn't create an administrative burden, and implement security policies that tightly control what guests can do and access while on the network.

Aruba and its technology partners have a proven solution by which visitors can be automatically badged and enrolled on the building Wi-Fi network, guided to their hoteling space or destination using wayfinding, and enable personally-owned devices to securely connect to projection screens and other network resources in designated areas.

Key components include Aruba Wi-Fi 6 Access Points, ClearPass Guest Access, ClearPass Policy Manager, Envoy's visitor management solution, WPA3 Enhanced Open, and an Access Code captive portal. Performance of the offered services are monitored using the Aruba User Experience Insight (UXI) solution to ensure that service level agreements are satisfied, and application performance meets guidelines. A comprehensive validate reference design guide for guest access is available on request.

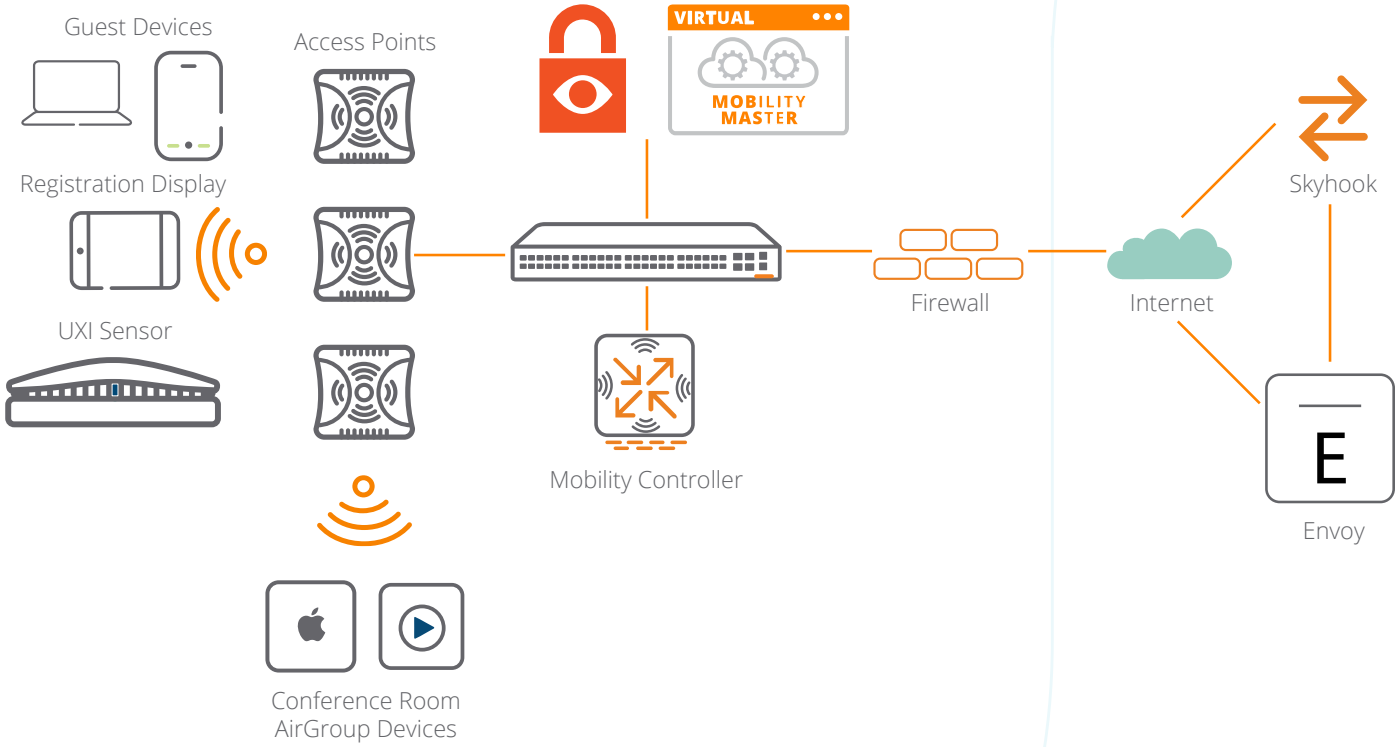


Figure 20: Automated Guest Access Solution To Enhance Staff Efficiency

Aruba 500 Series Wi-Fi 6 Access Points are recommended because of their Wi-Fi performance and integrated IoT radios for smart building sensing and control. ArubaOS 8.4 or newer code running on a Mobility Master/Mobility Controller, Aruba Instant, and/or Central are supported. A comprehensive validated reference design is available for controller-based deployments.

ClearPass 6.7.2 or newer is required. ClearPass runs on hardware appliances with pre-installed software or as a Virtual Machine under VMware (ESXi 5.5, 6.0, 6.5 or higher), Microsoft Hyper-V Server (2012 R2 or 2016 R2), Hyper-V on Microsoft Windows Server (2012 R2 or 2016 R2), and KVM (CentOS 7.5).

Envoy

Envoy Visitors is a guest management platform for a modern front desk that helps streamline guest sign-in. When guests arrive, Envoy makes it easy for them to register, presents relevant non-disclosure and health/safety forms for completion, and notifies hosts of the guest's arrival via e-mail or SMS. Simultaneously, ClearPass dynamically provisions temporary Wi-Fi access credentials for their devices sends an individualized security code for Wi-Fi access via e-mail or SMS.

Envoy leverages ClearPass' microservice extensions running in a container independent of the ClearPass operating system. ClearPass extensions are used to interact with external systems, including advanced two-factor authentication services and IIoT firewalls.

The joint Aruba/Envoy solution automates the entire onboarding process, minimizing the need for manual assistance, and ensuring that security standards are enforced throughout the visit. Never again will guests, service personnel, and contractors need to circumvent IT security just to obtain reliable connectivity.

MIGRATING FROM BREAK-FIX TO PROACTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep 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%.

Predictive 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.

Spending on predictive maintenance is expected to hit $12.9 billion in the next two years. Juggling the high cost asset performance management solutions, and its security risks, 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 in a plant to capture machine status from IIoT sensors. A dual-use IT/IIoT 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 predictive maintenance, a digital transformation that reduces downtime, enhances asset utilization, and optimizes scheduling of field 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 AbilityTM Condition Monitoring application. Using Aruba zero trust infrastructure as a data collection platform provides uniform security and visibility across both IT and IIoT 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 802.11ac and 802.11ax access points equipped with a BLE radio and AOS 8.6 or later. This means that predictive 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 life cycle of a plants since adds, moves, and changes are easy and inexpensive.

The intersection between OT and IT has historically been a point of friction, but not so with the ABB-Aruba joint solution. Both companies are respected leaders in IIoT 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.

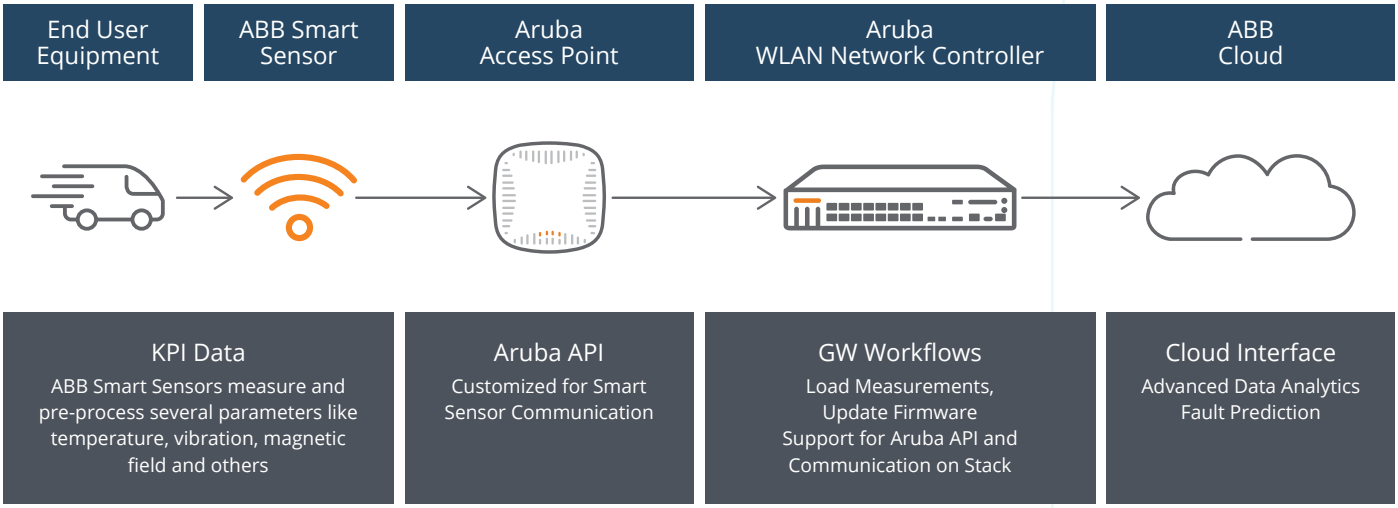


Figure 21: Aruba and ABB Integration Overview

MOBILE DURESS ALARMS FOR ENHANCED STAFF AND PHYSICIAN SAFETY

Violence toward healthcare professionals is a hidden problem. According to the World Health Organization (WHO), health workers are at high risk of violence all over the world. Between 8% and 38% of health workers suffer physical violence at some point in their careers.8

Providers are looking for ways to help protect their staff members. Enabling staff to call for help when they are uncomfortable or in a compromised situation is top of mind at many healthcare facilities. Leveraging the secure network infrastructure is one way to empower staff to easily call for help.

Aruba has partnered with three companies that provide healthcare solutions to provide staff safety. The solutions offer a staff duress system that allows staff members to request help by pressing a button on their badge. These solutions use a combination of Wi-Fi, Bluetooth, infrared, and ultrasound technology to provide accuracy to meet specific demands. Technologies like infrared and ultrasound can guarantee room level accuracy when required because those technologies do not penetrate walls like Wi-Fi and Bluetooth do.

Sometimes room level accuracy is not required and other technologies can provide a more cost-effective answer for this use case. Each of these solutions uses the Aruba infrastructure as an IoT platform to transport the IoT data.

AiRISTA Flow provides a variety of battery powered Wi-Fi personnel tags that can leverage Aruba APs to transmit location data to their Unified Vision Solution (UVS) software when a staff member presses a physical button on the badge. In addition to options for RF fingerprinting, the overall solution can leverage Aruba ALE (Analytics and Location Engine) to provide additional location data to UVS.

The AiRISTA Flow B4 badge shown below is unique in having a text display that can provide confirmation to the staff member that help is on the way.

Figure 22: AiRISTA Flow B4 Badge

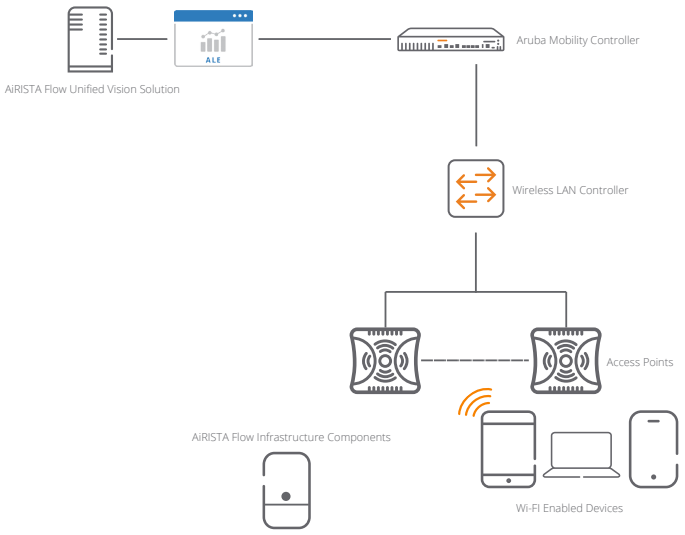


Figure 23: AiRISTA and Aruba Wi-Fi System Overview

CenTrak's solution uses a combination of Wi-Fi and infrared to provide solutions for staff duress. When room level accuracy and certainty is required, infrared is a preferred technology since it cannot penetrate walls like other RF signals can. The battery-operated infrastructure components (such as monitors or Virtual Walls™) are able to provide a unique location number and pinpoint any staff member requesting help. The solution leverages the Aruba Wi-Fi network to communicate location information to CenTrak's Security Services platform to alert authorized hospital personnel.

Figure 24: CenTrak Staff Badge

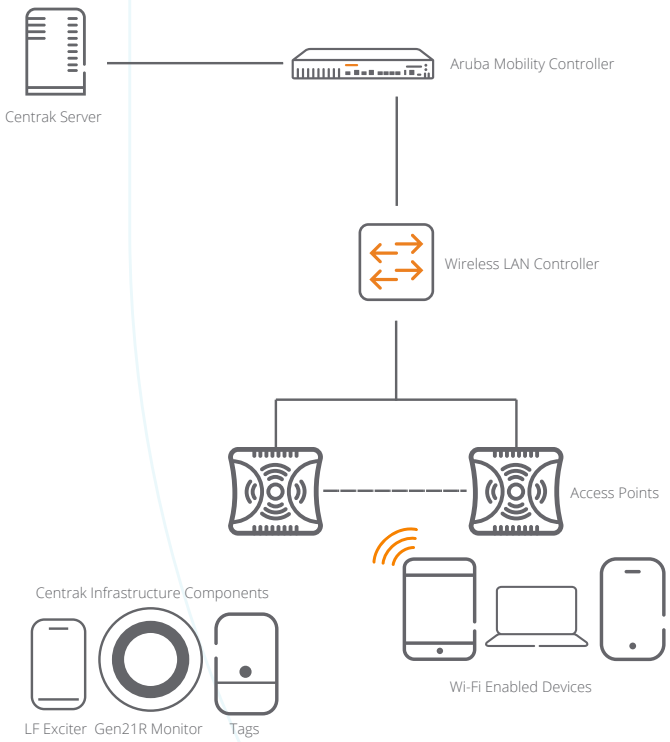


Figure 25: CenTrak and Aruba Wi-Fi System Overview

The Sonitor solution uses a combination of Wi-Fi and ultrasound to provide room level and even sub-room level accuracy for duress use cases that demand room level accuracy. Quad-LTs (location transmitters) are wireless (PoE optional), multi-function, battery-operated devices that are mounted on ceilings or walls and are assigned unique identifications. These LTs transmit ultrasound signals that are synchronized by Sonitor gateways and are then picked up by staff badges that also have a unique ID. When the staff badges receive the location information from the LTs, they communicate that location via Aruba Wi-Fi to a server, providing the exact location of that person at the exact moment the signal is received. Ultrasound LTs can combine both ultrasound and low frequency transmitters in a single unit and enhance positioning accuracy.

SenseVIEW is the Sonitor software program that provides customers with immediate, visual confirmation that their system is working optimally, and through unique mapping capabilities, pinpoints the exact location when a device is not performing. In addition, SenseVIEW displays tag and infrastructure signal strength and battery status information.

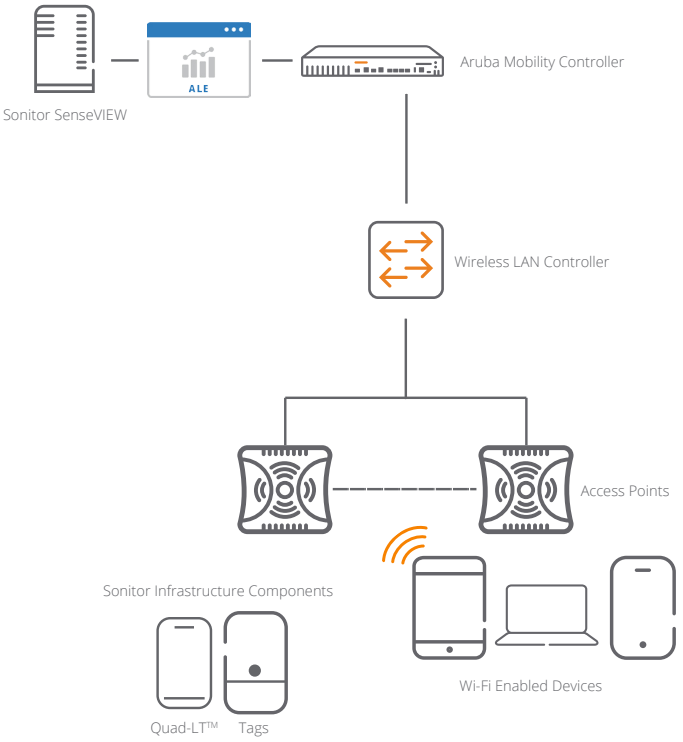


Figure 26: Sonitor and Aruba Wi-Fi System Overview

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 27: HALO Smart Sensor Powered By Aruba Switches And Pass-Thru 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 28: 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.

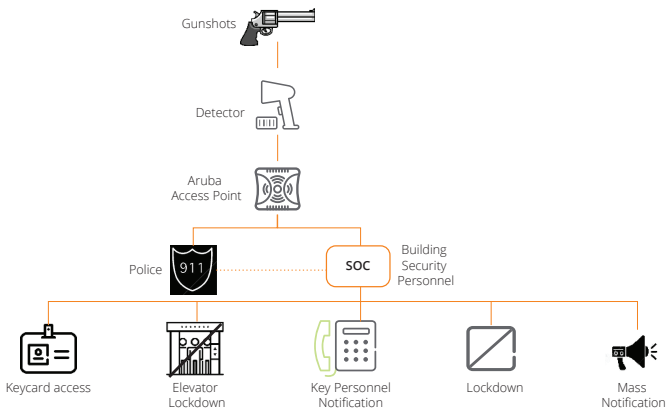


Figure 29: AmberBox Gunshot Detection And Notification System

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're 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 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.

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 30: 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 HEALTHCARE NETWORKS WITHOUT LOSING CONTROL

Healthcare wireless network access is typically tightly controlled out of concern that critical services and devices, such as staff Wi-Fi calling, or biomedical device data transfers could be negatively impacted by wireless users. However, 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. Both IT and facilities groups 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 manages. 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.

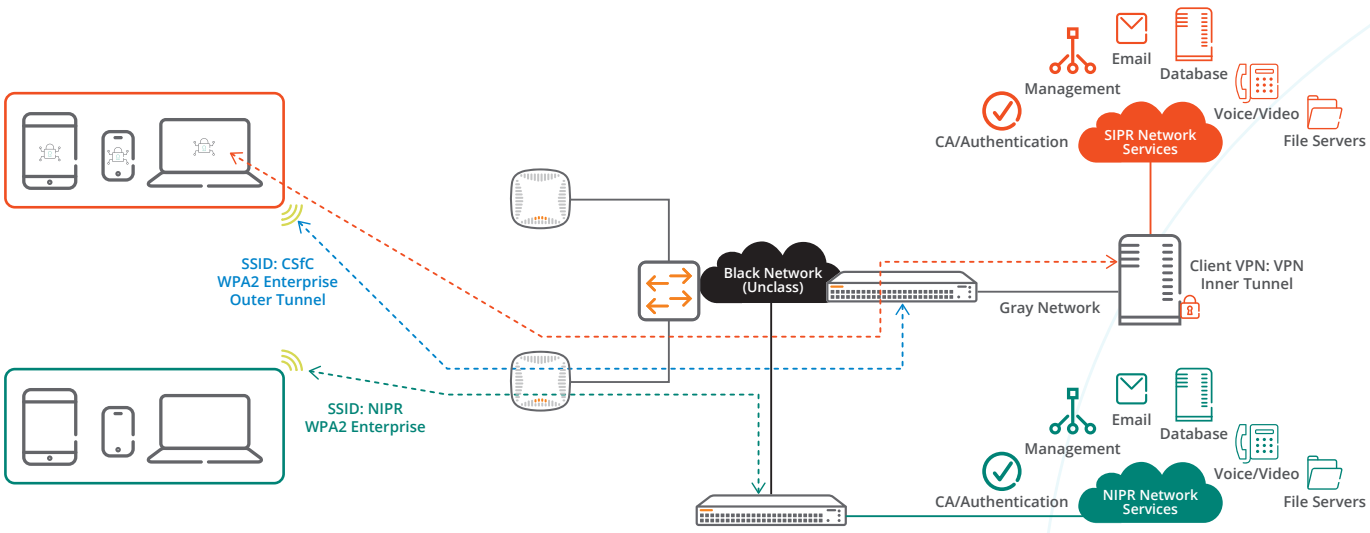


Figure 31: Aruba Multizone Solution

The multi-tenancy design of MultiZone is ideal for healthcare applications. Separate Data Zones can be allocated to the groups managing, say, building controls, biomedical devices, corporate services, contractors, and auditors. Each group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services. Defense-related healthcare can use MultiZone in conjunction Aruba's commercial solutions for classified applications, including elliptic curve encryption and other FIPS 140-2 and Common Criteria related 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 hospital or clinic, 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 buildings. 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.

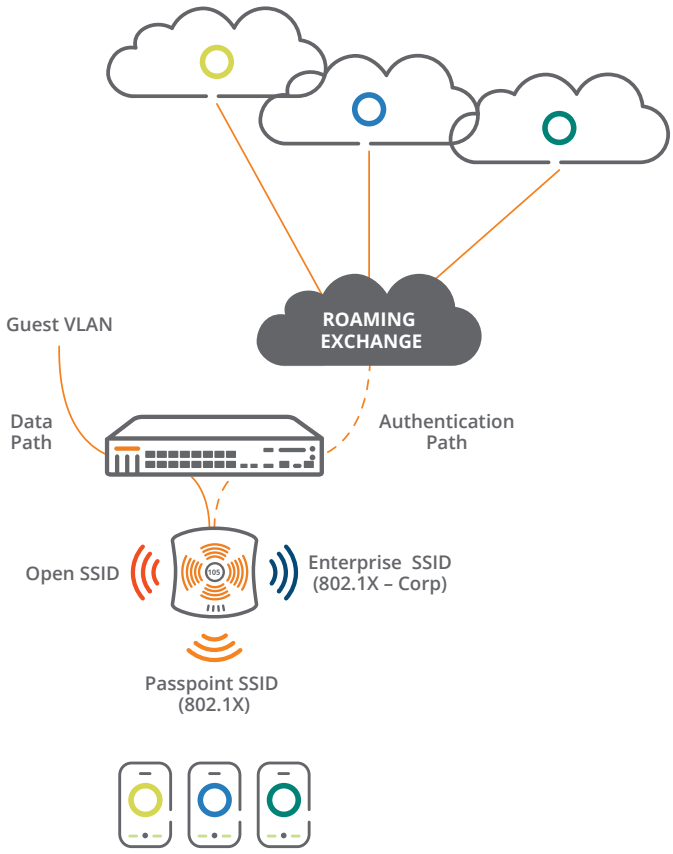


Figure 32: Aruba AirPass System Architecture

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, user names, 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.

Mobile users and IoT devices are increasingly accessing cloud services and other bandwidth-intensive applications like augmented and 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 CLINICS AND WORKERS

Industry analysts have long opined that the rise of smart machines, cognitive technologies, and algorithmic business models could render obsolete the competitive advantage of offshoring. Hyper-automation, it is argued, 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.

Labor arbitrage aside, there is no denying the central role of IoT on the journey to run businesses more efficiently, productively, and profitably. The underpinnings of IoT are the sensors, actuators, and related control systems that for decades have been running our buildings and campuses.

Large, geographically-distributed healthcare institutions typically have buildings and mobile clinics spread across a broad areas, and depending on the remote site it could be unattended for large parts of the day. 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.

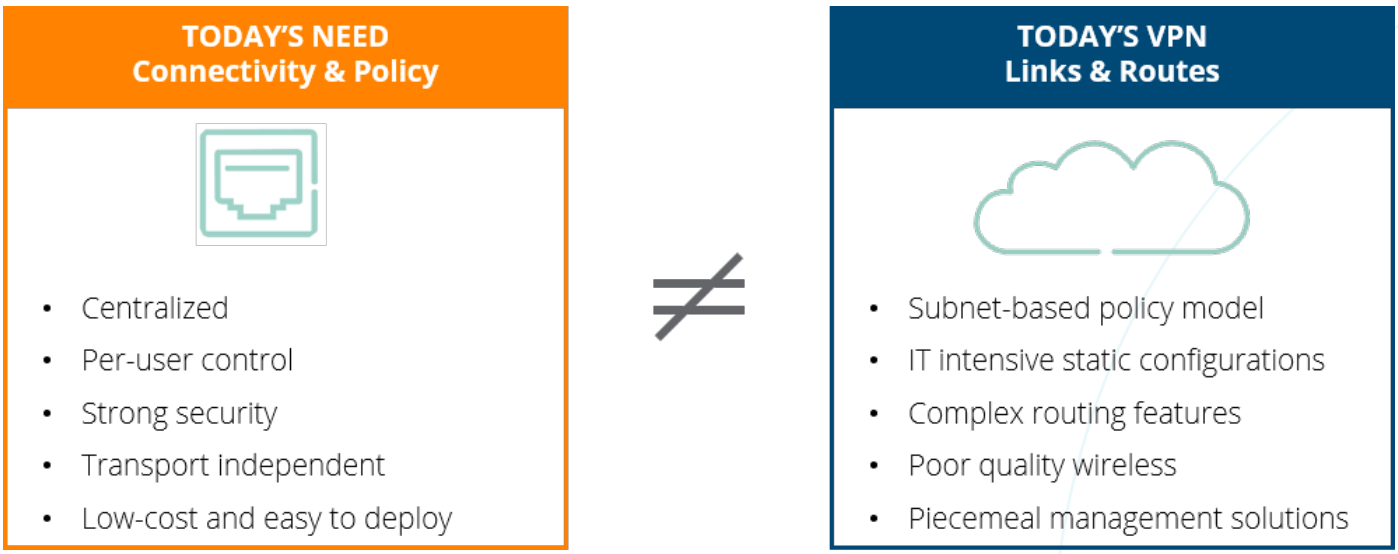


Figure 33: Limitations Of Traditional VPNs

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 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.

Government or defense-related healthcare facilities 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 main buildings or data center. The controller runs the Aruba Operating System (AOS) and terminates the VPN tunnels, manages identity assignment, centralizes encryption, and runs Aruba's unique role-based firewall. Every IoT device and field engineering 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.

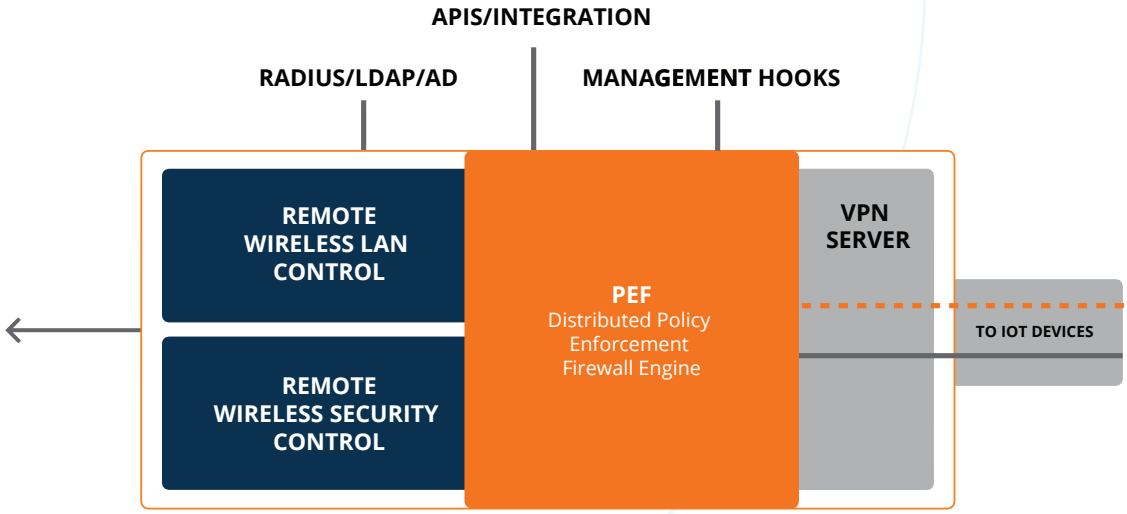


Figure 34: Aruba VPN Concentrator Controller

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 instance, 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 mechanisms to set up a secure, encrypted tunnel with an Aruba VPN concentrator controller at the plant or data center. Suite B support is available 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.

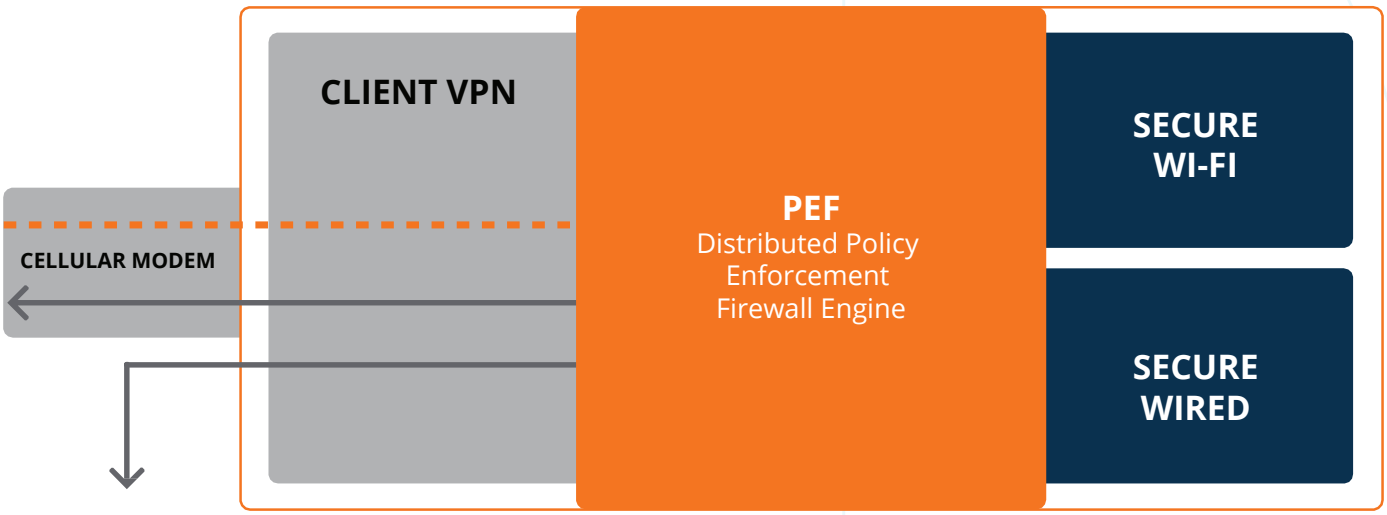


Figure 35: Aruba Remote Access Point

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 engineering 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 a 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 building or campus IoT application. RAP updates are pushed automatically from time to time, and no manual or local intervention

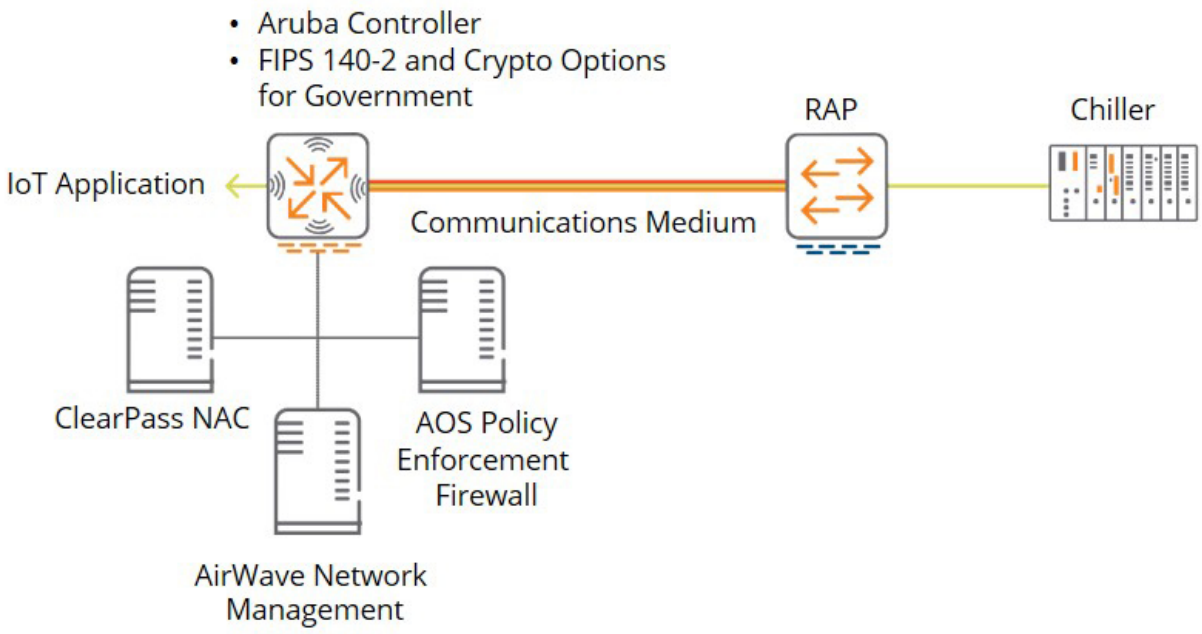


Figure 36: Remote Chiller Monitoring

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 engineering tools (like ruggedized laptops and tablets) as they move between buildings. 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 clinic or a large healthcare campus, Aruba has you covered.

SECURING HEALTHCARE NETWORKS THAT CAN'T PROTECT THEMSELVES

Healthcare is one of the most targeted vertical segments by hackers because of the value of medical records on the black market. When a credit card is stolen, the card can easily be cancelled and a replacement card issued. When medical records are used by criminals, it may take months or years to notice the fraud and you cannot simply replace your identity with a new one.

With the influx of IoT and BYOD devices, the strategy of a defensive perimeter simply doesn't scale to meeting today's healthcare security needs. As an infrastructure provider, Aruba is uniquely positioned to provide a closed-loop zero-trust network security solution with dynamic segmentation, policy management, and AI monitoring to catch attacks early and before they can cause damage.

On the black market, the going rate for your social security number is 10 cents. Your credit card number is worth 25 cents. But your electronic medical health record (EHR) could be worth hundreds or even thousands of dollars.[6]

Aruba has partnered with two leading healthcare IoT security vendors to identify healthcare devices on the network. With integration into ClearPass Policy Manager, it can provide a comprehensive solution to identify and secure devices on the healthcare network. Once devices on the network have been identiifed, proper policy can be applied as part of the zero trust framework.

CyberMDX, an Aruba 360 Security Exchange technology partner, provides medical cybersecurity software for healthcare organizations by adding layers of cyber protection and improving cyber insights. Aruba and CyberMDX have partnered to integrate Aruba ClearPass Policy Manager with the CyberMDX platform to enforce security policies across IT and IoMT networks. REST APIs provide ClearPass with the real-time status of medical devices on a network, which then assigns the appropriate level of network access.

At the time a device authenticates on the network, a risk analysis is conducted based on known vulnerabilities, detected threats, original research, and deviations observed from baseline performance measures collected by CyberMDX. CyberMDX automatically pushes these updates to ClearPass Policy Manager (CPPM) via device custom attributes for policy enforcement, VLAN assignment, and dACL policy management. These attributes are further used to define and enforce context and risk aware policies within CPPM, including VLAN assignment and downloadable ACLs, to reduce the attack surface. Together, the itemized inventory and individualized risk assessment provide comprehensive visibility into devices and their cybersecurity posture.

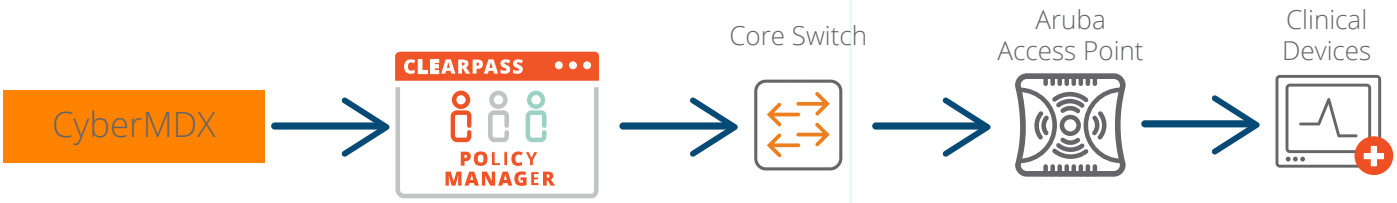


Figure 37: Aruba ClearPass Policy Manager and CyberMDX Joint Solution Diagram

The Medigate platform is focused on providing visibility into the Medical and Healthcare space, it discovers and precisely identifies every connected device on your clinical network. Utilizing industry-leading medical device signature database developed by Medigate Research Labs, they fingerprint each device with deep packet inspection (DPI) techniques, allowing dynamic inventory management and facilitating advanced detection and prevention capabilities.

This endpoint data is then shared directly with ClearPass via the ClearPass Security Exchange framework and the open API exposed under Policy Manager. Medigate will automatically update the ClearPass Policy Manager Endpoint Database with endpoint classification data and a number of custom security attributes, these attributes can then be used to drive role-mapping and or enforcement policies, a great source of context for segmentation policies.

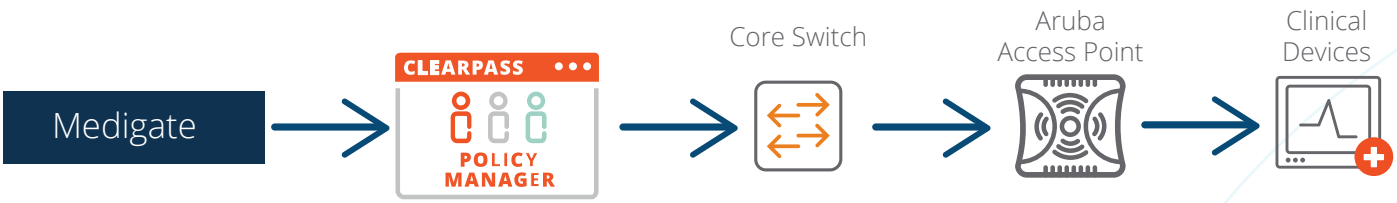


Figure 38: Aruba ClearPass Policy Manager and Medigate Joint Solution Diagram

SUMMARY

The availability of IoT data and relevant context enables healthcare institutions to adapt to the environment and occupants. The richer the set of available data and context, the more adaptive the healthcare provider can become.

Key technology partners - working in concert with Aruba's ESP-based unified infrastructure, zero-trust security, and AI powered solutions - enable healthcare to boost efficiency, productivity, reliability, safety, security, and profitability while at the same time improving patient care.

Please contact us for more information on how we can help your hospital, clinic, or institution 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

[5]https://www.nursingtimes.net/archive/nurses-waste-an-hour-a-shift-finding-equipment-10-02-2009/

[6]https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers

[7]https://www.cdc.gov/handhygiene/pdfs/provider-infographic-508.pdf

[8]https://www.who.int/violence_injury_prevention/violence/workplace/en/

WP_DesigningHyper-AwareHealthcareFacilities_RVK_100720 a00100715enw