WHITE PAPER

aruba
a Hewlett Packard Enterprise company

DESIGNING HYPER-AWARE CIVILIAN GOVERNMENT FACILITIES

SECURE INFRASTRUCTURE AND PARTNER SOLUTIONS FOR BUILDINGS, CAMPUSES, PHYSICAL PLANTS, AND CITIES

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 the physical phenomena acted upon by those machines (voltage, temperature, flow, speed), contextual data generated by networks connecting the machines (identity, location, applications in use), and applications that analyze, mine, share, and respond to those data. In civilian government applications, the machines and applications are tailored to optimizing human activity and productivity monitoring, organizational redesign, and health and safety.

By securely interfacing IoT devices, and generating contextual information, Aruba's networks enable facilities to become hyper-aware of their operating environments. Aruba's unified infrastructure, zero-trust security, and AI-powered software - used in conjunction with solutions from key technology partners – enables institutions to successfully and economically deploy and exploit IoT solutions. The richer the set of available data and context, the greater the opportunities to boost citizen enablement, efficiency, productivity, reliability, safety, and security.

Solutions from Aruba and its technology partners are applicable across a broad range of government environments spanning from government offices to multi-campus institutions, mobile service vehicles to municipalities. Use cases discussed in this white paper are shown below, and additional information on the specific technology partner solutions can be found at https://www.arubanetworks.com/partners/programs/:

- **Health**
  - Physical Distance Monitoring And Contact Tracing (Aruba, Minew and Polestar, AisleLabs, CXapp, Kiana, Meridian Kiosk, SkyFii)
- **Human Activity & Productivity Monitoring**
  - Space Utilization Analytics (Lone Rooftop)
  - Migrating From Break/Fix to Predictive Maintenance (ABB)
  - Facility Control And Digital Twin Enablement (EnOcean and Microsoft)
- **Human Productivity Optimization**
  - Automating Visitor Access To Enhance Staff Efficiency (Aruba, Envoy)
  - Securely Sharing Wireless Networks Without Losing Control (Aruba MultiZone)
  - Seamless 5G To Wi-Fi Roaming Without Distributed Antenna Systems (Aruba AirPass)
  - Reducing Mean Time To Repair With Real-Time Location Services (Aruba APs and Meridian)
- **Safety and Security**
  - Vaping And Air Quality Monitoring (IP Video, Piera)
  - Gunshot Detection (AmberBox)
  - Connecting And Protecting Remote Users And Facilities (VIA, RAPs, SD-Branch)
  - Rapid Deployment Disaster Recovery (Silver Peak SD-WAN, BEC)
  - Reduce Costs and Improve Housing Experience With Electronic Door Locks (ASSA ABLOY)
  - Mobile Panic Button Location Solutions (TraknProtect)
  - Redundant Intra-Site Wireless Video And Data Links (Aruba 5/60GHz Access Point)
  - Monitoring The Switching Fabric To Detect Security-Impacting IoT Issues (Aruba NAE)
  - Context-Aware, Real-Time Integrated Emergency Response And Notification (Meridian and CriticalArc)
  - Securing Control Networks That Can't Protect Themselves (Claroty, Microsoft, Nozomi, Tenable)

INTRODUCTION

What is a smart government facility, and why is the Internet of Things (IoT) relevant to it? A smart facility - whether a high rise building, historic site, mobile clinic, or post office - is an instrumented structure 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 smart facility, and generates logical representations of physical data, i.e., temperature, enthalpy, current consumption, and occupancy, among many others. These data are supplemented with contextual information generated by a smart facility's data network, i.e., identity, location, and applications in use. The combination of data and context enables smart 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 facility can become. Facilities with limited instrumentation have minimal cognizance, while others are fully instrumented and hyper-aware.

Before the advent of IP networks, facility systems operated autonomously from each other with independent wiring plants, devices, and applications for audio/visual, clocks, 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 standby battery life; security for high speed, multi-drop sensors; video for analog signaling over coaxial cable; and so on.

Systems started converging with the advent of modern IP networks and the adoption of the Building Automation and Control (BACnet) communication protocol as an ISO standard in 2003. Sensors and actuators, however, have remained stubbornly isolated from IP networks, relying on specialized, non-interoperable physical layers and protocols. At the edge, smart facility devices are a tower of babel, teeming with systems that operate in parallel but can communicate only thru EnOcean, KNX, DALI, ZigBee, LONWORKS, Hochiki SD, Wiegand, and other gateways.

In some cases local regulations have mandated 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 applications need edge data to deduct status and infer occupant needs. For example, an automated room scheduling system needs identity, presence, calendar, and location data to know when occupants 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 facility IoT systems enough to share context and data is highly problematic.

The 'Achilles heel' of smart facility IoT is security because IoT devices are fundamentally untrustworthy. 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 decades and predate the advent of both modern cybersecurity and the Internet. Replacing legacy devices is often technically and economically unviable, not to mention highly disruptive to on-going operations. Many new IoT devices also lack sound cybersecurity features. For this reason many CISOs will not permit either 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.

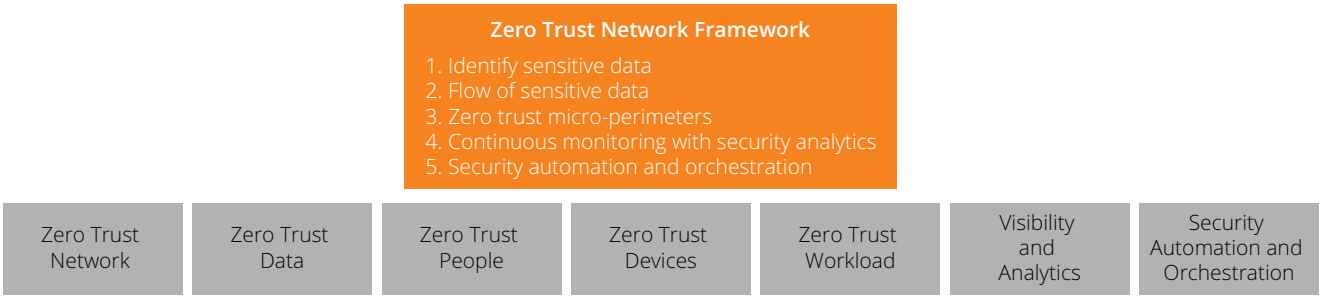


Figure 1: Zero Trust Framework

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 continuous AI-based analytics for anomalous behavior 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 Windows tablet PC tries to masquerade as a chiller, network access should be immediately denied.

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

The government facility control market is very conservative, and the rate of technological change has been significantly slower than the consumer product industry. As a consequence, protecting today's smart facility systems require expertise outside the realm of traditional facility management vendors. Unified communications, cloud-based productivity tools, and augmented reality expertise are needed for activity monitoring, intelligent spaces, and servicing complex systems, respectively. Cybersecurity has to underpin all smart facility systems, and is not a core skill for most suppliers. Nor are location-based services, which have long been the province of IT. And finally there's analytics, a family of highly specialized tools that help institutions leverage the data they collect and are yet another province of IT.

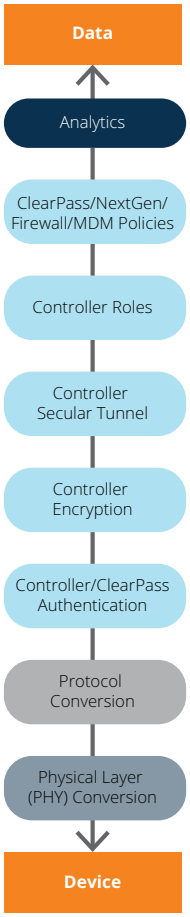


Figure 2: IIoT Protection Mechanisms

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 facility 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 institution's strategic goals for cognitively aware facilities to be realized without incurring unacceptable risk. Let's now examine how to align an institutions strategic goals with the implementation of cognitively aware facilities.

GOVERNMENT 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 institution 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 smart facility IoT projects. Whether it's the allure - or misunderstanding - of the IoT concept, fear of being viewed as a laggard, or pressure to do something new, institutions frequently rush head first into smart facility projects without clearly defining objectives, value propositions, or the suitability of tools. The result is a high rate of failure, and disillusionment among administrators and staff.

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.

How does one determine what is or is not relevant information? Relevance is established by a chain that stretches from the institution's strategic goals, to business objectives designed to achieve those goals, to what Gartner3 calls "business moments" – transient, end user-related opportunities that can be dynamically exploited. A business moment is the point of convergence between the institution's strategic goals and relevant IoT context and data that when properly exploited will positively change experiences, reliability, performance, safety, or security.

Business moments must be carefully orchestrated, even if they appear spontaneous to students or staff. Success hinges on a second chain that stretches from relevant IoT context and data thru 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.

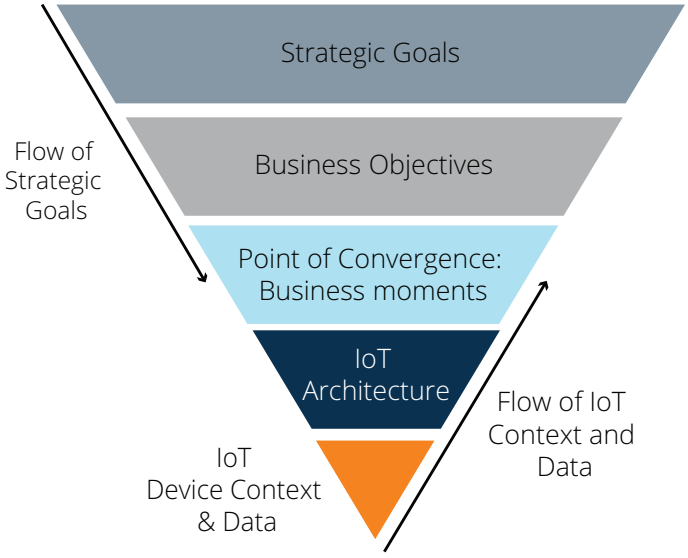


Figure 3: IIoT Strategic Hierarchy

And so we return full circle to the professor and the woodsman. The first order of business in any smart facility IoT project is to identify the institution's strategic 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.

The institution's goals and objectives should inform the smart facility IoT architecture and relevant devices to tap, not the other way around. Solutions selected for eye candy appeal or hype alone will go wanting. And one-size-fits-all IoT solutions simply won't work. The breath of civilian government facilities spans from mobile clinics to city-sized campuses.

Example Devices	Mobile Clinic	Temporary Trailer	Buildings & Public Housing	Bus & Rail Facilities	Campus or Airport
Multimedia Devices	✓	✓	✓	✓	✓
Security Cameras	✓	✓	✓	✓	✓
IoT Devices (Leak Detection, Intrusion, Air Quality, etc.)	✓	✓	✓	✓	✓
Disaster Recovery	✓	✓	✓	✓	✓
Building Lighting		✓	✓	✓	✓
HVAC Controls		✓	✓	✓	✓
Asset Tracking			✓	✓	✓
Food Safety Monitoring				✓	✓
Power Plant					✓
Street Lighting					✓
Water & Waste Water Processing					✓

Table 1: Examples Devices Required By Civilian Government Facilities

Aruba's goal is to help customers access relevant IoT data and context, define and successfully deliver business moments, and, in turn, attain their objectives and strategic goals. Take the City of London, for example. The City is one of 33 local authorities in the UK capital. Also known as the Square Mile, it is the financial district and historic center of London and arguably the most high-profile. The City of London's strategic goal was to drive a digital transformation and mobility enablement agenda that enabled new, more efficient and economical ways of working.

The first task in any smart facility project is to identify the institution'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 manage costs by more efficiently using space and managing people? Enhance personal safety with social distancing and thermographic monitoring? Enhance site security and surveillance? Lower energy consumption? The answer(s) will impact the business moments that need to be delivered, and what constitutes relevant data and context.

To facilitate remote working and enhanced collaboration objectives, the City rolled out Microsoft Office 365 to 4,000 employees across 120 locations while simultaneously consolidating IT across the Police and city operations. To achieve cost and manpower reduction efforts, the consolidation necessitated a single network architecture, but with clearly defined management and security for both stakeholders in compliance with strict Home Office data security standards. Additionally, the City needed identical network and connectivity experiences for all users, across all local and remote locations, without imposing burdensome new workloads on the IT team. The City needed to control who accessed the network, the means by which they accessed it, and what they accessed.

The solution involves more than 1,000 Aruba Wi-Fi access points and almost 400 switches running on the Edge Service Platform across the 120 sites, from Tower Bridge to Epping Forest to the Animal Reception Centre at Heathrow Airport. Aruba ClearPass manages secure and policy-based network access and endpoint integrity, across both wired and wireless infrastructures, for employees, engineers, and visitors. Aruba AirWave proactively monitors and manages the performance and availability of the network and applications.

The result is a hyperaware network with consistent, high-performance wired and wireless connectivity across all locations and mobile devices. The solution radically changed workplace dynamics: new ways of working – on new productivity toolsets – are being driven by users from the bottom up instead of imposed from the top down. For example, video conferencing has spread across the organization including static workers, work-from-anywhere users, and remote users. Business analysts, communication experts, and mobile technology experts can now simultaneously work on a business problem and quickly apply solutions.

REQUIREMENTS

- Consolidate wireless and wired network estate
- Establish a solution and toolset from single vendor
- Meet strict data security regulations
- Encourage a forward-looking organisation, better able to promote London as a place to live, work and visit

SOLUTION

- Aruba 802.11ac Wi-Fi access points
- Aruba campus core and edge switches
- Mobility controllers
- AirWave Network Management
- ClearPass Secure Network Access
- ClearPass OnGuard for advanced endpoint security

OUTCOMES

- Enabled 70% of employees to work from mobile devices
- Transformed productivity with greater use of mobile applications, from video calls to digital stock control to fingerprint scanning
- Strengthened network security with single pane of glass managing access for diverse user groups
- Delivered network insight to better inform future usage
- Inspired culture of innovation, creating a service-led approach to IT

Figure 4: City of London Digital Transformation Outcomes

The reliability, flexibility, and extensibility of the ESP platform accelerates innovation by allowing more mobile applications to be leveraged. Remote working allows the City to consolidate its fixed offices, and greater productivity allows personnel to be refocused on new services. For example, the City of London Police can now use an app to scan fingerprints for improved suspect identification, there is an app to easily report graffiti and pot holes, and another to manage stock at London's largest meat market. When called upon the ESP infrastructure can extend into the City's diverse property portfolio using IoT for smart buildings and air quality monitoring.

The solution completely changes what work means to City workers. Work is no longer a destination but rather the application of technologies wherever users happen to be. While installed to achieve specific objectives, the

infrastructure supports further transformation just by layering new services to the network in an additive process - no rip-and-replace required.

This document presents IoT use cases that are relevant across a broad range of civilian government applications, including and extending beyond those leveraged by the City of London. Many of the use cases include at least one Aruba technology partner whose solution, used in concert with Aruba infrastructure, helps address specific strategic challenges.

SMART GOVERNMENT MARKET

According to McKinsey[4] the total economic impact of IoT in smart cities and facilities in 2025 will be over $1 trillion. Among top areas they identified include air and water monitoring ($400B-$700B), adaptive traffic management ($220B-$500B), human productivity monitoring ($48B-$115B), disaster/emergency services ($20B-$40B) energy monitoring ($12B-$21B), and building security ($3B-$6B):

- Safer air and water are expected to reduce pollution-related fatalities by 15%;
- Traffic management will reduce congestion by 10%;
- Human activity monitoring is expected to increase productivity by 5%;
- Energy monitoring should reduce costs by 20%; and
- Building security should yield a 20-50% reduction in labor costs.

Public health and safety is a top focus for many government institutions, and areas in which IoT can play an important role include video surveillance for crime monitoring, improving disaster response through rapidly deployable solutions, and monitoring the health of street furniture (like municipal lighting) and structures (like bridges and buildings). Applying IoT to air and water quality monitoring could help identify sources of contamination and leaks, and help prevent illness and death.

With regard to smart facilities, commercial real estate services company Jones Lang LaSalle5 observed that, in general real, estate tenants spend roughly $3 per square foot (0.092 per square meter) per year for utilities, $30 for rent, and $300 per for payroll. This "3-30-300" rule of thumb is applicable to government institutions that own or lease facilities, and demonstrates the leverage that comes from improving productivity and efficiency. Pivoting toward human productivity optimization improves space efficiency, and can be leveraged to minimize both real estate footprint and energy costs.

Historically smart facility initiatives focused on energy efficiency because this was – and remains – one of the specialties of building automation vendors. Prioritizing human productivity requires a second pivot towards vendors and applications that specialize in creating cognitively-aware digital spaces. IoT can change the way in which machines and humans interact to make people more productive in those spaces. Done well, frictionless machine-human interchanges belie the complexity of the computing, security, and communications systems needed to accomplish the task. This challenges us to find new ways to simplify human interaction with complex machine-based systems, and new ways to train integrators to install and support these systems.

The breadth of smart facility 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., optimizing energy consumption in research labs or quickly identifying the location of an active shooter? Or is an optimized system-level solution required, i.e., migrating from break/fix to site-wide proactive facility maintenance?

In all cases an extensible platform will be required because smart facility requirements change over time; unlike a point solution, a platform allows institutions to build a broad range of services today and into the future. However, while the platform is necessary by itself it's insufficient to enable a solution since no one vendor makes a universal set of government facility-oriented 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 create cognizant smart government facilities are presented below.

PHYSICAL DISTANCE MONITORING AND CONTACT TRACING

Facility safety extends beyond physical and environmental hazards. Today, physical distance monitoring and contact tracing are essential for both back-to-work initiatives and stay-healthy-at-work programs. Whether mandated by local regulations or institutional policies, maintaining safe distances from others 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 sites, real-time location services and identity

stores have an essential role to play in every physical distancing and infection control solution.

Aruba has both released a Meridian contact tracing application and teamed with multiple technology partners to deliver a broad range of health monitoring 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 government-issued devices;
- Presence detection systems that pick-up Wi-Fi signals from personally-owned or government-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.

aruba
a Hewlett Packard Enterprise company

Aruba Central provides two options for contact tracing using network telemetry from Wi-Fi and BLE, enabling customers to select whichever option best leverages existing infrastructure. Central Proximity Tracing allows username or MAC address queries to identify who came into contact with a specific individual and for how long. This solution leverages existing Aruba wireless infrastructure and intelligent location triangulation. Customer using Aruba AirWave can export data into the Central dashboard as well as popular third-party visualization tools such as PowerBI and Tableau.

The Meridian BLE solution uses Aruba 300/500 series access points in conjunction with Aruba Tags to provide close proximity contact monitoring, heat mapping, and location analytics within a physical building or campus. Tags provide location data for each person or physical asset within the range of BLE-enabled access points, and eliminate the need for a dedicated network of readers or observers.

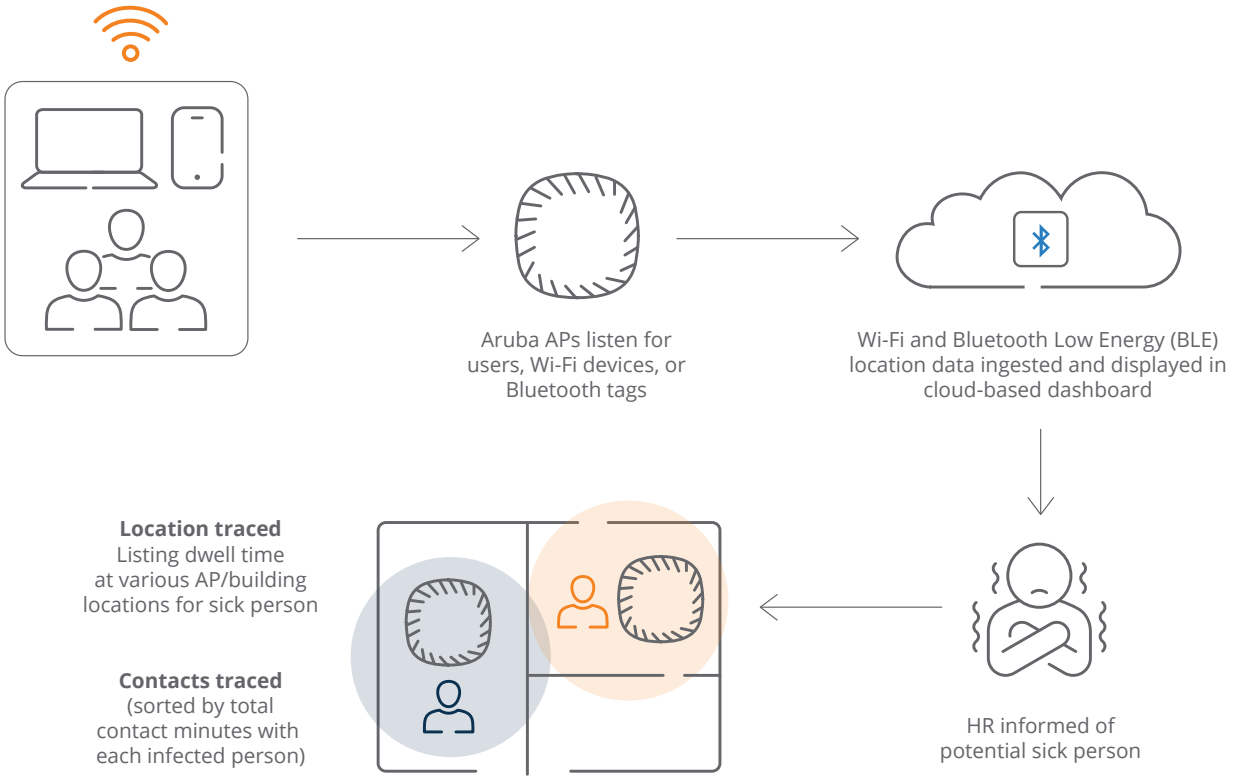


Figure 5: Aruba Distance Monitoring & Contact Tracing Solutions

Minew and Polestar have collaborated to bring to market a social distancing and contact tracing solutions that uses Minew wireless BLE tags to help enforce guidelines for social distancing and automate contact tracing. Available in a wide variety of shapes and sizes, Minew tags forward proximity violations via Aruba access points to the Polestar monitoring application. The solution can provide a prevention score, social distance and overdensity alerts, site maps, expose contact lists, and contact heatmaps

Fig 6: Minew Proximity Tags with Polestar Contact Tracing Applications

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.

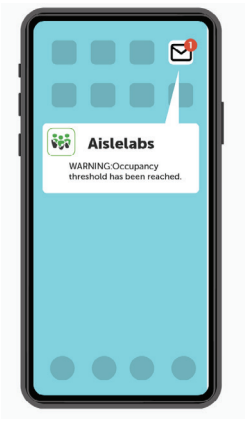


Fig 7: AisleLabs COVID-19 Social Distancing Solution

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 users per square foot, 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.

Traditionally building access control focused on regulating physical access to and within a site, and cyber access to IT, IoT, and OT systems. The COVID19 pandemic, and subsequent health organization guidelines for reducing infections, has forced institutions to expand controlled access to include the health posture of everyone accessing a facility. Enforcing safe social behavior requires vigilance throughout the site journey, starting at the entrance portal and extending across roaming behavior and proximate contacts.

Entrance portal monitoring can take many forms, from manually controlled turnstiles to automated thermographic kiosks that register identity, detect abnormally high body temperatures, and manage access door locks. The former can be implemented in a manner of hours but is subject to manual error during entrance registration and can create significant backlogs during peak entry periods.

Automated kiosks have the advantage of high throughput, highly accuracy temperature measurement, and integration with visitor management, badging systems, and both physical and cyber access control systems. Implementation can be expedited by using proven, off-the-shelf kiosk designs.

Meridian Kiosk is a fully integrated manufacturer of Personnel Management Kiosks (PMKs) that feature user check-in, temperature verification, and optional facial identification. PMKs are designed to protect health and safety by preventing anyone with a high temperature from entering a facility. Kiosks are available in pedestal, countertop, and wall mount versions, with and without a credential printer. All models have a standardized user interface, so regardless of the kiosk style or location users enjoy a consistent access experience. This feature also minimizes the time required to train personnel on kiosk operation.

Meridian Kiosk's MzeroManage software application allows administrators to remotely manage kiosks without needing local access to the site. The software provides e-mail and pop-up alerting, report generation, account management, and APIs to building control and other facility applications.

Aruba and Meridian Kiosk have partnered to integrate Aruba switches and wireless 802.11ax (Wi-Fi 6) and 802.11ac (Wi-Fi 5) access points with Personnel Management Kiosks to securely address the need to rapidly deploy real-time entrance portals indoors and outdoors on a temporary or permanent basis. The kiosks operate on both existing and new Aruba infrastructure, allowing the solution to be retrofit to deployed networks. PMKs work with Aruba campus, Instant, and Instant On access points, as well as Aruba LANs. This flexibility enables PMKs to be deployed anywhere, from mobile clinics using Instant On or Central-based Instant access points, to large campuses using controller-based wireless.

The joint solution allows administrators and public safety officers to check the temperature of every entering a facility, and through integration with scheduling systems control who is allowed access to specific areas and buildings.

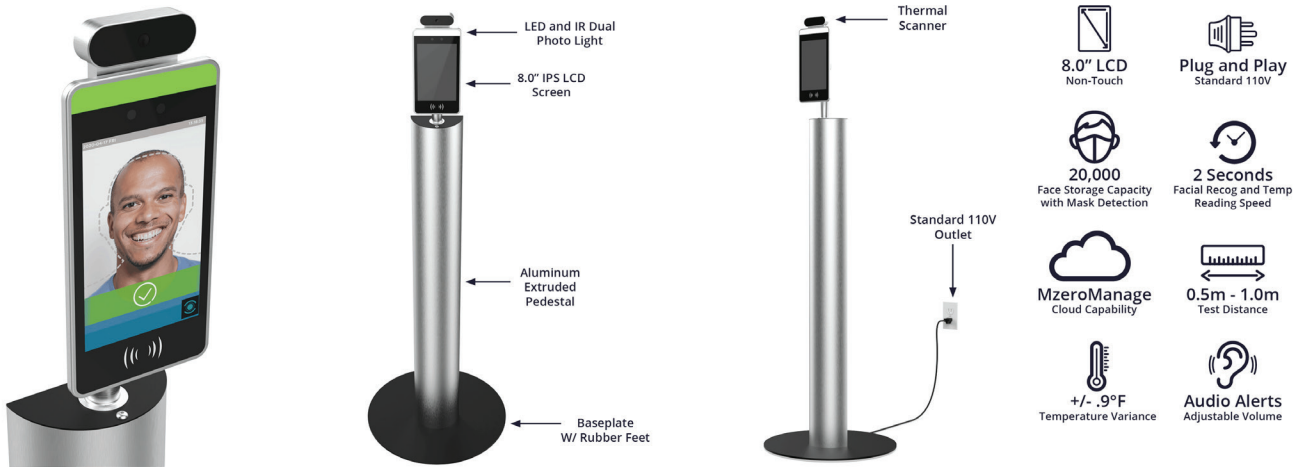


Figure 8: Meridian Kiosk Thermographic Measurement And Registration Station

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.

CITIZEN ENABLEMENT – HOT SPOTS FOR PEOPLE AND THINGS

Citizen enablement is the process of providing fair and equal access to information, advice, advocacy, and justice to a population. Successfully delivered, citizen enablement helps the populace make better informed decisions, understand their rights and responsibilities, enjoy a higher quality of life, and build caring and responsible communities. In the past this was accomplished with a combination of in-person government outreach, printed documentation, and community volunteers. In today's information age, while those factors remain important the great equalizer is Internet access.

Local, municipal, and national governments deploy Aruba Wi-Fi infrastructure as a foundational platform for citizen enablement, initially deploying Wi-Fi hot spots for Internet access and then leveraging the access points' Wi-Fi and IoT radios for a broad range of other services. As noted above, the potential economic impact of IoT in smart city applications could exceed $1.7 trillion in 2025, with nearly $700 billion captured from the improved health outcomes resulting from air and water monitoring. The impact of real-time traffic flow management and the more efficient use of public transportation thru smart routing is estimated at $570 billion. While universal Internet access might be justification enough for the deployment of an Aruba Wi-Fi hot spot network, the pull-thru economic benefits of other citizen enablement initiatives using the same platform can justify expanding and expediting deployments.

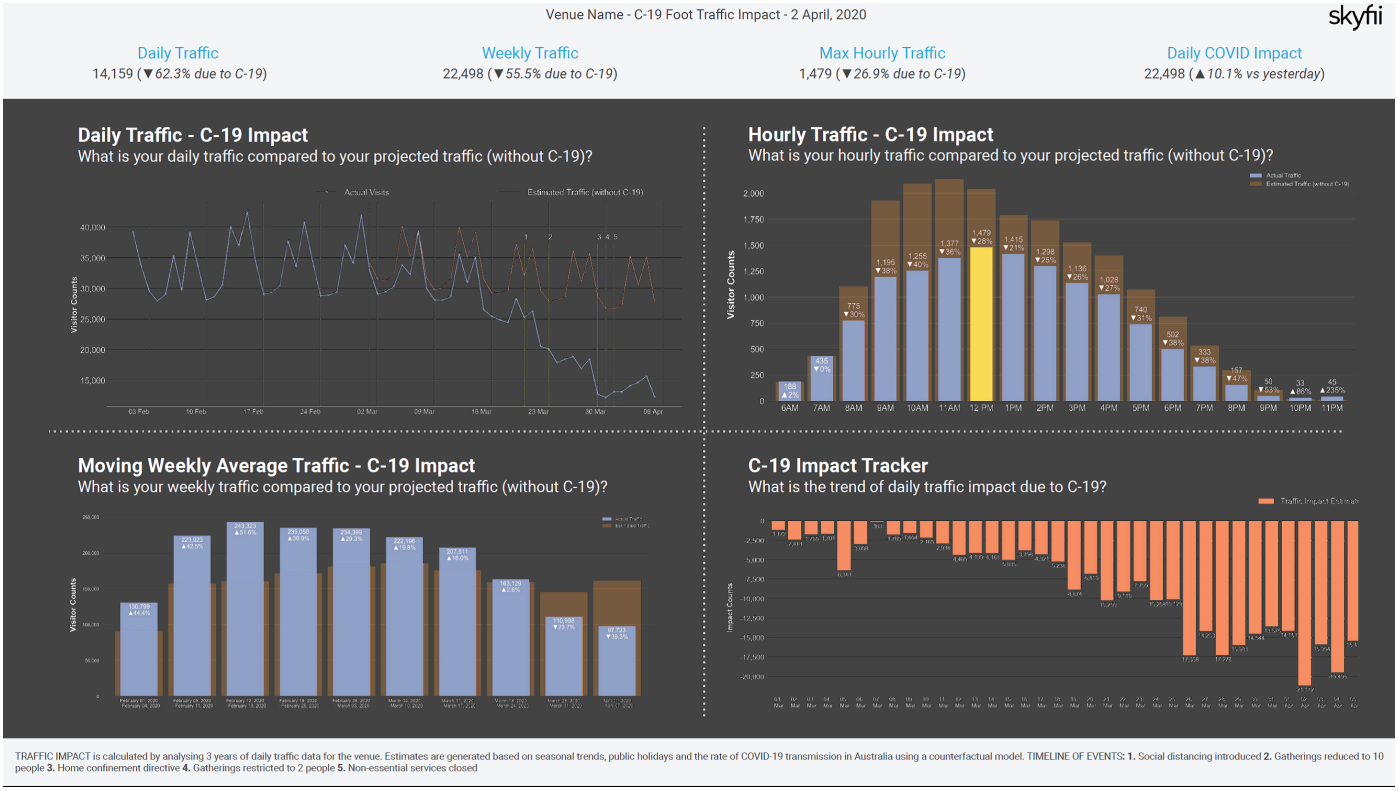


Figure 9: SkyFii OccupancyNow Dashboard

Added-value IoT-based citizen enablement services include among others:

- Broadcasting bus/train/ferry schedules
- Demand-based public transportation routing
- Monitoring air and water quality
- Deploying video surveillance cameras and downloading surveillance video from police vehicles and buses,
- Powering tourist and resident-related information kiosks
- Running wayfinding and tourist-related wayfinding services
- Managing municipal lighting systems

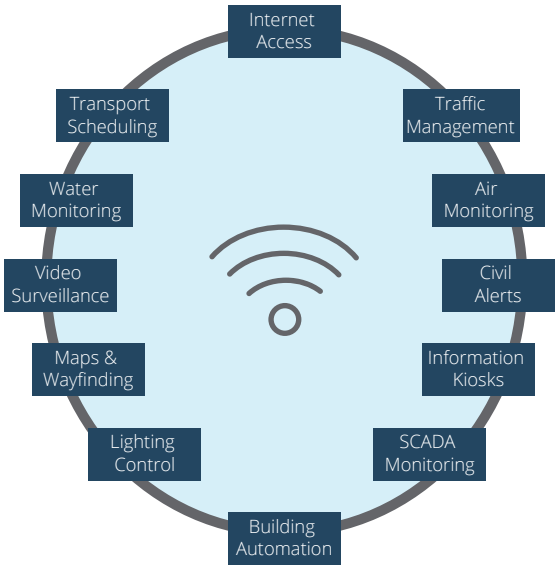


Figure 10: Aruba Wi-Fi Hot Spots form the foundation for an array of citizen enablement services

Aruba's outdoor access points feature a design aesthetic akin to a street lighting luminaire, helping them blend in to architecturally sensitive areas. The compact access point is small enough that it can be concealed within a radio-transparent, customer-sourced fiberglass housing when period authenticity is needed. That's possible because, unlike most competing devices, Aruba outdoor access points are available with internally hidden antennas. Concealed antennas reduce weather-related water incursion, have no external antenna connectors to corrode, and are less likely to be vandalized than access points bristling with visible antennas.

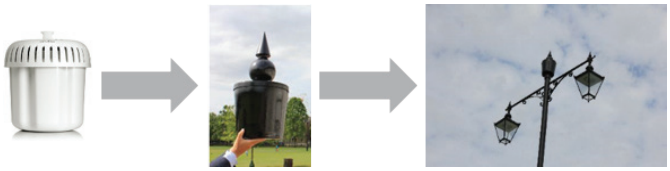


Figure 11: Aruba Access Points: Rugged, Diminutive, Concealable

Citizen enablement is exemplified by the RajNet Wi-Fi connectivity project. A state in northern India, Rajasthan is the largest state by size and the seventh largest by population. Prior to the RajNet project large swathes of rural areas has been without Internet access. RajNet was launched to bring rural citizens access to all the Internet has to offer—from micro-loan financing to remote learning to public safety.

To accomplish this Rajasthan deployed outdoor Wi-Fi at 15,000 locations to provide connectivity for citizens and tourists at government offices and state-owned enterprises. Each village has a self-contained Wi-Fi cell using an Aruba access point powered by solar energy, and the system is centrally managed in Jaipur. Among the connected sites are 10,000 Atal Sewa Kendras (ASK) government institutions, which provide public utility services such as the Aadhaar identity card, the PAN card for tax identification and payment, utility bill payments and ration cards.

SPACE UTILIZATION ANALYTICS

We commonly think of Wi-Fi networks as access ramps onto government networks and the Internet, but Aruba access points are also IoT platforms that generate contextual information for facility-critical services and applications. Location data identifying the position of people and assets are especially valued because they can be applied in so many ways including space utilization, facility operations, process optimization, safety, and energy management. Successful exploitation of location starts with simplifying the collection and dissemination of location data, and then extracting deep insights by leveraging a powerful analytics engine.

Aruba's Analytics & Location Engine (ALE) software simplifies location data collection by calculating the x/y position of all associated and unassociated Wi-Fi enabled smartphones, laptops, tablets, and IoT devices within range of Aruba access points. These data are then aggregated and streamed to analytics applications over a secure link. Aruba has built a stable of analytics partners that consume ALE data to deliver location-enriched business insights.

LONE ROOFTOP
building intelligence

Lone Rooftop is an ArubaEdge technology partner that leverages ALE data to show facility and real estate managers in real-time how many people are in the building, and where and when they're present. Their Position Intelligence Engine (PIE) is a cloud-based technology platform that uses ALE to

automate occupancy data collection traditionally undertaken manually by staff members equipped with clipboards and spreadsheets.

Understanding the utilization, frequency, recency, and other parameters impacting how space is used can better inform space requirements and spending decisions. Oversubscribed spaces can be identified and expanded, while underutilized floors or even entire buildings can be decommissioned or subleased. Real-time reporting and alerts broaden the number of use cases. For example, adjusting cleaning schedules based on actual space usage and real-time cleaning demand lowers costs and directs resources only to spaces that need them. Similarly, predicting facility cleaning usage based on building occupancy can lower cleaning time and cost.

Real-time analytics can also boost productivity. Statistics show that 40% of flex space staff routinely waste working time looking for available hoteling desks. PIE-enabled mobile apps and kiosks can instantly identify which spaces are available so workers don't have to hunt on their own. PIE's Building Intelligence Dashboard draws from real-time location data, and allows cross-comparisons between sites. PIE data are centrally stored and managed, and can be easily shared with new applications that require location data.

The joint solution uses Aruba 802.11ac and 802.11ax access points, ALE, and AirWave Management Platform already deployed on site. No access points need to be ripped-and-replaced, no occupancy sensors or people counters are required. All that's needed is an instance of ALE 2.0 or higher.

PIE anonymizes personally identifiable data: the system counts the number of people in spaces but cannot identify who they are. The cloud-based solutions can be quickly brought online and produce meaningful insights in just a matter of weeks.

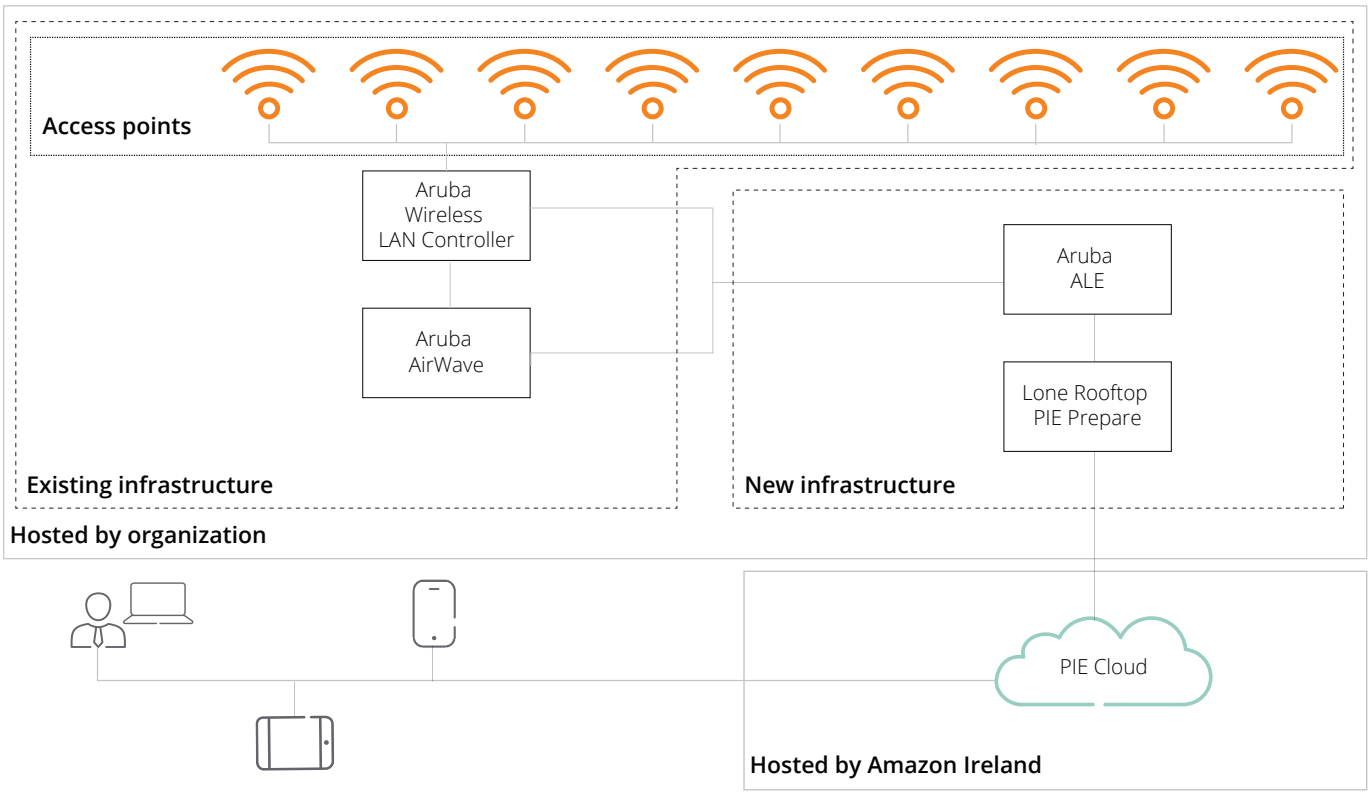


Figure 12: Aruba and Lone Rooftop Integration Overview

Combining an Aruba mobility network with Lone Rooftop space analytics delivers some very unique value propositions:

- Space analytics can be easily retrofit to existing Aruba deployments;
- Implementation does not require occupancy, footfall, or video sensors;
- Adds/moves/changes to the building layout are easily accommodated without rewiring; and
- Anonymized data overcome the privacy and union labor restrictions of video-based analytics.

Space analytics are an essential element of a contextually aware facility, helping sites assess real estate footprints and predict future needs based on actual usage. Aruba's secure mobility platform is the ideal foundation on which to build space analytics for facilities of virtually any size.

MIGRATING FROM BREAK/FIX TO PROACTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep facilities 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 facilities 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 to additionally capture machine status from IoT sensors. A dual-use IT/IoT 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 Ability™ 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, chillers and pumps for abnormal behavior indicative of pending failure. Status is communicated over a secure Bluetooth link, and analyzed by ABB's advanced algorithms. Facilities 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 move from break/fix to proactive 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 Ability™ Smart Sensor data to the ABB Ability™ Condition Monitoring application. Using Aruba zero trust infrastructure as a data collection platform provides uniform security and visibility across both IT and IoT domains. It eliminates the costs and security risks and costs associated with large fleets of gateways. Since gateways filter raw data streams that can be rich in visibility data, removing them has the added benefit of improving visibility all the way down to individual sensors.

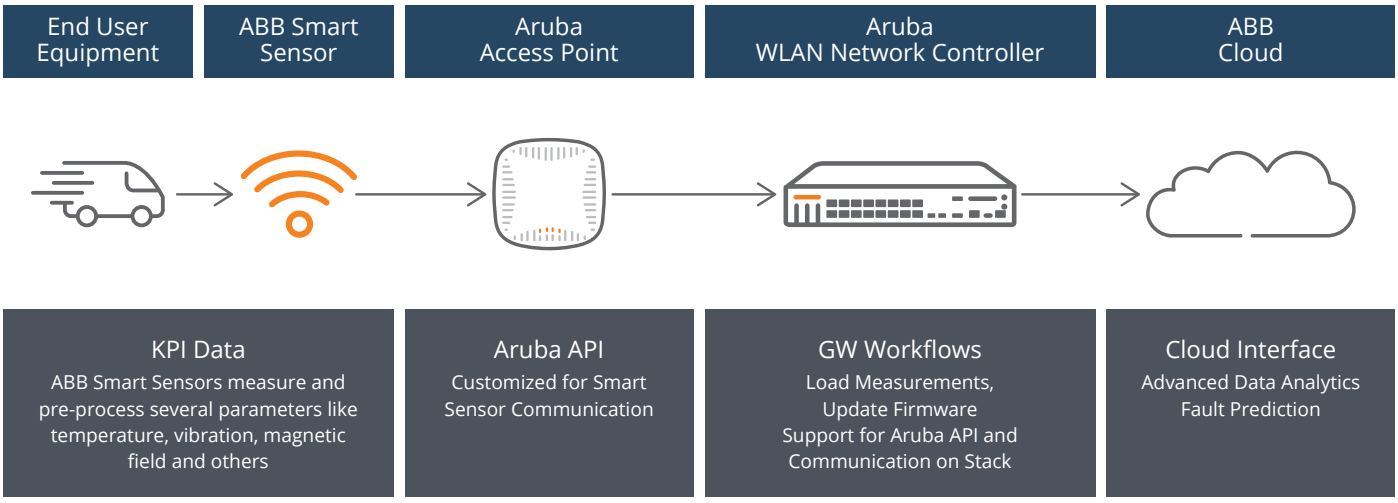


Figure 13: Aruba and ABB Integration Overview

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 deployment since adds, moves, and changes are easy and inexpensive.

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

FACILITY CONTROL AND DIGITAL TWIN ENABLEMENT

Situational awareness is essential to building cognitively aware facilities. IoT devices are the eyes and ears of a smart building, and are given voice by the secure connectivity infrastructure through which they talk with facility applications. The better instrumented the site, the more informed the insights that can be made across time and space, including projections of future occupant and system behavior. For example, energy monitoring cuts across many sub-systems, encompassing a wide variety of IoT data including power quality, power consumption, leak detection, air and fluid flow, enthalpy, refrigeration, lighting, temperature, and humidity.

Digital twin modeling combines IoT monitoring data with artificial intelligence, historical data, domain knowledge expertise, and graph modeling to establish and analyze relationships between and among devices and systems. By creating real-time simulation models in the digital world that change and learn in lock-step with the classroom, lab, building, or campus, digital twins can identify sub-optimized processes, recommend operational enhancements, assess complex systems that would be too difficult for a human to track, and monitor the trajectory of energy usage needed for proactive interventions.

The benefits of facility monitoring and digital twin modeling hinge on the availability of timely access to relevant IoT data. Securely and economically interfacing IoT monitoring devices across a site can be challenging. The breadth of telemetry to be gathered, interfacing with legacy IoT devices that use non-interoperable protocols, securing the data path, and importantly the cost of deployment – initially and during adds/moves/changes – can be daunting and expensive.

Wired monitoring systems require dedicated cabling, which is expensive to deploy and labor intensive to maintain. Wireless IoT devices are more economical to deploy but the cost of battery maintenance can be prohibitive.

As buildings deploy next-generation Wi-Fi 6 wireless networks for human activity monitoring, that same secure IT infrastructure can be leveraged for facility monitoring and digital twin applications. Advanced access points that have built-in IoT radios, and support for external USB adapters, can serve as IoT data gathering platforms.

The remaining hurdle is to eliminate batteries wherever possible. Energy harvesting technology derives, captures, and stores power from external sources, e.g., kinetic and visible light. Miniaturized energy harvesting power sources, embedded inside IoT sensors, can solve this problem and allow sensors to be placed wherever needed with no wires or maintenance.

enocean® enocean® alliance

EnOcean, a venture-funded spin-off of Siemens AG, is the creator of the ISO/IEC 14543-3-10/11 energy harvesting 800/900MHz wireless standard. More than 400 EnOcean Alliance vendors make facility monitoring and control systems using this standard. Sensors require no batteries for power, and no wires to communicate, making them economical to deploy and maintenance-free.

RS-232, RS-485, ModBus, LONWORKS, BACnet, KNX, and DALI control systems and devices are supported via locally powered, EnOcean-enabled gateways. These gateways extend the reach of monitoring and digital twin applications into legacy infrastructure, yielding deeper visibility and insights without incurring the cost of ripping-and-replacing installed devices.

EnOcean and Aruba have partnered to allow Aruba Wi-Fi 5 and Wi-Fi 6 access points equipped with EnOcean 800/900MHz USB adapters, and using Aruba OS version 8.7 or later, to communicate bi-directionally with ISO/IEC 14543-3-10/11 compatible devices. With literally thousands of such devices and gateways from which to choose, virtually any monitoring application can be accommodated. The joint solution can be retrofitted to existing Aruba deployments, extending the value of sunk capital investments.

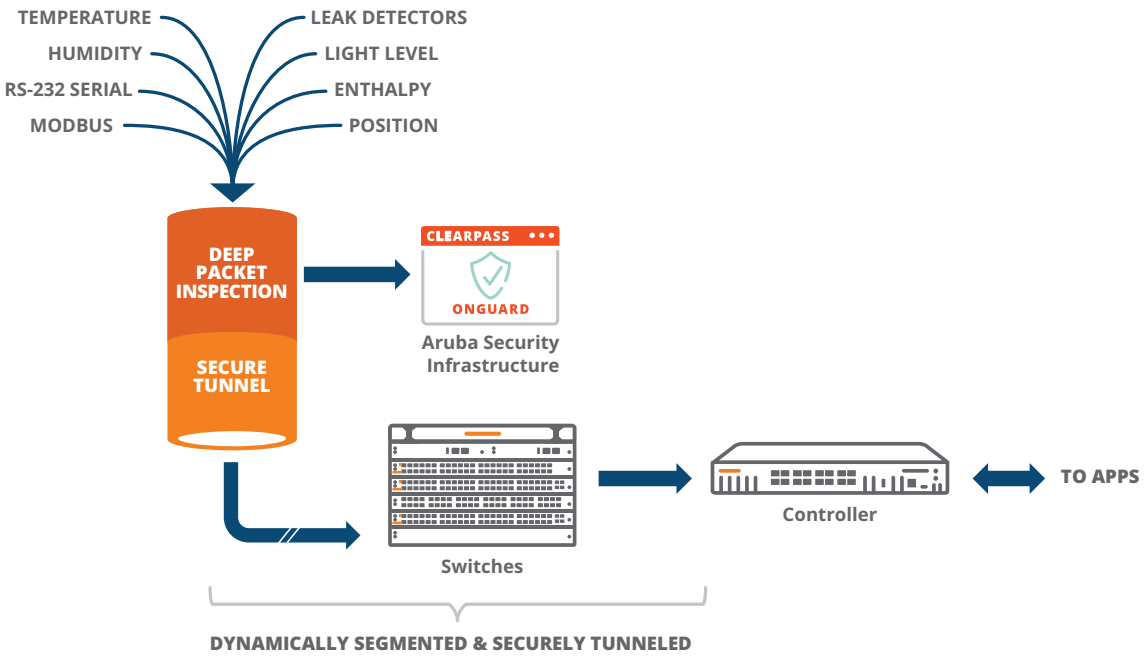


Figure 14: Aruba Access Points are IoT Platforms for EnOcean device data

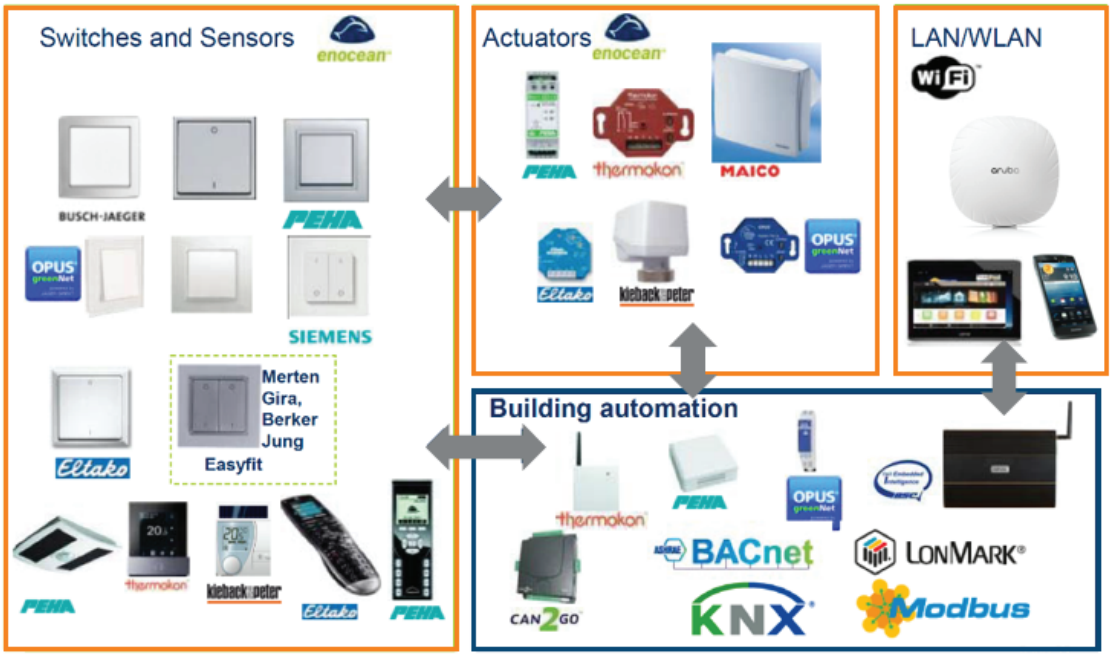


Figure 15: EnOcean Ecosystem

Aruba access points stream EnOcean telemetry data in real time via protobuf to monitoring applications over a secure Web socket connection. Applications can be on-premise, or in a public or private cloud. The EnOcean Alliance includes software application vendors as well as device vendors, and ensures interoperability between both.

The wide range of available ISO/IEC 14543-3-10/11 compatible devices, combined with the security and extensibility of Aruba infrastructure, delivers an extraordinarily flexible and economical way to monitor energy and other building functions. The solution can be extended into satellite buildings and branches should remote monitoring and control be needed.

Azure IoT Hub

For Azure IoT customers, Aruba access points can directly forward EnOcean and other IoT packets to the Azure IoT Hub for processing. Using either AOS 8.8, or an add-on software interface available from Aruba for previous AOS releases, the access points establish a secure Web Socket connection with the Azure cloud and payloads are converted into a JSON format consumable by the Azure IoT Hub. This feature eliminates the need for separate gateways, reduces processing latency, and gives customers the flexibility to add/move/change Azure IoT support at any time.

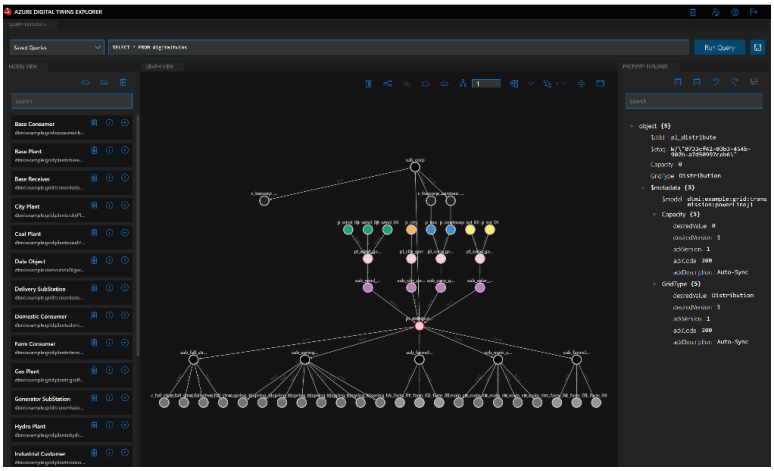


Figure 16: Azure IoT Digital Twins IoT Live Execution Visualization

Customers that want digital twin modeling and telemetry monitoring can use this feature - on-premise or in the Azure cloud – to leverage the Azure Digital Twins IoT service. The Azure Digital Twins service creates spatial intelligence graphs to model relationships and interactions. Thru the service users can build reusable, highly scalable, spatially-aware digital models based on their physical plants, and use them to identify optimize processes and remedy issues.

Key features include:

- Open modeling language to create custom domain models of any connected environment using Digital Twins Definition Language;
- Live execution environment to bring your digital twins to life in a live graph representation;
- Input from IoT and business systems to connect assets, including IoT devices, using Azure IoT Hub, Logic Apps, and REST APIs; and
- Output to Time Series Insights, storage, and analytics using event routes to downstream services including Azure Synapse Analytics.

For additional documentation on Azure IoT Digital Twins please go to https://docs.microsoft.com/en-us/azure/digital-twins/. For a video overview of features and capabilities please go to https://azure.microsoft.com/en-us/resources/videos/azure-digital-twins-video/.

AUTOMATING VISITOR 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 visiting personnel and contractors. On-boarding visitors onto IT, IoT, or OT 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 local security systems and/or have no access to on-site applications and servers. The solution must both simplify visitor access so it doesn't create an administrative burden, and implement security policies that tightly control what visitors 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 facility network(s), guided to their destination using wayfinding, and enable personally-owned devices to securely connect to projection screens, applications, 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.

Aruba 500 Series Wi-Fi 6 Access Points are recommended because of their Wi-Fi performance and integrated IoT radios for smart facility sensing and control devices. ArubaOS 8.4 or newer code running on a Mobility Conductor/ Mobility Controller, Aruba Instant, and/or Central cloud 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).

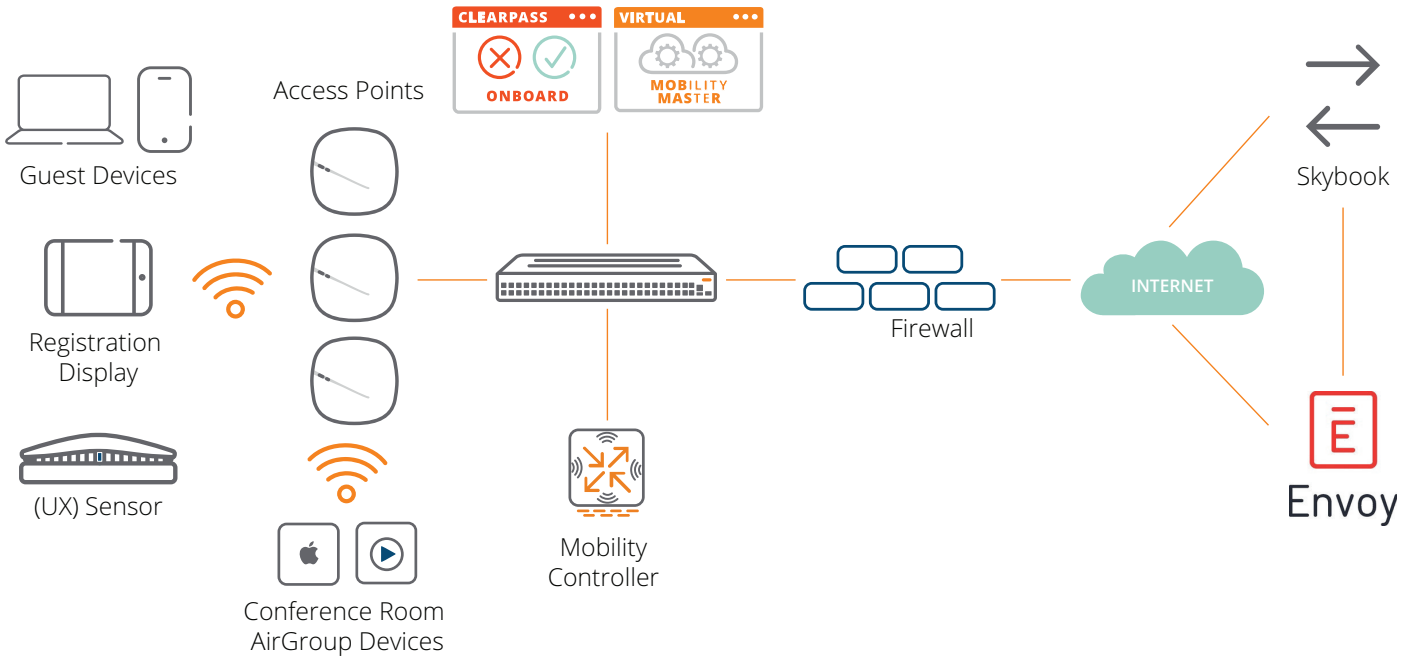


Figure 17: Automated Visitor Access Solution to Enhance Security & Efficiency

Envoy

Envoy Visitors is a visitor management platform for a modern front desk that helps streamline visitor sign-in. When visitors arrive, Envoy makes it easy for them to register, presents relevant non-disclosure and health/safety forms for completion, and notifies the sponsoring host of the visitor's arrival via e-mail or SMS. Simultaneously, ClearPass dynamically provisions temporary Wi-Fi access credentials for the visitors' devices and 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 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 visitors need to circumvent IT security just to obtain reliable connectivity.

SECURELY SHARING WIRELESS NETWORKS WITHOUT LOSING CONTROL

Security concerns aside, smart facility wireless network access is often tightly controlled so that critical services, such as multimedia applications and Wi-Fi Calling, are not impacted by wireless users. However, growing demands for mobile device wireless access to enhance 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 had access to the traffic they managed. 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.

The multi-tenancy design of MultiZone is ideal for smart facility applications. Separate Data Zones can be allocated to the groups managing, say, government employees, auditors, building controls, and contractors. Each group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services. Institutions 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 building, then you can't extract or share information. The prevalence of reinforced concrete, low-emission glass, energy-efficient construction materials, and evolving building codes have made indoor wireless coverage from outdoor cellular networks a recurring challenge in government facilities. 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, institutions have addressed indoor cellular issues 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.

As a result, 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.

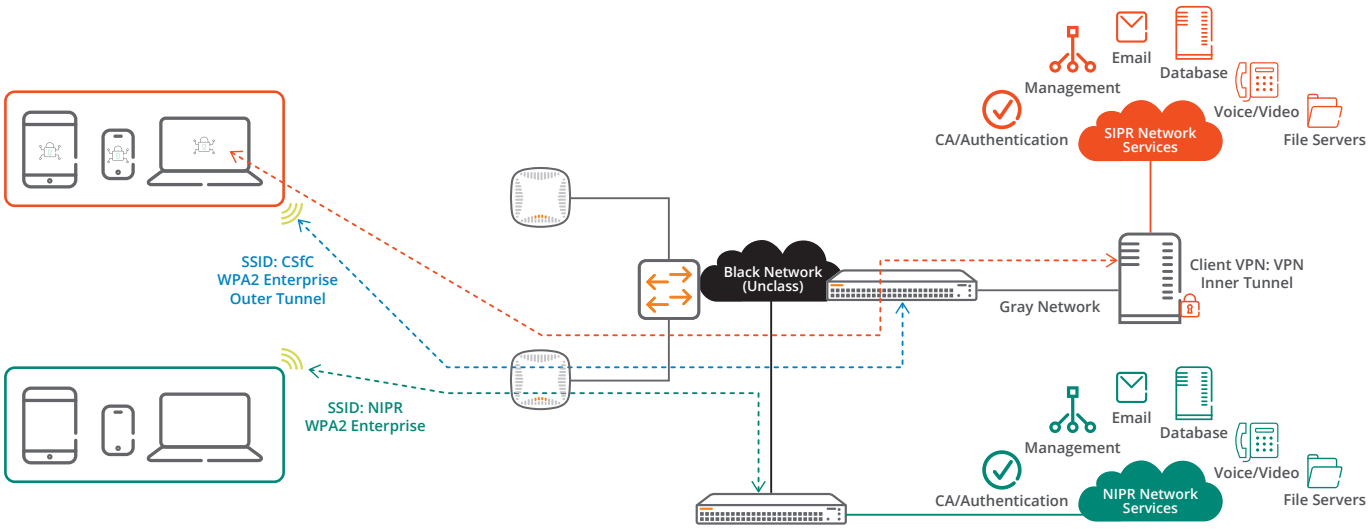


Figure 18: Aruba Multizone Solution

Aruba Air Pass is the industry's first seamless cellular roaming solution designed to unify on-premise 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 nconsistent cellular connectivity.

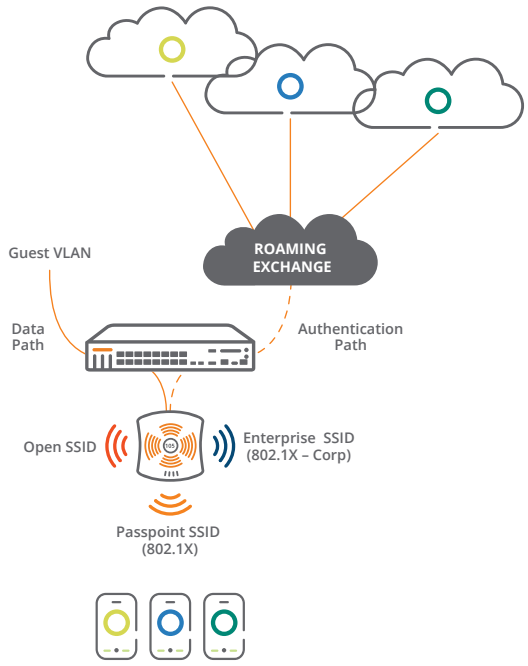


Figure 19: Aruba AirPass System Architecture

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 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 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 staff, administrators, visitors, and devices work and roam.

REDUCING MEAN TIME TO REPAIR WITH REAL-TIME LOCATION SERVICES

Many facility subsystems today have siloed repositories of IoT device data. Even though these data are rich with insights if properly mined, the justification for isolation is that these data are needed for facilities-owned processes which, if exposed, could be attacked or impacted by IT actions such as system updates, reboots, or maintenance.

The downside of isolating data is that it deprives applications of valuable insights that could make a building more cognizant if mined in conjunction with other data sets, i.e., location data and predictive maintenance. Sharing contextual data – location, users, devices, and applications that originate from IoT devices and the personnel who use and manage them – can significantly enhance cognitive insights. With proper data life cycle governance these sources can be safely and securely shared, and reveal trends in usage, traffic flows for scheduling maintenance, excessive energy consumption relative to peer buildings, and so on.

Application	Role of Location-Based Services
Human productivity optimization	Guide occupants to meetings and places of interest Improve time and motion paths Validate contractor activity
Predictive maintenance	Wayfinding to guide service personnel
Inventory optimization	Quickly find displays and high value equipment
Health and safety	Guide occupants to muster points Social distance monitoring

Figure 20: Location-based services by application

From among the many types of available contextual data, location data are particularly insightful. Location data can guide us unescorted through facilities, improving our experience without encumbering others to assist us. They can help us keep track of people wherever they learn, work, or roam. And they can track capital assets so they can be quickly located and repaired.

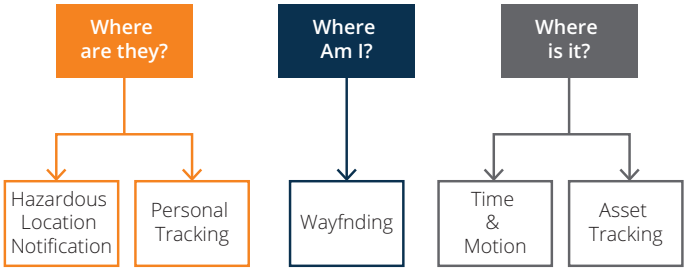


Figure 21: Aruba Location Services and Target Applications

Large facilities and campuses can be difficult to navigate. If someone is delayed or lost traversing the facility the consequences can range in severity from lost revenue or time to loss of life. Engineers, contractors, and public safety officers can all benefit when a self-navigation solution – "wayfinding" – delivers them to their destinations quickly and unassisted.

Additionally, the contextual data generated along the way can be mined for process-improvement related information. Examples include notification of hazardous areas that require safety gear, flagging occupied areas in the event of a security incident, and tracking contractor time spent on site relative to what was billed.

Aruba's Meridian platform is a mobile application platform that provides self-guided wayfinding, geofencing, and push messaging services for a broad range of IoT applications. The system consists of the following components:

- Location Beacons - standalone or integrated into Aruba access points;
- Meridian Application (App) for tablets and phones; and
- Meridian cloud service.

Beacons use Bluetooth Low Energy (BLE) to broadcast an anchor location that is picked up by the Meridian App and shared with the cloud service to assist with locationing. Beacons are built into Aruba Wi-Fi 5 and Wi-Fi 6 access points, including Class 1 Division 2/ATEX Zone 2 models qualified for HazLoc environments like fuel refilling stations. Standalone battery- and USB-powered beacons are also available.

Fig 22: AP-530 Wi-Fi 6 Access Point With 802.11ax, BLE, And 802.15.4 Radios

Fig 23: AP-375EX Access Point for Hazardous areas like Propane Storage and Fuel Refilling

Typical wayfinding applications include:

- Guiding campus visitors to locations of interest and muster stations;
- Navigating service personnel to machines in need to repair; and
- Providing self-service navigation around large sites and complex buildings like medical centers and maintenance yards.

Self-guided wayfinding directs users to specific locations, and offers a simple way to pinpoint their current location, search for points of interest, and access turn-by-turn directions both indoors and out. A glowing dot shows the user's location on a map, and tracks their progress along the route. Users can retrieve turn-by-turn directions from their current location without entering a starting point, an important time saver in emergencies that require mustering to safe areas.

Wayfinding also enables contractors to navigate sites without assistance, conserving operational and administrative resources from acting as guides. Upon nearing a target destination, a logical geofence can be triggered and push a contextually-relevant message or notify a relevant application, i.e., retrieve machine service records. The power of Meridian comes from the context it applies to user engagement, the precision of its geofencing, and the flexibility with which it can interact with other systems.

Reducing mean time to repair (MTTR) is a prime example of the value Meridian brings to smart facilities applications. Imagine that the bearing on an air conditioning chiller to wear unevenly, and is picked up by multi-axis accelerometer in an ABB Ability Smart Sensor. The sensor relays an alert via an Aruba access point to the ABB Ability monitoring application, which dispatches an engineer preemptively before the bearing fails.

Instead of leaving it to the engineer to navigate the building on his or her own, however, the Meridian App triggers a geofence when the engineer enters the building – notifying the institution's Finance Department when work commences - and then guides the engineer using turn-by-turn navigation to the failing machine.

Fig 24:Meridian Turn-By-Turn Wayfinding

As the engineer approaches the machine another geofence is triggered, recalling the service record for that chiller and again notifying Finance that repair work has commenced. Once the repair has been effected the engineer is guided to back to his/her truck and a third geofence notifies Finance that the work has been completed.

In large campuses wayfinding can reduce the mean time to repair by tens of minutes per incident, making engineers more efficient and reducing the risk of equipment failing while awaiting the arrival of service personnel. Equally important, the same location services can reconcile service charges and labor allocations, a complex tasks at sites with many contractors and/or service engineers.

ENHANCING THE RELIABILITY AND QUAILTY OF MOBILE STAFF COMMUNICATIONS

As institutions accelerate their migration from wired phones to mobile communication devices – for food services workers, lab and clinical staff, maintenance and cleaning teams, and administrators - network edge access has to shift from wired Ethernet to Wi-Fi. Providing the quality of service (QoS), bandwidth, and management tools necessary to deliver secure, toll-quality voice and jitter-free video at scale to mobile devices over Wi-Fi requires sophisticated wireless infrastructure. Aruba's AI-based application and device fingerprinting enable the infrastructure to detect the types of traffic flows, and the devices from which they originate. The network is then dynamically conditioned to deliver the required QoS - on an application-by-application, device-by-device basis - needed to deliver highly reliable voice, video, secure texts, and other multimedia services. The result is a superb user experience in which users can roam while staying connected with each other, anywhere in the facility.

These services are delivered over the same Aruba Wi-Fi infrastructure that is used for mobile IoT telemetry, IT devices, and OT facility operations systems. Converging all services under Aruba's extensible ESP platform yields considerable cost savings, enables IT to deliver uniform security and visibility from end-to-end, and allows additional services to be added on without ripping-and-replacing infrastructure. These features supplement Aruba's Air Pass technology – discussed elsewhere in this paper – which allows cellular users to seamlessly handoff voice and data between cellular and Wi-Fi networks.

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

Application Prioritization

Wi-Fi bandwidth is a limited and shared commodity, so it's important that business-critical applications can be prioritized over social media and lesser priority apps. Aruba's deep packet inspection engine automatically identifies thousands of different mobile applications on launch. When a work-critical application is recognized, the network will automatically establish a bandwidth contract to reserve sufficient bandwidth for proper operation. Non-critical applications are given bandwidth prioritization to deliver the best possible experience needed without compromising performance.

QoS

Many applications use end-to-end encryption to protect confidentiality and privacy. Unfortunately this breaks QoS mechanisms on typical wired and wireless networks, as they are unable to differentiate between non-critical and latency-sensitive encrypted 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/video call type, and client sessions active at the time of the call

This method allows Aruba's management and operations tools to display dropped calls, low MOS values, and performance degradation per user location and device. Aruba controllers and virtual controllers can then use these data to implement Call Admission Control (CAC) based on bandwidth and call count to boost available throughout, reduce dropped calls, minimize bandwidth oversubscription, and lower traffic congestion. The result is significantly improved user experience involving multimedia and latency-sensitive calls.

Locating, harvesting, and conveying relevant, trustworthy IoT data and context is easier said than done. Data must be captured with fidelity, over networks that reach wherever IoT devices are working or roaming. And cybersecurity must be implemented and enforced, from machines that run the plants up to administrators that manage the institutions.

It is on these last points that fractures typically appear in many applications. Data input is often hit or miss. Voice communications with staff are unreliable, especially when roaming.

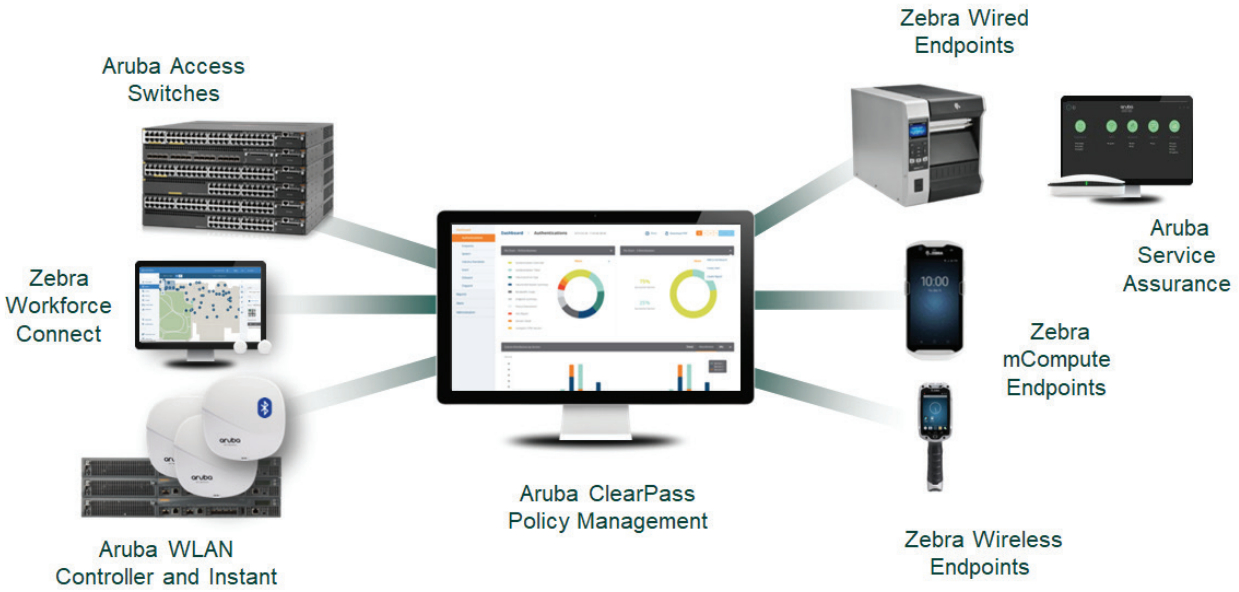


Figure 25: Aruba and Zebra Integration Overview

Zebra's Workforce Connect solution provides a single platform for collaboration with workflows based on contextual data. This enables users to more efficiently do their job while only needing to carry one mobile device.

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

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 point-of-sale, clinical, retail, large public venue, and public safety applications. Joint systems go in faster and more reliably.

REDUCE COSTS AND IMPROVE HOUSING EXPERIENCES WITH ELECTRONIC DOOR LOCKS

Historically, housing-related Wi-Fi, door locking, lighting control, and heating and ventilation systems have been tailored for each application. The result has been a network of networks that don't interoperate, are expensive to deploy and maintain, and have multiple management and diagnostics systems. Lacking a consistent digital identity for each occupant, these solutions were also unable to deliver highly personalized experiences.

Aruba ESP addresses this issue by unifying IoT, IT, and OT networks so institutions can quickly integrate new systems and adapt to changing environments and user requirements. ESP is the first fully programmable platform to power more efficient decision making, and used with devices and applications from Aruba's technology partners, Aruba ESP helps institutions quickly adapt to evolving occupant needs. Virtually every subsystem - from machine inputs and outputs (I/O) in chillers to multimedia rooms, social distance monitors to air quality monitors detectors, HVAC monitoring to campus wayfinding - can be accommodated.

ASSA ABLOY
Global Solutions

ASSA ABLOY Global Solutions is the world's largest supplier of hospitality locks and in-room safes. ZigBee-enabled VingCard® products are the most widely deployed in-room door locks for lodging applications in the hospitality, healthcare, and education markets.

ASSA ABLOY Global Solutions and Aruba have collaborated to certify Aruba access points for use with VingCard in-room locks, and securely connect them with the Visionline management software by ASSA ABLOY Global Solutions. Separate Zigbee gateways are not required, and the solution can be used in both new and existing Aruba Wi-Fi deployments.

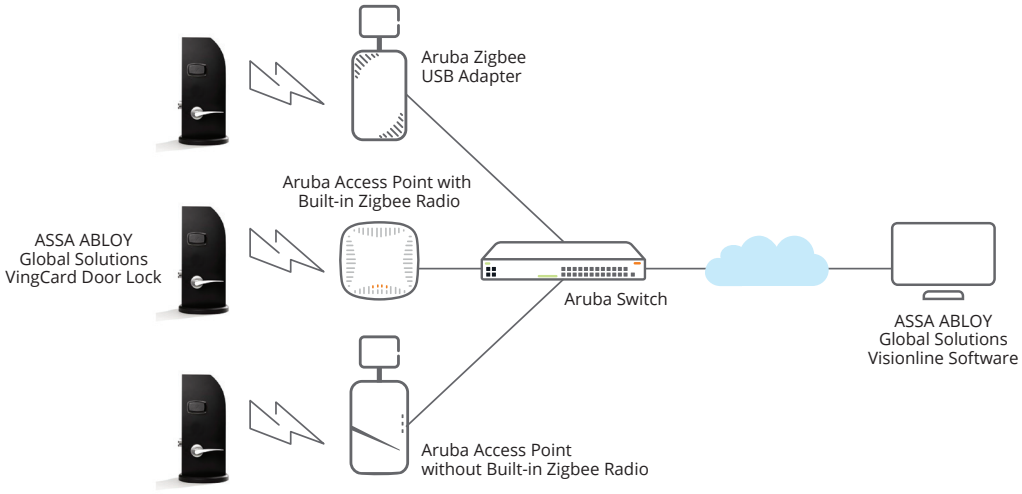


Figure 26: ASSA ABLOY and Aruba Joint Solution Diagram

Once deployed, the access points secure communications between the in-room locks and Visionline lock management software, while simultaneously handling occupant Wi-Fi and multimedia content delivery. Aruba Wi-Fi 6 access points have an integrated 802.15.4 radio running Zigbee already built-in. Customers that have deployed Aruba Wi-Fi 5 access points can add Zigbee support by using Aruba's low-cost, plug-in ZigBee USB Adapter.

The joint solution allows housing staff to remotely manage and monitor VingCard locks, eliminating needless trips by students to the housing office, and by operations staff to the rooms. Benefits include greater security and control, enhanced services, and more efficient service desk and engineering operations. The platform uses the latest in data encryption and secure channel transmission technology to ensure that only authorized users can gain room access.

Occupant benefits include dropped key and door ajar protection. In a traditional off-line lock, if an occupant inadvertently drops a room key then whoever picks it up can go door-to-door until they find a door the key will open. With the ASSA ABLOY Global Solutions on-line system, an alert will be raised and the key invalidated after a specified number of unsuccessful unlocking attempts. If a door isn't closed properly and remains ajar, the system can automatically notify security staff to check the room.

Facility operations also benefit from converging VingCard locks and Aruba wireless technology. Engineering can be notified automatically of low battery and other maintenance conditions before locks stop functioning and occupants are locked out.

MOBILE PANIC BUTTON LOCATION SOLUTIONS

Staff and administrators are routinely exposed to safety risks in parking garages, housing facilities, unoccupied buildings, clinics, and maintenance yards. These risks impact health, morale, and retention – not to mention human life - and represent a serious threat to the reputation and financial wellbeing of an institution.

Portable panic buttons, also referred to as Employee Safety Devices (ESDs), alert security personnel in the event of dangerous or threatening situations. Used in conjunction with location-based services, ESDs can quickly raise an alert and guide safety personnel to the incident location. Besides raising assistance, the physical presence of ESDs can also serve as a visible deterrent to individuals with malicious intent.

Installing a dedicated network to support ESDs is not economically viable, and many IT departments will not permit an overlay network. Battery-operated wireless sensor networks present cybersecurity risks because they bypass standard IT security monitoring tools, and have maintenance issues associated with battery replacement.

Aruba's access points overcome these issues by incorporating Bluetooth and other ESD-compatible radios. This allows IT managed infrastructure to enhance safety, using Aruba security mechanisms to protect against malicious or unintentional security breaches.

TraknProtect

TraknProtect is a leading supplier of BLE-based RTLS safety and asset tracking solutions The TraknProtect staff safety solution is comprised of Bluetooth-enabled panic buttons for carrying on one's person and tags for locating physical assets. The panic buttons and tags are interoperable with Aruba's Wi-Fi 5 and Wi-Fi 6 access points. Used together, a joint TraknProtect and Aruba solution eliminates the need for separate staff safety radios and makes the most of existing capital investments in the wireless infrastructure.

When an activated ESD is detected, all access points within range report the device's presence and signal strength to the TraknProtect cloud-based platform. By correlating ESD signal strength with the location of the access points, the TraknProtect platform can accurately report the location of the activated ESD in real time, even if the individual is on the move.

Once the individual in duress has been located, the joint solution sends alerts to security with location updates via SMS, email, and mobile app. The real-time dashboard provides context as to the exact room/floor and tracks movement until the incident is resolved. An incident log is also updated for evidentiary purposes.

With the integrated Aruba and TraknProtect solution, institutions no longer need a separate overlay safety network. The Aruba infrastructure that's installed for IT services can do double-duty as a staff safety and asset tracking system. The solution provides peace of mind to site occupants, and helps comply with state and local legislation related to staff safety.

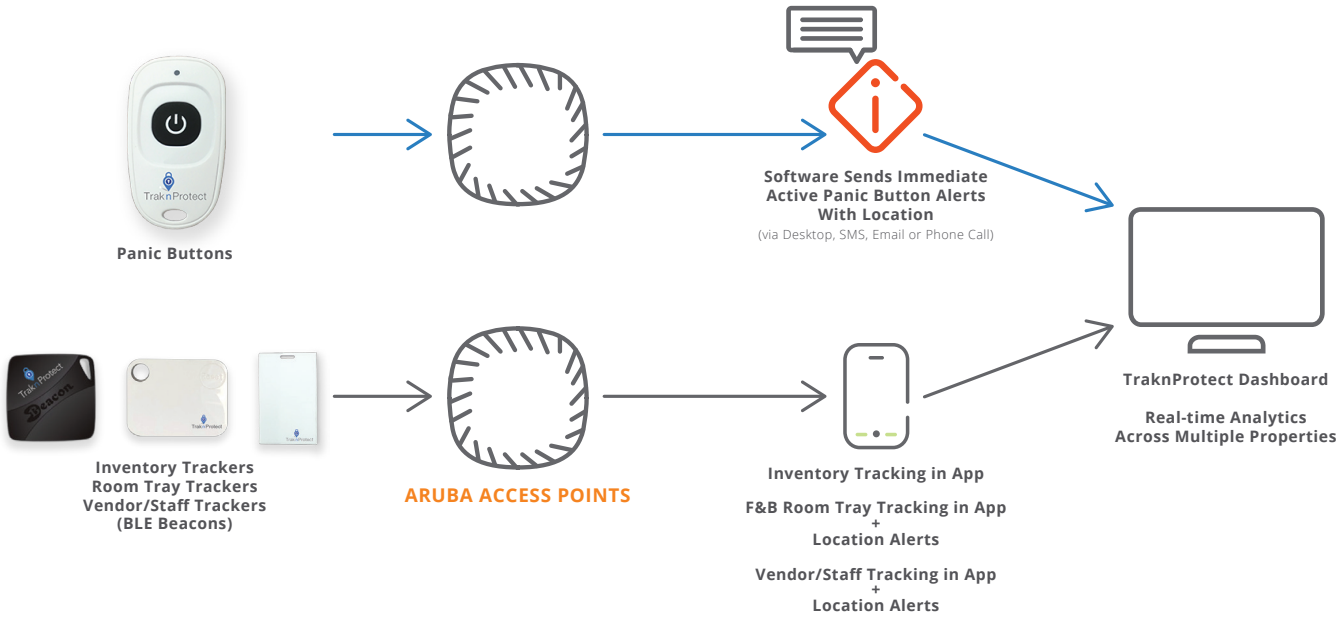


Figure 27: Aruba and TraknProtect Joint Solution Diagram

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 more sophisticated multi-sensor detectors to detect ammonia and other chemicals present in e-cigarette vapors. Multi-sensor devices have a much lower false alarm rate, and raise confidence that a vaping alert is valid.

Piera Systems

Piera Systems is a Mississauga, Canada-based developer of Intelligent Particle Sensors (IPS) that can detect particles as small as PM0.1 and count them with real time performance. IPS can be programmed to detect a wide range of particle sizes allowing for a single sensor to be used in a range of applications including vaping detection and air quality monitoring of CO2 and fire-related particulate matter. The IPS identifies the Particulate Matter and calculated its mass concentration, using machine learning to classify the components.

Piera Systems and Aruba have collaborated to enable any Aruba Wi-Fi 5 or Wi-Fi 6 access point equipped with a USB port, and running AOS 8.8 or later, to become a vaping and air quality monitoring station. The sensor can be easily retrofit to any site without pulling cabling or adding switch ports. The joint solution is ideal for enforcing no-vaping rules, and monitoring for other signs of danger.

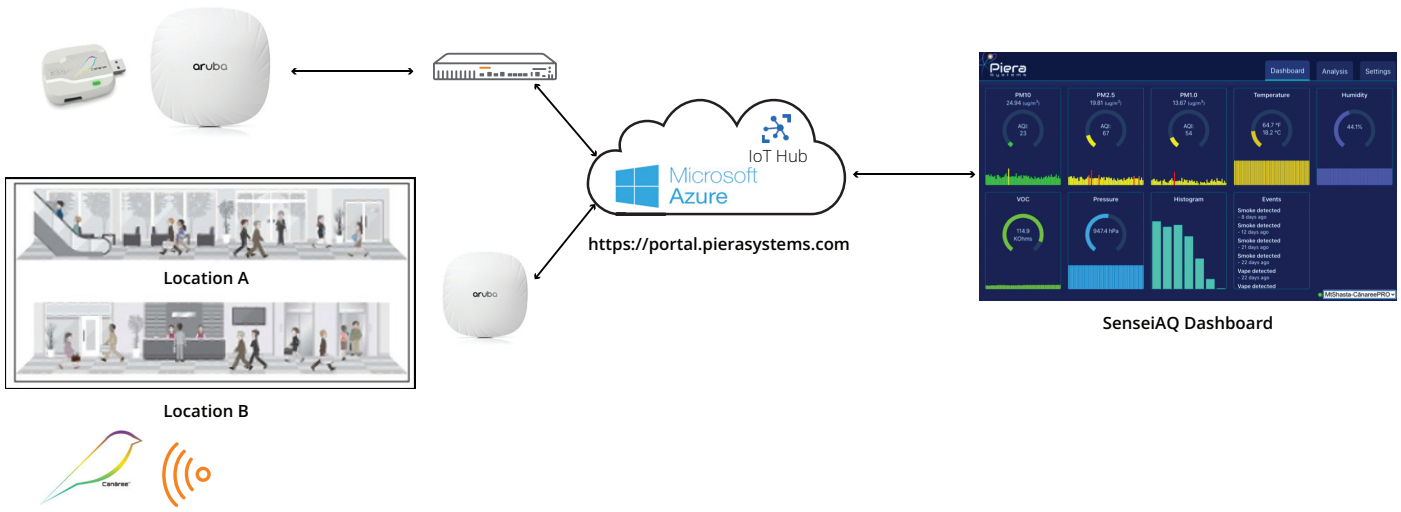


Figure 28: Piera Systems IPS USB Air Quality Sensor

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 29: HALO Smart Sensor Powered by Aruba Switches and Pass-Thru PoE Access Points

Powered by Aruba PoE pass-thru access points and PoE switches, HALO detects vaping and THC using dual-triggers to reduce false alarms. 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.

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 Aruba Wi-Fi 6 (802.11ax) or Wi-Fi 5 (802.11ac) 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 entrances, administrative offices, and publicly accessible spaces.

Figure 30: AmberBox Gunshot Detector

The joint solution works with Aruba Wi-Fi 5 and Wi-Fi 6 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.

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 response forces via the AmberBox cloud-based e911-certified platform, with additional notifications to facility/campus security and other responding parties. A conference call line is automatically established to share information and coordinate efficiently. Real-time shooter location tracking can be viewed through the Web or a mobile response platform.

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.

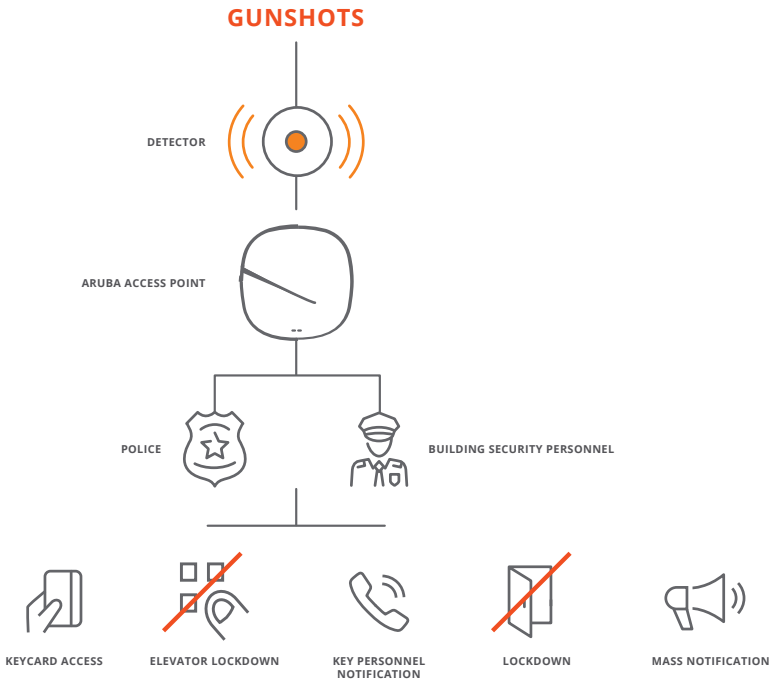


Figure 31: AmberBox Gunshot Detection and Notification System

CONNECTING AND PROTECTING REMOTE USERS AND FACILITIES

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 using automated IT and IoT on the journey to run institutions 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 institutions have people, call centers, and buildings spread across geographically-distributed areas. Connecting employees and machines, and the complexity of setting up and managing those connections, has been a challenge. Virtual private network (VPN) access is 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 locally.

Aruba addresses these issues by simplifying remote site access and connectivity to IoT devices. Aruba's VIA VPN Client application can be used to link laptops, tablets, and smart phones. VIA can also link standalone IoT controller running Linux, Windows, iOS, MacOS, or Android operating systems. VIA scans and selects the best Ethernet or broadband connection from the device to the enterprise network, offering a zero- touch experience by automatically connecting to an Aruba VPN concentrator controller on which it has been whitelisted.

Institutions that need very high security can run the VIA Suite B VPN client. The client is a hybrid IPsec/SSL VPN. 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.

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 device 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.

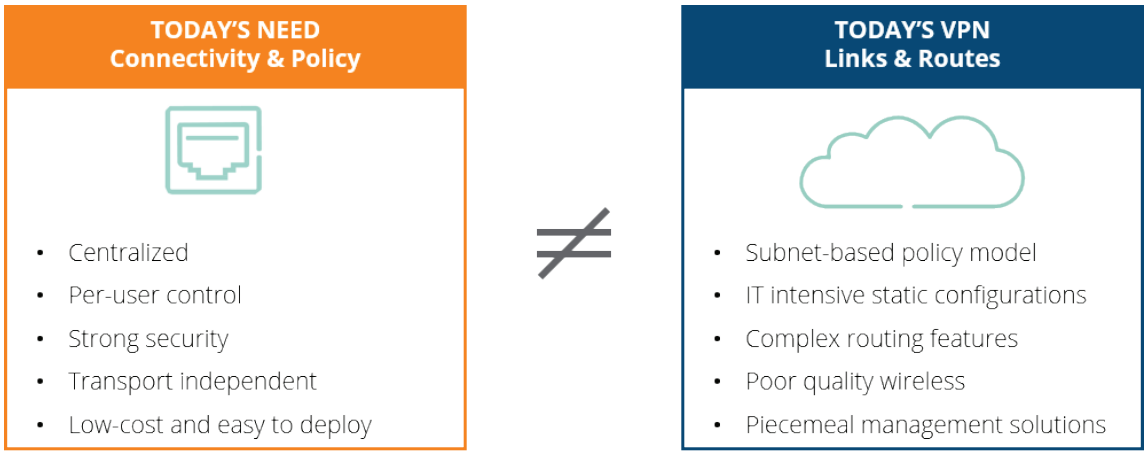


Figure 32: Limitations of Traditional VPNs

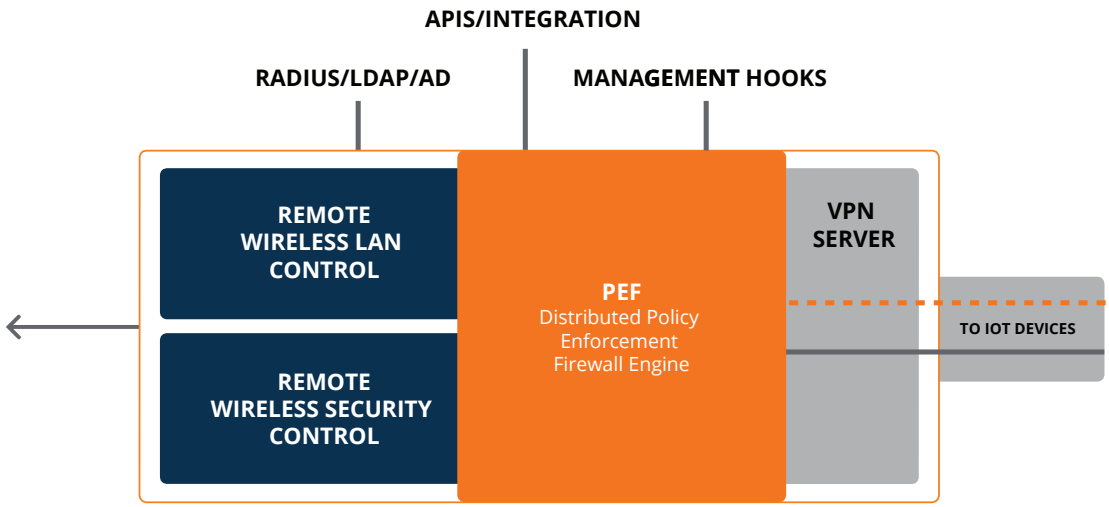


Figure 33: Aruba VPN Concentrator Controller

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, which 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.

Distributed call centers with associates working in small groups or at home – or when multiple IoT devices need to connect simultaneously - Aruba's 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.

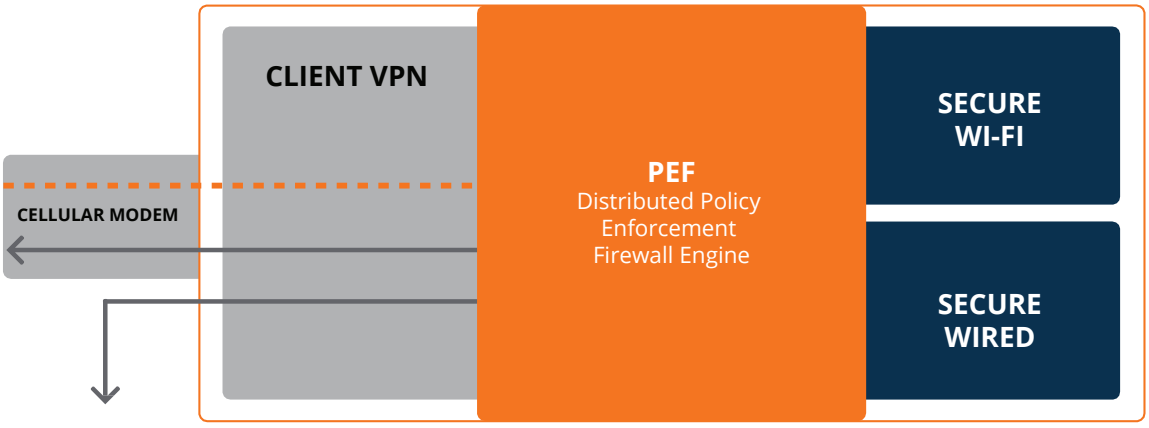


Figure 34: Aruba Remote Access Point

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.

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

An example remote IoT 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 is required.

For sites than need secure, high-bandwidth connectivity with back-up communication paths with service level agreements, a software defined wide-area network (SD-WAN) may be appropriate. 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 WAN solutions address these issues by providing a central point for configuring routing and access control policies, and a simple means of pushing those policies to remote sites. There is no on-premise management equipment to update or maintain. WAN management is orchestrated through the cloud, from which it's easy to distribute routes and build secure, scalable VPN tunnels on demand. The entry and exit points of traffic can be monitored regardless of uplink type, making it easy to manage WAN environments using public WAN connections.

To ensure uniform security, access policies dynamically follow IT and IoT client devices should they move between buildings. High availability active/active and active/standby modes deliver full redundancy for sites that need it

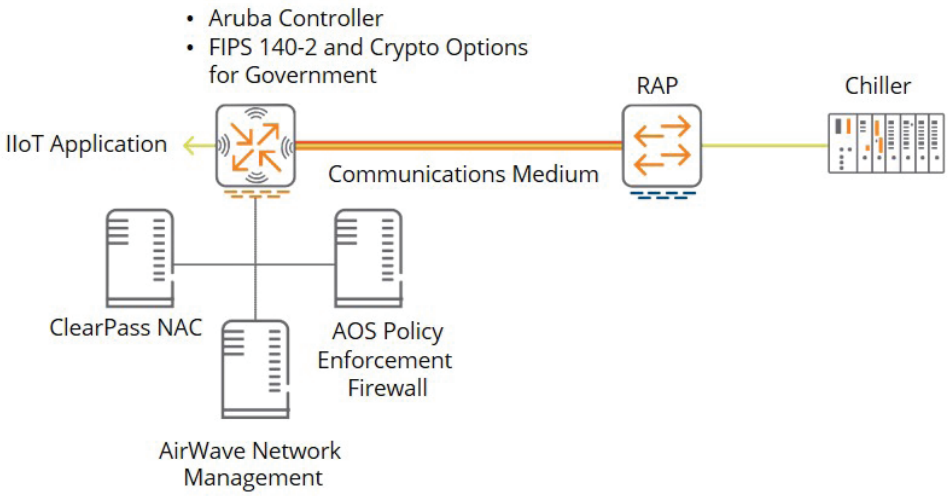


Figure 35: Remote Chiller Monitoring

For example, Aruba EdgeConnect SD-WAN appliances located at remote sites are designed to support multiple broadband, MPLS, or cellular links. A mesh of AES encrypted IPSec connections is built between pairs of devices using each available transport link (e.g., MPLS and the Internet), and these connections can be bonded together to enhance resiliency: a high error rate or complete failure of one link doesn't bring down the logical connection. The unbonded 4G/LTE link remains available to provide additional capacity when needed.

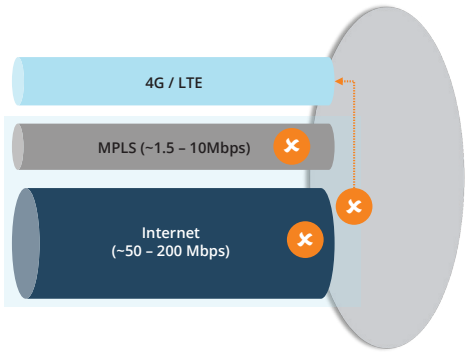


Figure 36: EdgeConnect SD-WAN Tunnel Bonding

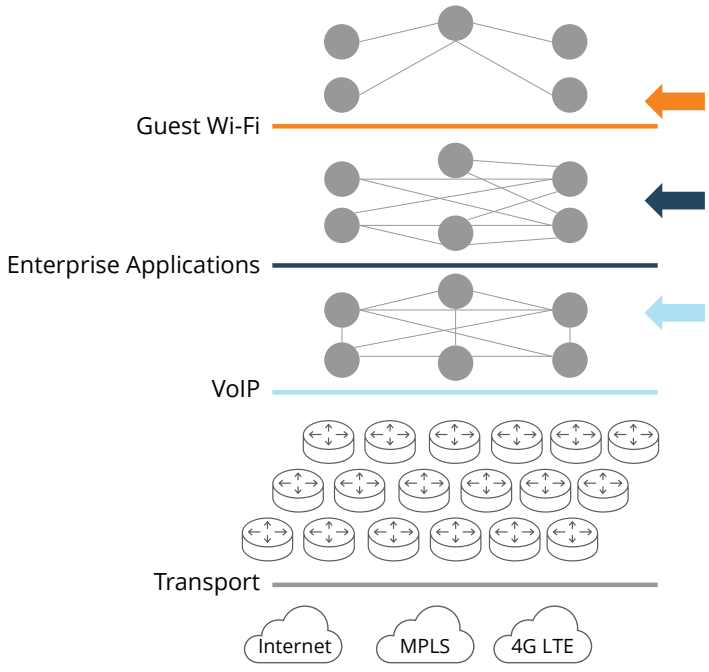
"Business Intent Overlays" map WAN traffic into the overlay network based on required availability, quality, throughput or efficiency on a per-application basis, and multiple overlays can run on top of a single physical infrastructure. Overlays separate network functions from the physical network to increase scale, function and flexibility.

Regardless of whether you need to connect a mobile classroom, monitor a remote facility IoT system, or connect a critical remote research lab with fault-tolerant WAN links, Aruba has you covered.

RAPIDLY DEPLOYABLE DISASTER RECOVERY NETWORKS

When a natural or manmade disaster strikes, networks are often brought down or destroyed. This can impact first responder communications, Internet access for staff and administrators, and access to local and cloud servers and applications. So when disaster strikes, it's imperative that networks be brought up as quickly as possible.

For many years Aruba has provided the U.S Air National Guard, U.S. Army National Guard, Federal Emergency Management Agency, and other government institutions with high security rapidly deployable networks for disaster recovery applications. While first responders have historically depended on private mobile radio and land mobile radio networks, in recent years these low bandwidth networks have given way to high availability LTE cellular networks that



Access Policy	Topology	Connection	QoS
Guest VLAN	Hub-Spoke	Internet	Min Cost
Data VLAN	Dual Hub and Spoke	MPLS + Internet	Max Availability
Voice VLAN	Full Mesh	MPLS + LTE	Max Quality

Figure 37: EdgeConnect SD-WAN Business Intent Overlay

include push-to-talk and video features to simplify their use and expand the services they provide. Combining LTE cellular with SD-WAN infrastructure provides a nearly universally available radio access network with a means to prioritize the delivery and quality of service of essential applications and multimedia communications.

Aruba's Silver Peak has teamed with BEC Technologies to deliver such an LTE-based SD-WAN solution for both ground mobile and ground fixed rapid deployment applications. Used in conjunction with Aruba switches and tactical or ruggedized Wi-Fi access points, the solution provides instant-on communications anywhere connectivity is needed.

The joint solution is inexpensive compared with satellite communication-based alternatives, and can be used in any EdgeConnect SD-WAN deployment. Aruba Orchestrator Business Intent Overlays prioritize LTE bandwidth usage based on application requirements.

BEC's advanced SX/AN antenna technology increases signal reception coverage, and can be cloud managed via the BECentral service. BEC's MX-200 4G/LTE Router connects to a WAN interface on the EdgeConnect appliance, enabling the antennas to be more optimally located than systems that integrate LTE into the SD-WAN appliance.

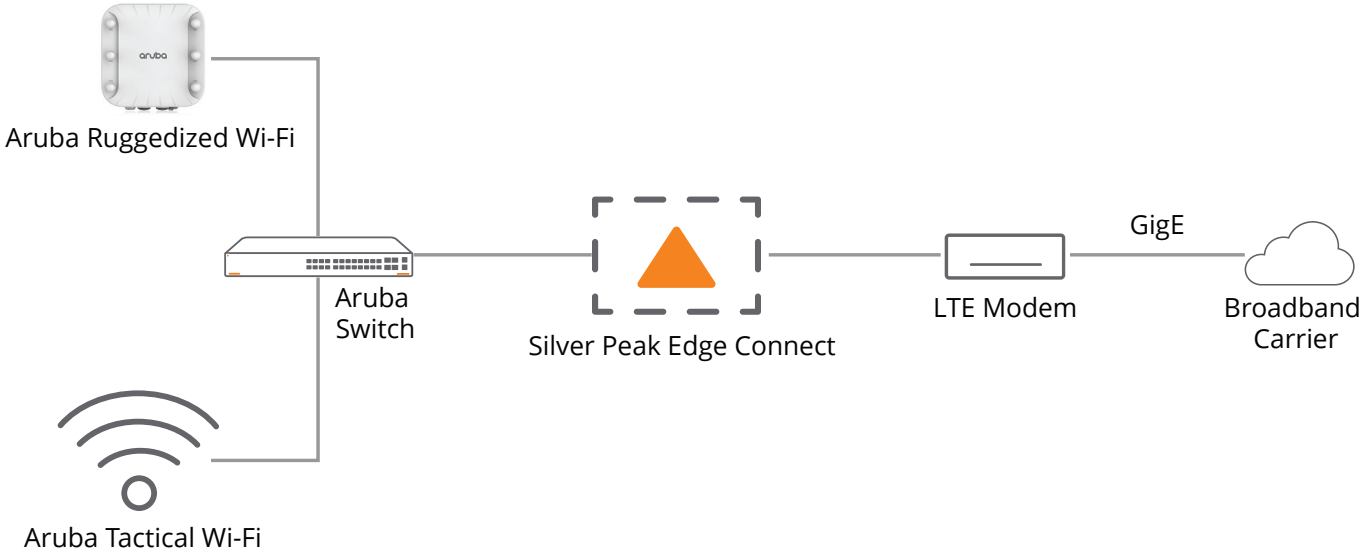


Figure 38: Rapid Deployment SD-WAN/LTE Solution

All the capabilities of the EdgeConnect solution are supported on LTE links, including packet-by-packet link bonding, dynamic path control, path conditioning and Boost WAN Optimization. EdgeConnect also incorporates sophisticated NAT traversal technology that elimi¬nates provisioning the LTE service with extra-cost static IP addresses.

Figure 39: Silver Peak EdgeConnect Appliance and BEC LTE Modem

Silver Peak and BEC work with a select group of wire¬less resellers that provide MX-200 hardware and in¬stallation services, post-sales support, LTE rate plans and consolidated billing for the LTE service. The MX-200 is certified with the major mobile operators, and for existing Silver Peak customers with pre-existing LTE ser¬vices, MX-200 commissioning is as simple as installing the SIM card.

When powered from a generator, or solar/battery power pack from ArubaEdge partner Solis Energy, a preconfigured system can set-up in minutes. And the components are compact enough to fit in fly-away cases. These features make the joint solution ideal for a broad range of fixed and mobile disaster recovery applications.

REDUNDANT INTRA-SITE WIRELESS VIDEO AND DATA LINKS

Outdoor surveillance video and remote gate access control systems often require outdoor data links. The choice between wired or wireless data links typically comes down to cost. If a wired network requires reaching across a parking lot or gully to surveillance cameras or an out building, it can easily take days of work to trench and repair asphalt or concrete. If there is hazardous buried material in the path, pipelines to cross, or the right of way is unavailable, the challenges continue to mount.

Wireless data links are easier to deploy than buried cables, however, the cost of a point-to-point high-speed microwave link can make it prohibitive for short-haul links under 400 meters. Less expensive links represent a single point of failure because they typically don't offer redundancy and can be impacted by nearby cellular networks. Additionally, in areas subject to high winds, even the slightest movement of the mounting brackets can throw an antenna out of alignment and require a service call.

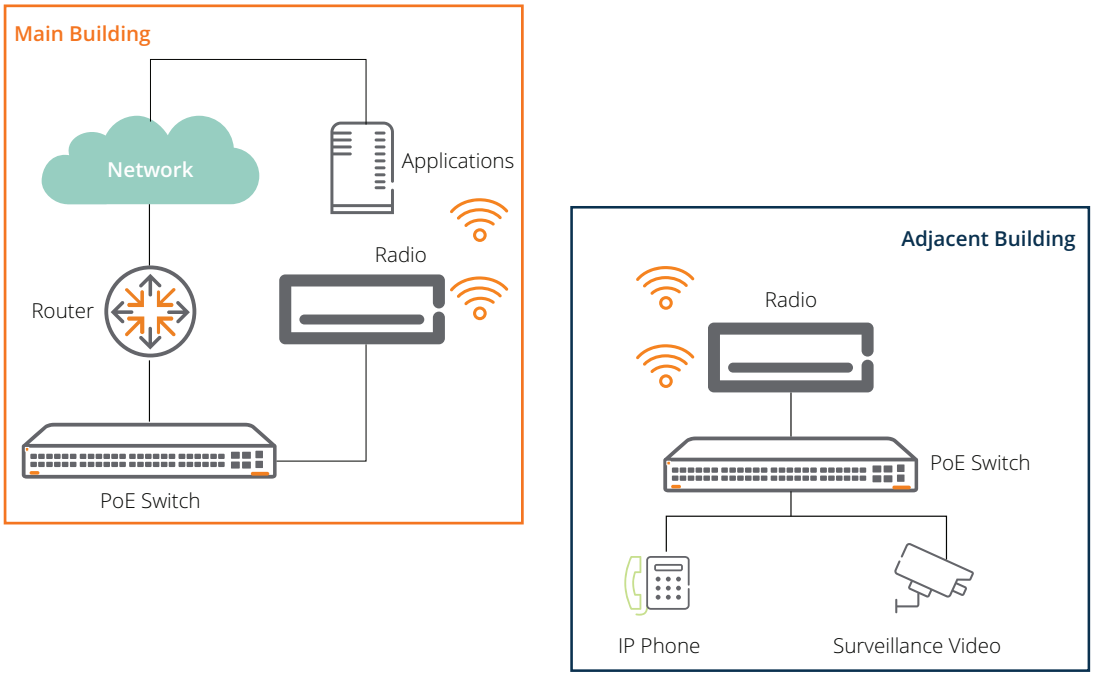


Figure 40: Point-To-Point Extension of a Plant Network to an Adjacent Building

Aruba's AP-387 is a high-speed, dual-radio, point-to-point link that addresses the shortcomings of today's point-to-point links. Incorporating a 60GHz millimeter wave radio with electrically steerable antenna array, the AP-387 provides automatic fallback to a 5GHz radio in the event that rain or snow attenuate the 60GHz signal. Redundant radios ensure that the link is always optimized, offering an aggregate peak rate of 3.37Gbps and a fallback rate of 867Mbps. Advanced cellular coexistence minimizes interference from cellular networks, distributed antenna systems, and commercial small cells, and femtocell equipment.

The auto-adjusting 60GHz antennas can dramatically reduce labor costs throughout the life of the site. The radios will intelligently link with alignment ±45 degrees azimuth, and ±17 degrees elevation; the 5GHz radio fixed sector antennas cover the same alignment zone. This eliminates the need for precision alignment, or high-cost skilled labor, during installation. Just point one radio in the general direction of the other, even if they are separated by as much as 20 stories of elevation, and the radios will link up.

Weighing just 1.2kg each, the radios can be commissioned by a single installer. The AP-387 includes an integrated BLE radio for hands-free set-up.

Running fiber or Ethernet cabling can take weeks of time for trenching, backfill, and restoration of surrounding areas. Depending on the construction environment, this work can cost $20,000 (€16,500)6 and must be repeated if a structure temporary or mobile. The AP-387 allows IT to deliver near-fiber speed and reliability without restricting where structures are placed or relocated.

Extending data links to other buildings and on-site locations shouldn't compromise reliability or your budget. The AP-387 can provide a redundant, point-to-point link up to 400 meters, and with an aggregate peak rate of 3.37Gbps it can support a very broad range of IoT, telephony, streaming video, and physical security applications.

MONITORING THE SWITCHING FABRIC TO DETECT SECURITY-IMPACTING IOT ISSUES

As facilities and campuses become more automated, the need to rapidly detect and correct IoT system errors grows in importance. Take, for example, a video surveillance system that uses networked cameras with on-board artificial intelligence to count people, detect tailgating thru access control portals, and alert when motion detection thresholds are crossed. These tasks require streaming data from cameras to application servers. In this machine-to-machine application, if the video stream starts going astray there is no human watching in real-time to detect image degradation on a monitor.

Figure 41: Aruba AP-387 High-Speed Outdoor Point-To-Point Link

An automated supervisory system is essential in this application for both operations optimization and preventive maintenance. Since the only common element among many machine-to-machine applications is the building's LAN that links everything together, it makes sense to look for an automated supervisory solution that runs within the switching fabric.

Figure 42: Aruba CX 8400 High-Availability Switch

Aruba's CX switch operating system uses a database-centric design and a programmatic interface to the entire database schema. All internal states, protocols, and statistics are expressed in the database, providing visibility into everything that happens on the network. With a database-driven operating system, any factor can be monitored and performance compared over time.

Aruba's Network Analytics Engine (NAE) uses Python scripts to define which switch resources to monitor and, optionally, rules for actions to take when certain conditions are true. CX is database-driven, and any factor can be monitored over time and acted upon. Python scripts typically target IIoT performance, security, and scale.

In the example above, the camera flows would be monitored with NAE scripts, and an automated notification sent to service personnel if degradation is detected in the data stream or switching fabric itself. Proactively addressing a video system problem prior to failure can prevent damage from undetected perimeter security breaches.

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.

criticalarc

CriticalArc is a global technology innovator and creator of the SafeZone® distributed command control solution. SafeZone provides real-time situational awareness to maximize response and minimize the impacts of an incident. Using a cloud service and dedicated first responder applications, SafeZone provides a real-time view of the location and status of all potential responders across multi-site institutions to optimize response to any situation that occurs.

The app can be used to summon help and receive updates about nearby incidents. Based on the user's location, the app can proactively notify them about the situation and guide them to safety.

CriticalArc and Aruba have partnered to integrate the Meridian SDK with the SafeZone app, using Aruba's access point and beacon based BLE location services to obtain more accurate indoor location information than is available with traditional GPS. Incidents can be isolated to a specific area on a floor, instead of just a building, allowing first responders to more quickly react to and resolve a dangerous situation. Since the solution uses Aruba infrastructure, it can reach everywhere in a building including lower floors and parking garages in which GPS signals are inaccessible.

The joint solution provides a 3D view of the environment, showing the location of occupants and responders in real-time. The situational awareness this provides is essential for determining appropriate responses and successfully guiding occupants to safe areas and muster points

All that is required for SafeZone support is a Meridian subscription and Aruba Beacons, standalone or embedded within Wi-Fi access points, throughout the facility. The SafeZone app leverages Meridian's maps and indoor location services, while the SafeZone cloud infrastructure can scale to sites and institutions of any size.

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

Figure 43: Meridian-Based CriticalArc Emergency Response Platform

those in danger from other occupants, or provide real-time situational awareness. Working together, SafeZone and Meridian location services fill this critical gap. 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;
- 3D site views to give first responders more details than they could obtain from just GPS;
- Exact location of safe and unsafe site occupants;
- Responders can send specific information to targeted recipients; and
- Incident recording ensures that all relevant data are saved for digital auditing and reporting.

CriticalArc and Aruba have created an event-triggered process that generates an immediate, personalized flow of information to those affected by an incident. Users can see their location relative to an incident, send and receive updates, and see perimeters and safe zones. If help is needed – anywhere, at any time - it's just one button-push away.

SECURING CONTROL NETWORKS THAT CAN'T PROTECT THEMSELVES

Physical plants typically incorporate Operational Technology (OT) like closed-loop sensors, actuators, programmable logic controllers, and human machine interfaces to run chillers, water treatment, power distribution, and other facilities-related infrastructure. Historically OT systems were air gapped from the rest of the facility systems because facilities teams wanted full responsibility for their operation. Unfortunately, cyber attacks on plants and equipment have crossed air gaps. That has turned a spotlight on the security of OT systems, and a pivot away from air gaps to active OT monitoring.

The objective of active OT monitoring is to provide uniform visibility and security policies across the OT control systems, programmable logic controllers, and related devices. Since OT systems use unique physical layers (PHY) and protocols, specialized tools are needed to monitor them and share data with the building's ClearPass IT security policy manager.

Inserting eyes and ears into an OT network requires tight alignment with the operating modes of OT infrastructure. In addition to understanding the OT physical layers and protocols, the monitoring system needs to have a library of devices types, know correct and abnormal operating modes, and do no harm in both normal operating and failure modes.

Aruba has partnered with best-in-class OT security companies to help bridge the IT and OT security divide. These partners couple deep knowledge of industrial control systems and machine learning-based threat analytics with a bi-directional link to ClearPass Policy Manager. The solution identifies OT devices, finds vulnerabilities, detects threats, and responds in a manner appropriate to the customer's needs, i.e., alert only, remediate thru ClearPass access control, or alert and remediate.

ClearPass Policy Manager uses device profiling, role-based access control, and real-time policy enforcement to identify, on-board, and control devices. OT security partners enhance these services by discovering OT devices, flagging risks and abnormalities, and enforcing security postures.

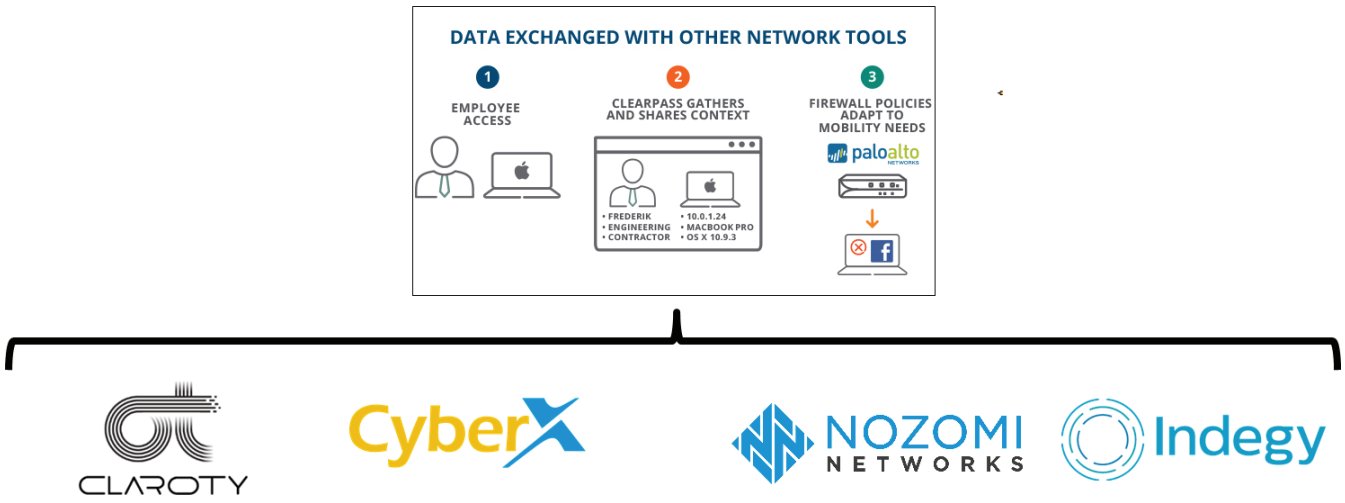


Figure 44: OT Security System Integration with Aruba ClearPass

The joint solution allows IT administrators to centrally manage connected devices and enforce policies governing what those devices can do: OT retains control of their devices, IT obtains uniform visibility and security policies across the entire institution, and the end user avoids costly downtime, safety incidents, and loss of intellectual property.

When an OT device connects to the network it is discovered by the OT security system, which synchronizes with ClearPass Policy Manager to give it a comprehensive view of all IT and OT devices. The supplied context is then used by Aruba to dynamically segment OT communications – a foundational element of a zero trust framework – ensuring that devices only communicate with appropriate applications.

These features enable OT managers to:

- Gain insight into network devices across IT and OT networks;
- Utilize contextual data to deploy seamless edge security; and
- Ensure that only devices compliant with the latest updates are allowed on the network.

OT security partners currently include Claroty, Microsoft CyberX, Nozomi, and Tenable Indegy. Additional partner integrations are anticipated in the near future.

SUMMARY

The availability of IoT data and relevant context enables government institutions facilities to adapt to the situational environment and occupants' needs. The richer the set of available data and context, the more adaptive the facility can become.

Working in concert with key technology partners, Aruba's unified infrastructure, zero-trust security, and AI powered solutions enable cognizant fixed and mobile facilities that can boost citizen enablement, efficiency, productivity, reliability, safety, and security.

Please contact us for more information on how we can help your 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 Jones, Lang, LaSalle, A surprising way to cut real estate costs, https://www.us.jll.com/en/trends-and-insights/workplace/a-surprising-way-to-cut-real-estate-costs, 16 September 2016

6 https://www.modular.org/documents/Relocatable_Classroom_Fact-Sheet.pdf

aruba
a Hewlett Packard Enterprise company

WP_Designinghyper-awarecivgovtfacilities_SK_021221 a00110316enw

Contact Us **Share**