WHITE PAPER

aruba
a Hewlett Packard Enterprise company

Designing hyper-aware smart buildings

Secure infrastructure and partner solutions for education, enterprise, and government applications

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 business applications that analyze, mine, share, and respond to those data. In smart building applications, the machines and applications are tailored to optimizing human activity monitoring, organizational redesign, augmented reality, human productivity, and health and safety

By securely interfacing IoT devices, and generating contextual information, Aruba's networks enable building control and business applications 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 - enable facility owners to successfully deploy and exploit IoT solutions. The richer the set of available data and context, the greater the opportunities to boost efficiency, productivity, profitability, reliability, safety, and security.

Solutions from Aruba and its technology partners are applicable across a broad range of smart building enterprise, education, and government markets. Use cases and partners discussed in this white paper include:

- Human Activity Monitoring
  - Physical Distance Monitoring And Contact Tracing (AiRISTA Flow, AisleLabs, CohuHD, CXapp, Kiana, Patrocinium, SkyFii)
- Human Productivity Organizational Redesign
  - Space Utilization Analytics (Lone Rooftop)
- Augmented Reality
  - Migrating From Break/Fix to Predictive Maintenance (ABB)
  - Building Control And Digital Twin Enablement (EnOcean and Microsoft)
- Human Productivity Optimization
  - Automating Guest Access To Enhance Staff Efficiency (Aruba, Envoy)
  - Securely Sharing Smart Building Wireless Networks Without Losing Control (Aruba MultiZone)
  - Seamless 5G To Wi-Fi Roaming Without Distributed Antenna Systems (AirPass)
  - Reducing Mean Time To Repair With Real-Time Location Services (Aruba APs and Meridian)
- Building Security
  - Vaping And Air Quality Monitoring (IP video)
  - Gunshot Detection (AmberBox)
  - Connecting And Protecting Remote Buildings (VIA, RAPs, SD-Branch)
  - 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 Python scripting)
  - Context-Aware, Real-Time Integrated Emergency Response And Notification (Meridian and Patrocinium)
  - Securing Control Networks That Can't Protect Themselves (Claroty, Microsoft CyberX, Nozomi, Tenable Indegy)

INTRODUCTION

What is a smart building, and why is the Internet of Things (IoT) relevant to it? A smart building 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 building, 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 building's data network, i.e., identity, location, and applications in use. The combination of data and context enables smart buildings to become cognizant of, and responsive to, the occupants and their environment. The richer the set of data and context, the more adaptive the building can become. Some buildings have only limited cognizance, while others are fully instrumented and hyper-aware.

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

Building 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 building devices are a tower of babel, teeming with systems that operate in parallel but can communicate only thru 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 building systems remain isolated and unable to share edge data.

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

The 'Achilles heel' of smart building 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 disruption to on-going operations. Many new IoT devices also lack sound cybersecurity features. For this reason many CISOs will not permit either building 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.

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;

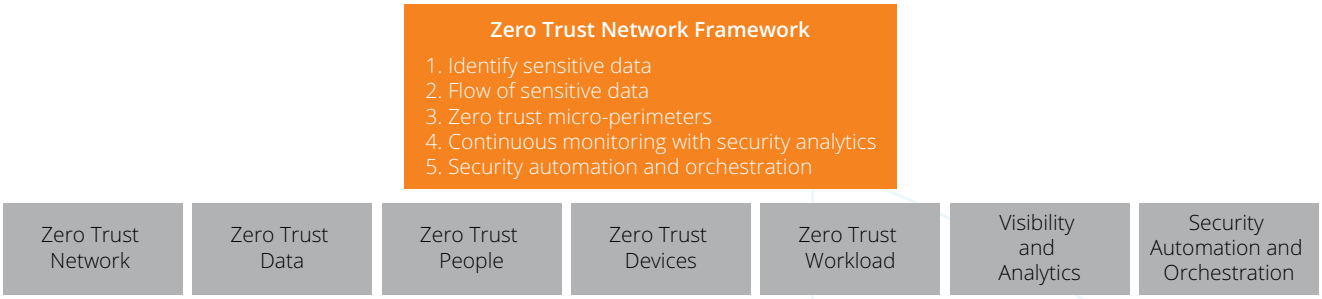

Figure 1: Zero Trust Framework

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

Legacy IoT devices can be identified as known or unknown upon connecting to the network using their MAC address in an external or internal database. The profiling data should flag if a device changes its mode of operation or masquerades as another IoT device – a common issue with MAC-based authentication - and then automatically modify the device's authorization privileges. For example, if a 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 building control market is very conservative, and the rate of technological change has been significantly slower than the consumer product industry. As a consequence, today's smart building solutions require expertise outside the realm of traditional building automation companies. Unified communications, cloud-based productivity tools, and augmented reality expertise are needed for activity monitoring, intelligent spaces, and servicing complex

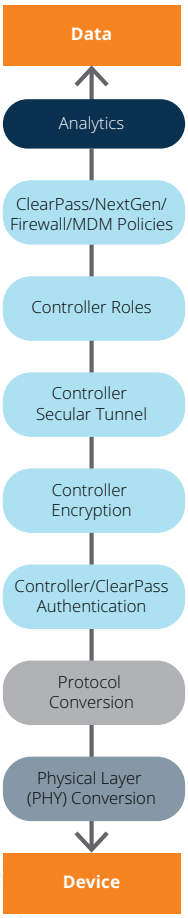

Figure 2: IIoT Protection Mechanisms

systems, respectively. Cybersecurity has to underpin all smart building systems, and is not a core skill for most smart building 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 companies monetize the data they collect and yet another province of IT.

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 strategic business goals of cognitively aware buildings to be realized without incurring unacceptable risk. Let's now examine how to align a company's strategic goals with the implementation of cognitively aware buildings.

BUSINESS TRANSFORMATION ENABLED

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

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

Originally intended to describe an ecosystem of interconnected machines, the phrase "Internet of Things" has been taken literally to mean connecting all devices to the Internet. The overarching objective of IoT is not to connect every device to the Internet. IoT devices are vessels for context and data, and the objective is to tap only relevant information and devices.

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

These business moments must be carefully orchestrated, even if they appear spontaneous to the building occupant or owner. 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.

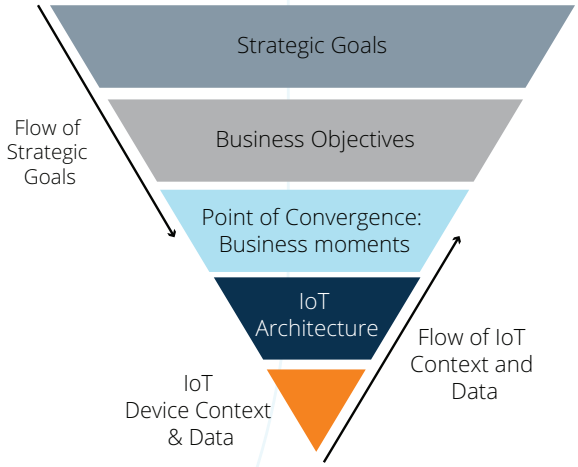

Figure 3: IoT Strategic Hierarchy

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

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

Where does one start this process? The first order of business in any smart building project is to identify the customer's strategic goals and the associated business objectives that must be met. Those will inform the business moments for which the IoT architecture needs to extract relevant IoT data and context. Is the objective to reduce real estate footprint by more efficiently using space and managing people? Enhance personal safety with social distancing and thermographic monitoring? Enhance building 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.

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

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

SMART BUILDING MARKET

According to McKinsey4 the total economic impact of IoT in smart buildings in 2025 will be $70B-$140B. The top areas they identified include human productivity monitoring ($48B-$115B), energy monitoring ($12B-$21B), and building security ($3B-$6B):

- Human activity monitoring is expected to increase productivity by 5%;
- Human productivity organizational redesign is expected to yield 3-4% productivity gains;
- Augmented reality is expected to yield 10% productivity gains;
- Energy monitoring should reduce costs by 20%; and
- Building security should yield a 20-50% reduction in labor costs.

Commercial real estate services company Jones Lang LaSalle 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 makes clear that the biggest financial benefits can be obtained by making people more productive and efficient. Pivoting toward human productivity optimization also improves space efficiency, which in turn reduces both real estate footprint and energy costs.

Historically smart building initiatives focused on energy efficiency because this was – and remains – ones 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 workplaces. IoT can change the way in which machines and humans interact to make people more productive. 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 building 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., identifying the location of an active shooter? Or is an optimized system-level solution required, i.e., migrating from break/fix to site-wide predictive maintenance?

In all cases an extensible platform will be required because smart building requirements change over time; a platform allows customers to build a broad range of services today and into the future. That platform is necessary but is by itself insufficient to build a solution since no one vendor makes a universal set of end customer solutions. Technology partners are an essential component of any use case. Aruba has curated a world-class cohort of infrastructure, security, and location technology partners, the solutions of which have been validated interoperable with Aruba infrastructure. Common use cases that leverage solutions from Aruba and its technology partners to create cognizant smart buildings are presented below.

PHYSICAL DISTANCE MONITORING AND CONTACT TRACING

Workplace safety extends beyond physical and environmental hazards. Today, physical distance monitoring and contact tracing are essential for back-to-work and stay-healthy-at-work initiatives. Whether mandated by local regulations or company policies, maintaining safe distances

from other workers and infection control tracing are top of mind for facilities teams. While there is no single physical distance monitoring and contact tracing application that will work for all enterprises, real-time location services and identity stores have an essential role to play in every workplace infection control solution.

Aruba has teamed with multiple technology partners to deliver a broad range of 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 company issued devices;
- Presence detection systems that pick-up Wi-Fi signals from personally-owned or company issued devices, but do not require an application; and
- Thermographic and facial recognition systems that monitor the temperature of individuals' heads, and can process dozens of people simultaneously.

AiRISTA FLOW

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

Fig 4: AiRISTA Flow BLE Proximity Tags With Haptic Feedback

Aislelabs

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

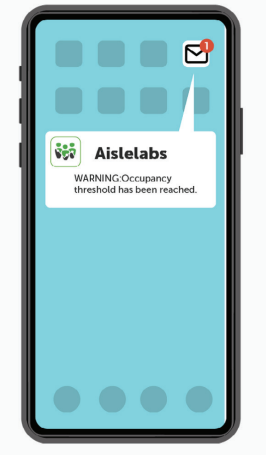

Fig 5: AisleLabs COVID-19 Social Distancing Solution

COHU | HD COSTAR

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

Figure 6: CohuHD Non-Contact Thermographic And Facial Recognition Camera

The CxApp Touchless Application leverages Meridian BLE Beacons strategically placed around the workplace, and the Meridian cloud service for location data. The mobile app sends notifications based on crowded times, vacant times, and total employees 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.

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

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

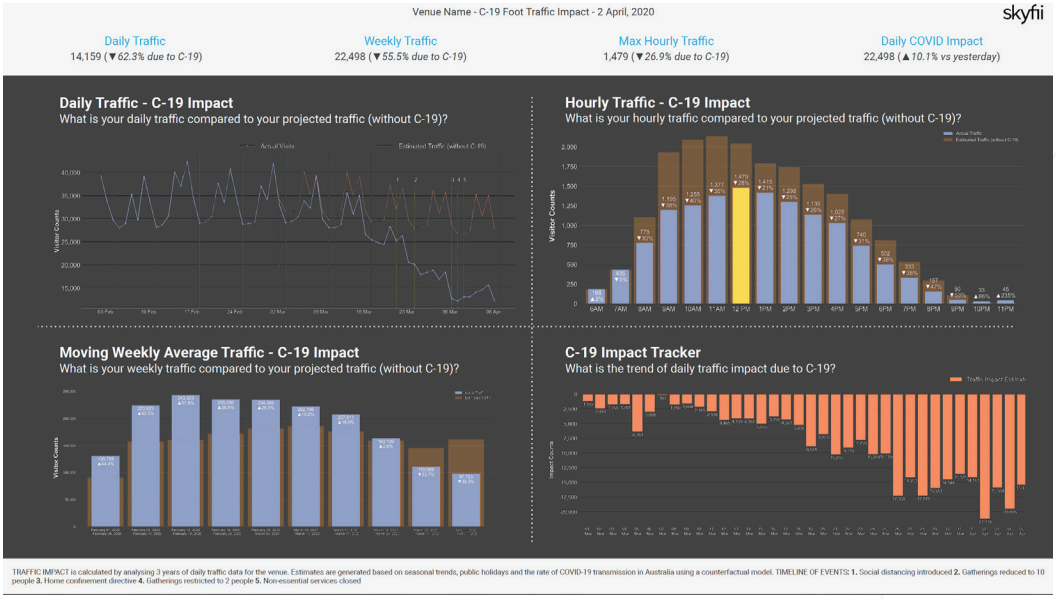

Figure 7: SkyFii OccupancyNow Dashboard

SPACE UTILIZATION ANALYTICS

We commonly think of Wi-Fi networks as access ramps onto corporate networks and the Internet, but Aruba access points are also IoT platforms that generate contextual information business-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 corporate cafeteria usage based on building occupancy can minimize food wastage.

Real-time analytics can also boost productivity. Statistics show that 40% of flex space workers 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-

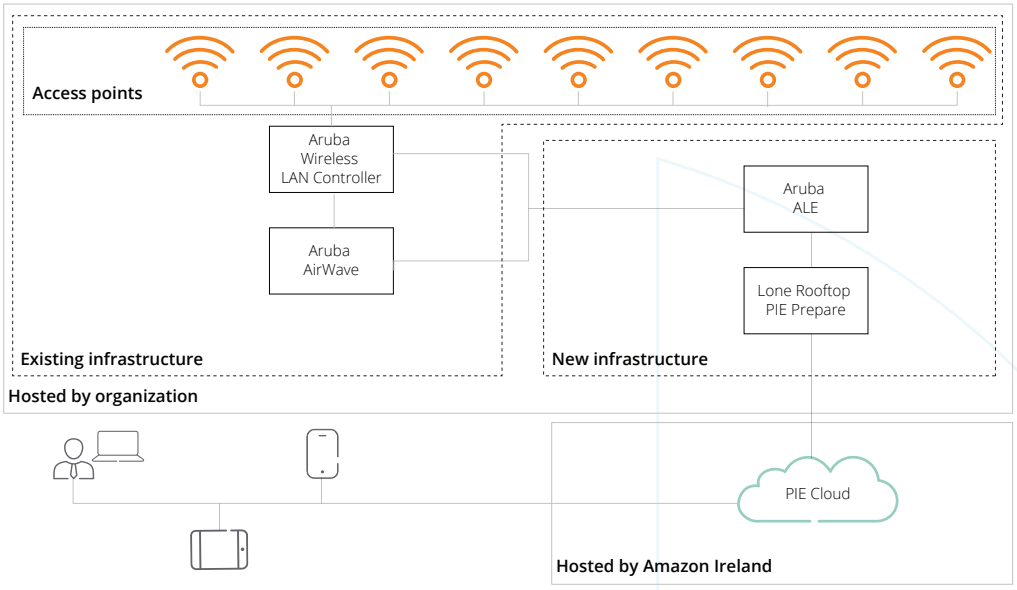

Figure 8: Aruba and Lone Rooftop Integration Overview

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.

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 building, allowing owners and tenants to 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 PREDICTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep buildings 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 in a building to 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 predictive maintenance, a digital transformation that reduces downtime, enhances asset utilization, and optimizes scheduling of field engineers. All of which ultimately boost efficiency and profitability.

ABB and Aruba have partnered to enable Aruba Wi-Fi 5 and Wi-Fi 6 multi-radio access points to securely collect and forward ABB 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.

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.

BUILDING CONTROL AND DIGITAL TWIN ENABLEMENT

Situational awareness is essential to building a cognitively aware building. IoT devices are the eyes and ears of a software defined building, and are given voice by the secure connectivity infrastructure through which they talk with smart building applications. The better instrumented the building, the more informed the insights that can be made across time and space, including projections of future occupant and system behavior. Energy monitoring cuts

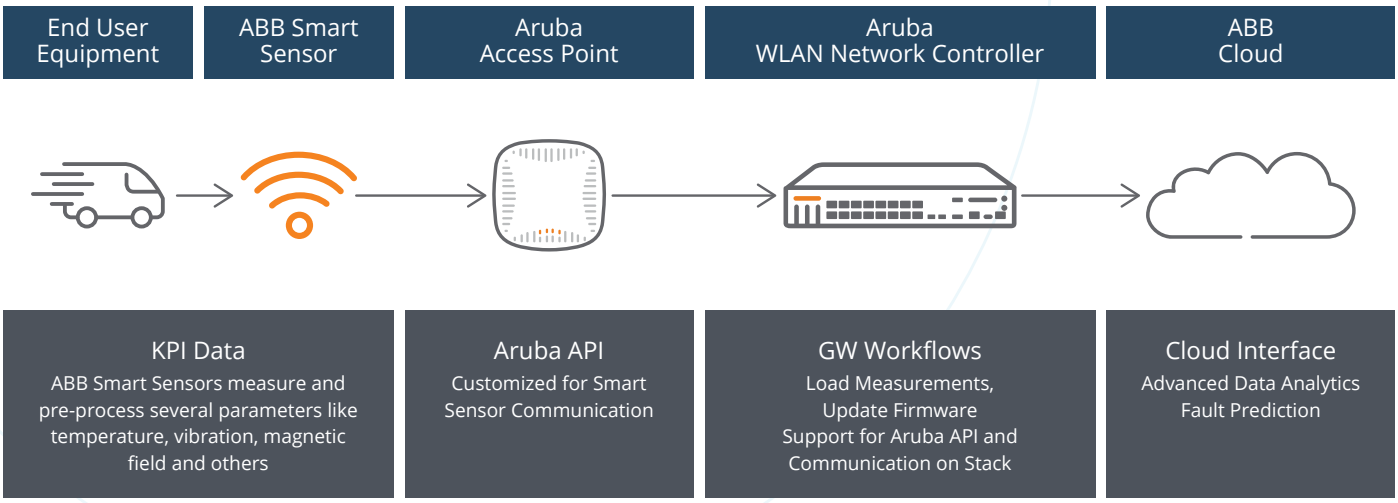

Figure 9: Aruba and ABB Integration Overview

across many building sub-systems, encompassing a wide variety of IoT telemetry 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 building devices and systems. By creating real-time simulation models in the digital world that change and learn in lock-step with the building, 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 building 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 building 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 building 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 building 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 build 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.

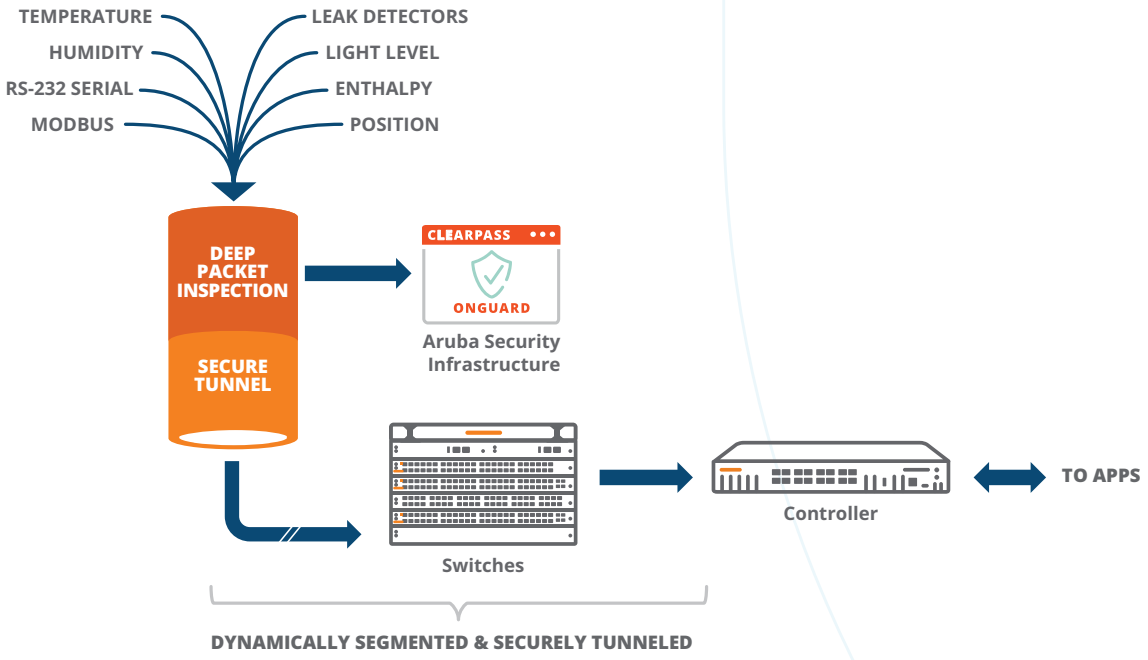

Figure 10: Aruba Access Points Are IoT Platforms For EnOcean Device Data

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 smart building monitoring application can be accommodated. The joint solution can be retrofitted to existing Aruba deployments, extending the value of sunk capital investments.

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

Customers that want digital twin modeling and telemetry monitoring can simply point Aruba's Web socket connection to Microsoft's Azure IoT Hub – on-premise or in the Azure cloud. Azure IoT Hub will extract the telemetry data from the protobuf stream, and make it available to 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.

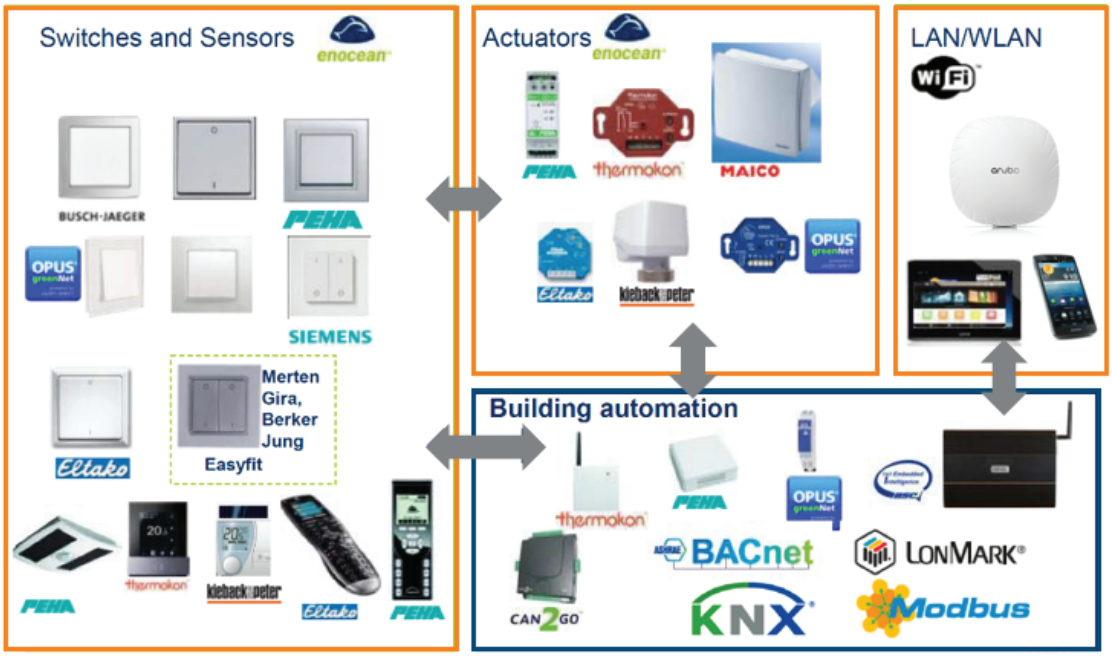

Figure 11: EnOcean Ecosystem

AUTOMATING GUEST ACCESS TO ENHANCE STAFF EFFICIENCY

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

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

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

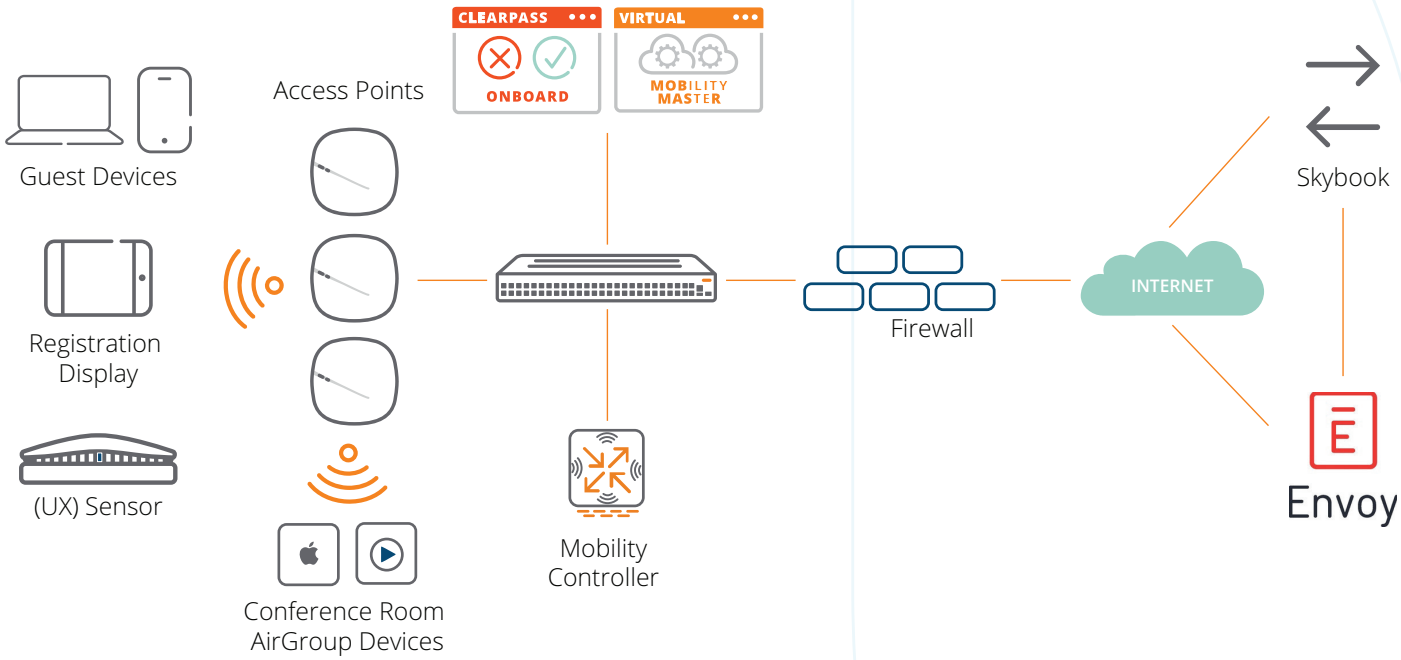

Figure 12: Automated Guest Access Solution To Enhance Staff Efficiency

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

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

Envoy

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

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

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

SECURELY SHARING SMART BUILDING WIRELESS NETWORKS WITHOUT LOSING CONTROL

Smart building wireless network access is typically tightly controlled out of concern that critical services and devices, such as Wi-Fi calling, could be negatively impacted by wireless users. However, growing demands for mobile device wireless access to enhance worker efficiency, productivity and safety increase pressure to open up wireless networks and avoid the cost and RF interference of parallel networks. Both IT and facilities groups are struggling to find a mutually acceptable solution.

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

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

The multi-tenancy design of MultiZone is ideal for smart building applications. Separate Data Zones can be allocated to the groups managing, say, building controls, machine-as-a-service, corporate services, contractors, and auditors, Each group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services. Defense-related enterprises 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.

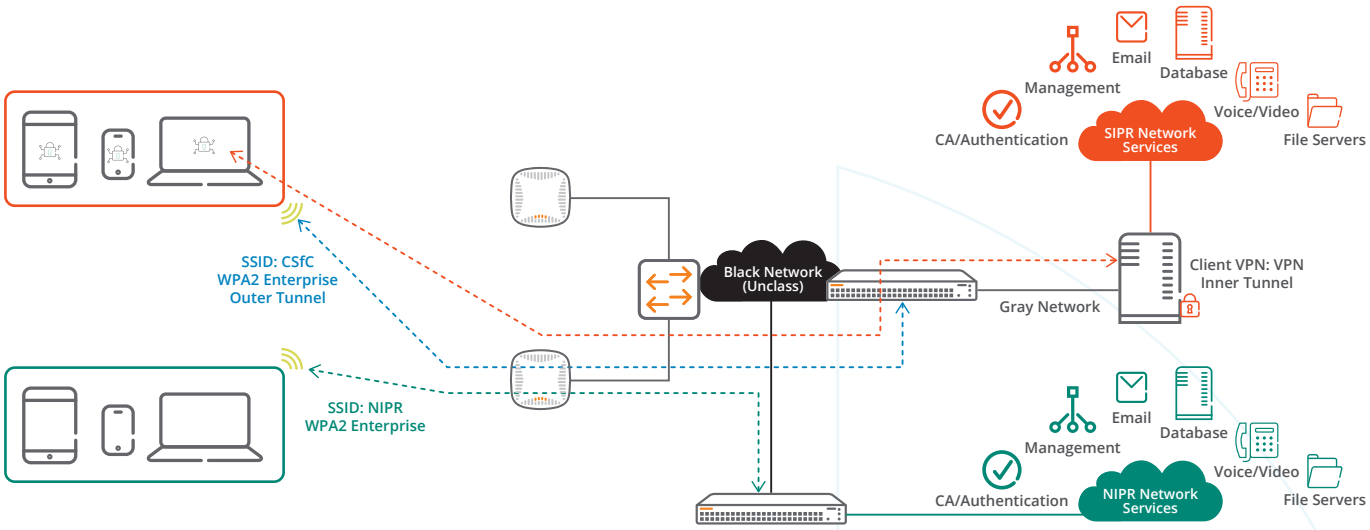

Figure 13: Aruba Multizone Solution

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 low-emission glass, energy-efficient construction materials, and evolving building codes have made indoor wireless coverage from outdoor cellular networks a recurring challenge. This results in inconsistent experiences for mobile users and devices as they roam in and out of buildings. These problems are compounded with high-speed 5G, which operates at higher frequencies that do not penetrate indoors as far as 3G or 4G cellular.

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

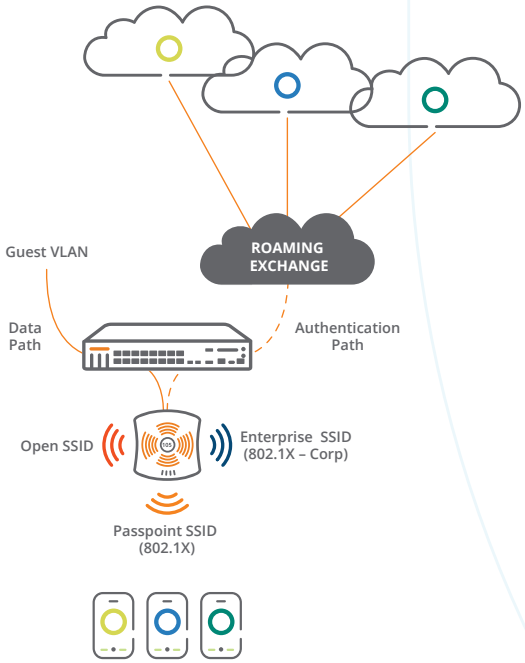

Figure 14: Aruba AirPass System Architecture

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

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

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

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

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

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

REDUCING MEAN TIME TO REPAIR WITH REAL-TIME LOCATION SERVICES

Many building 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 real estate utilization, occupant time and motion optimization, 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 15: 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 work or roam. And they can track capital assets so they can be quickly located and repaired.

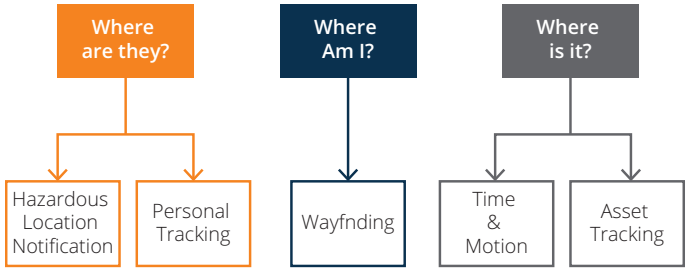

Figure 16: Aruba Location Services and Target Applications

Large buildings 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 business-relevant 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. Standalone battery- and USB-powered beacons are also available.

Fig 17: AP-530 Wi-Fi 6 Access Point With 802.11ax, BLE, And 802.15.4 Radios

Fig 18: AP-375EX Access Point For Hazardous Areas Like Propane Storage And Fuel Refilling

Typical smart building wayfinding applications include:

- Guiding employees to meetings, points of interest, and muster stations;
- Navigating service personnel to machines in need to repair; and
- Providing visitors with self-service navigation around large facilities.

Self-guided wayfinding directs users to a point of interest, and offers a simple way to pinpoint their current location, search for points of interest, and access turn-by-turn directions, inside or outside. 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 building facilities applications. Imagine that the bearing on a motor drive starts 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 Finance Department when work commences - and then guides the engineer using turn-by-turn navigation to the failing motor drive.

Fig 19: Meridian Turn-By-Turn Wayfinding

As the engineer approaches the machine another geofence is triggered, recalling the service record for that drive 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 sites, 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.

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. In particular, schools worldwide have been revising rules to ban vaping on school grounds. The hospitality and transportation industries, in particular, have forbidden vaping in hotel rooms, airplanes, and trains.

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

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

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

Figure 20: HALO Smart Sensor Powered by Aruba Switches and Pass-Thru PoE Access Points

IP Video and Aruba have collaborated to enable plants to combat vaping through automated sensing and response. Powered by Aruba PoE pass-thru access points and PoE switches, HALO detects vaping and THC using dual-triggers to reduce false alarms. HALO incorporates multiple sensors so it can serve additional roles, too. On-board sensors can detect particulates, carbon dioxide, carbon monoxide, volatile organic compounds (VOCs), oxidizing agents, and ethanol. These features make HALO well suited to air quality monitoring applications. Audio monitoring enables HALO to detect gunshots and cries for help, while a voice synthesizer lets HALO respond to occupants with context-appropriate messages, i.e., in response to a verbal request for “help” HALO can respond that “help is on the way.” Voice detection and response are processed locally, not in the cloud, to ensure that privacy is maintained.

The joint solution is ideal for enforcing no-vaping rules, and monitoring for other signs of danger.

GUNSHOT DETECTION

One of the most dangerous situations faced by first responders is a live shooter inside a plant. 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 dedicated wireless networks, like LoRa, present cybersecurity risks by bypassing standard IT security monitoring tools. There are also maintenance issues associated with battery replacement.

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

AMBERBOX Gunshot Detection

AmberBox, a leading provider of next-generation gunshot detectors, and Aruba have partnered to ensure that first responders can be reliably notified when an active incident is in process. Applications include both plants and corporate offices

Figure 21: Amberbox Gunshot Detector

The joint solution works with Aruba Wi-Fi 6 (802.11ax) or Wi-Fi 5 (802.11ac) access points already deployed on-site, avoiding the need for a separate overlay network. AmberBox sensors interface with the access points' USB ports, which provide both power and data access. Sensor spacing matches 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 law enforcement via the AmberBox cloud-based e911-certified platform, with additional notifications to plants security or other responding parties. A conference call line is automatically established to share information and coordinate efficiently.

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

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

Key benefits of a jointly deployed solution include:

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

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

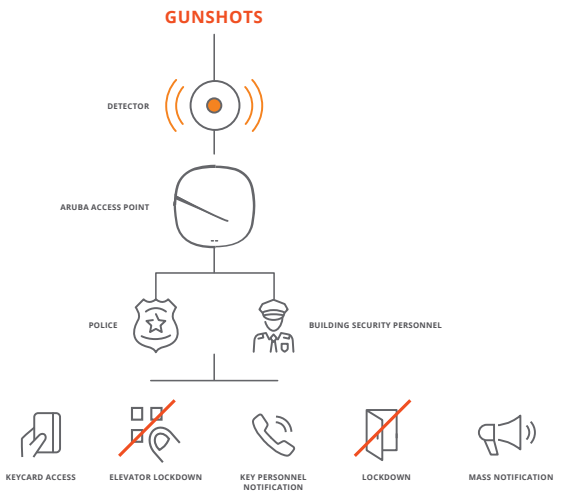

Figure 22: AmberBox Gunshot Detection And Notification System

CONNECTING AND PROTECTING REMOTE BUILDINGS

Industry analysts have long opined that the rise of smart machines, cognitive technologies, and algorithmic business models could render obsolete the competitive advantage of offshoring. Hyper-automation, it is argued, will be more influential than labor arbitrage in driving profitability and enhancing productivity. Smart machines will accomplish this by classifying content, finding patterns, and extrapolating generalizations from those patterns.

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

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

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

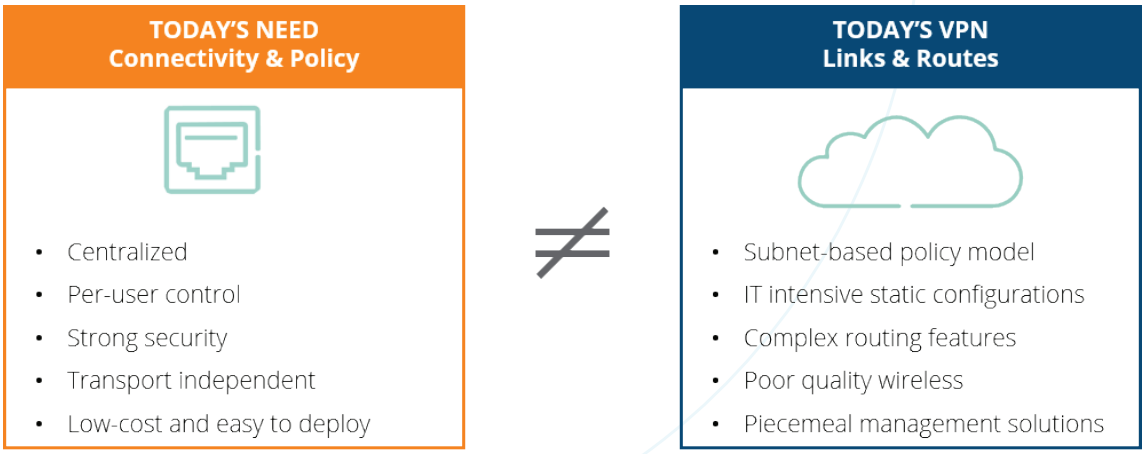

Figure 23: Limitations Of Traditional VPNs

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

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

High security government or defense-related buildings 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.

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

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.

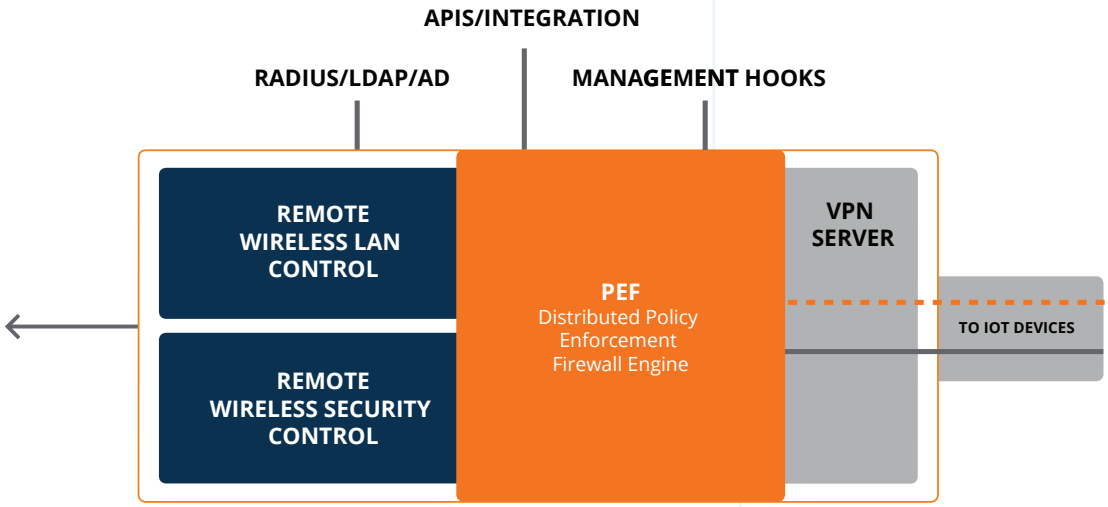

Figure 24: Aruba VPN Concentrator Controller

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

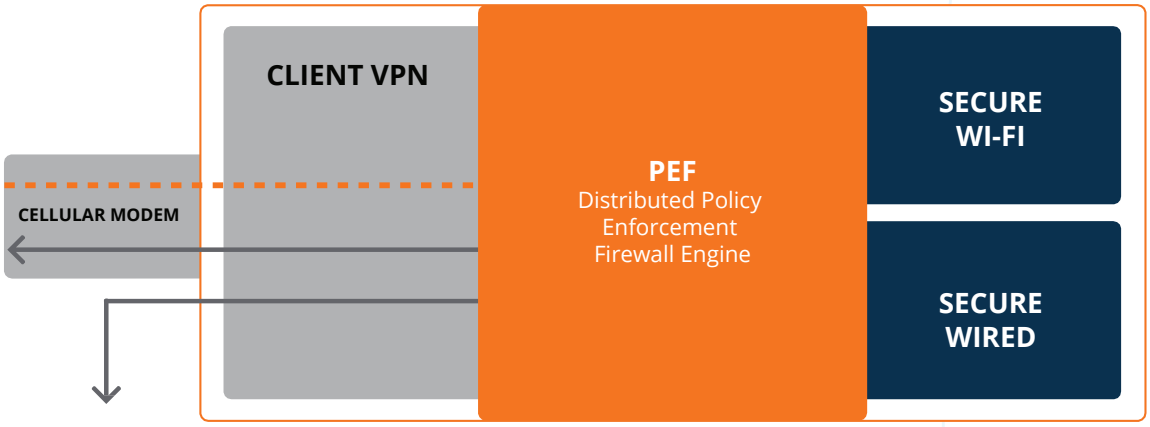

Figure 25: Aruba Remote Access Point

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

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

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

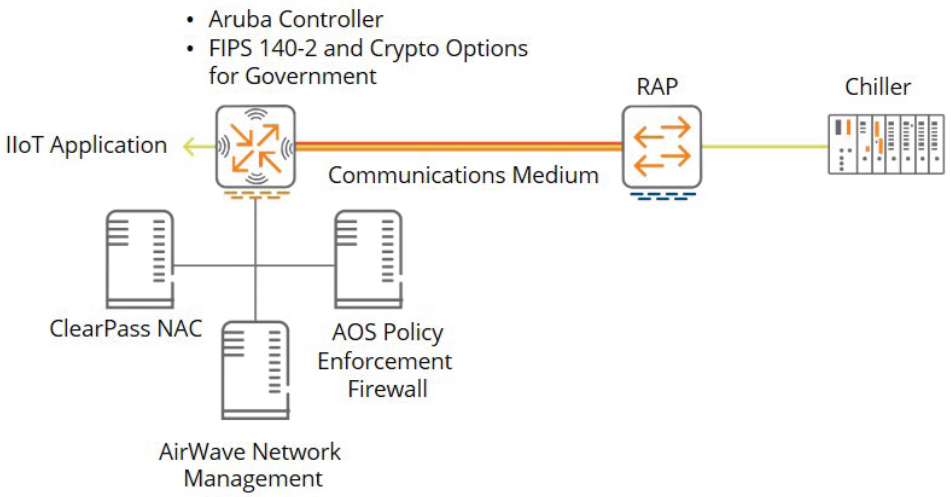

Figure 26: Remote Chiller Monitoring

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

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

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

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

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

Regardless of whether you need to monitor a single remote IoT device, and small buildings with multiple IoT devices, or a critical site requiring fault-tolerant WAN links, Aruba has you covered.

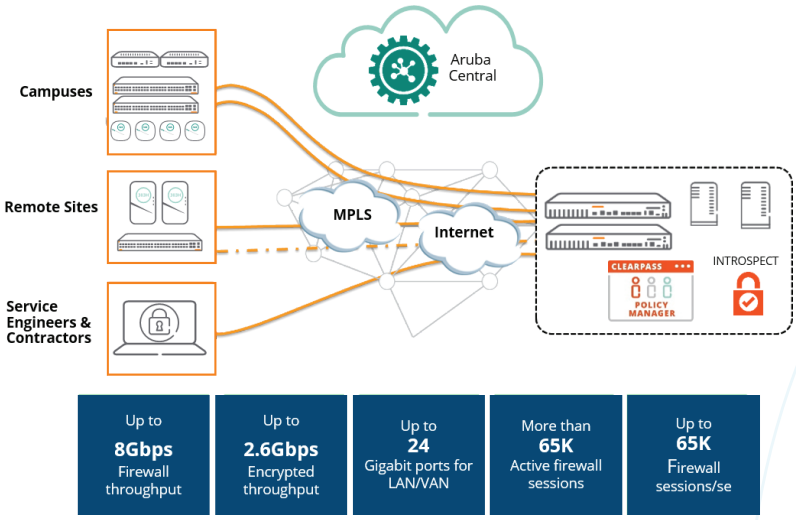

Figure 27: Aruba Remote SCADA Site Connectivity

REDUNDANT INTRA-SITE WIRELESS VIDEO AND DATA LINKS

Outdoor surveillance video and remote gate 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.

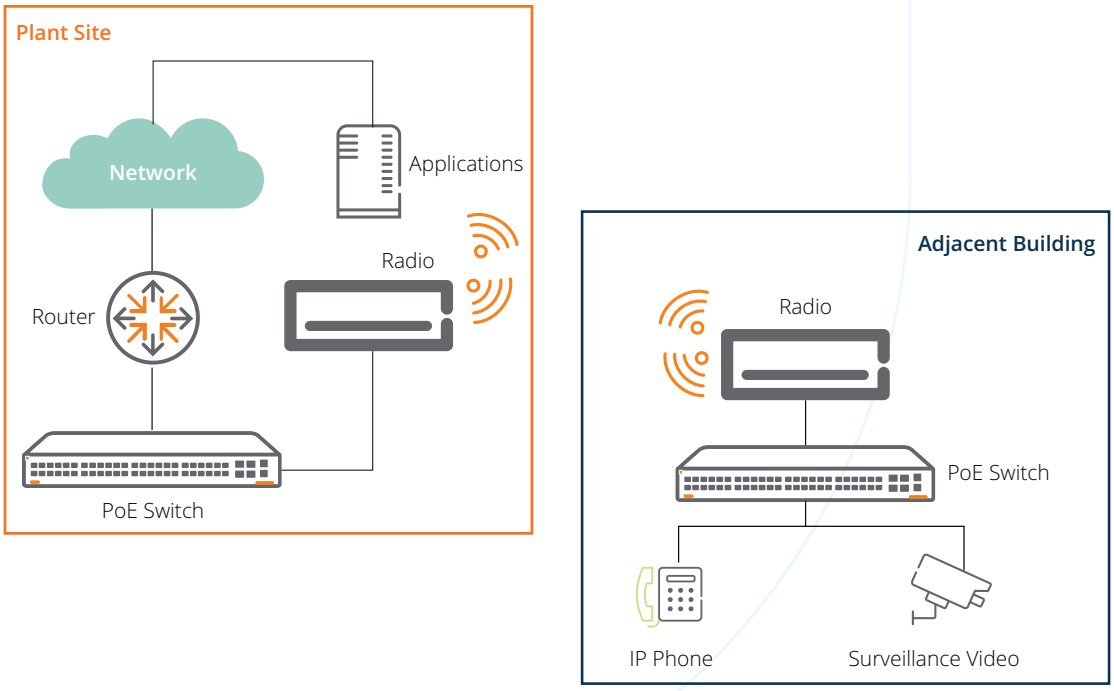

Figure 28: Point-To-Point Extension of a Plant Network to an Adjacent Building

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.

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.

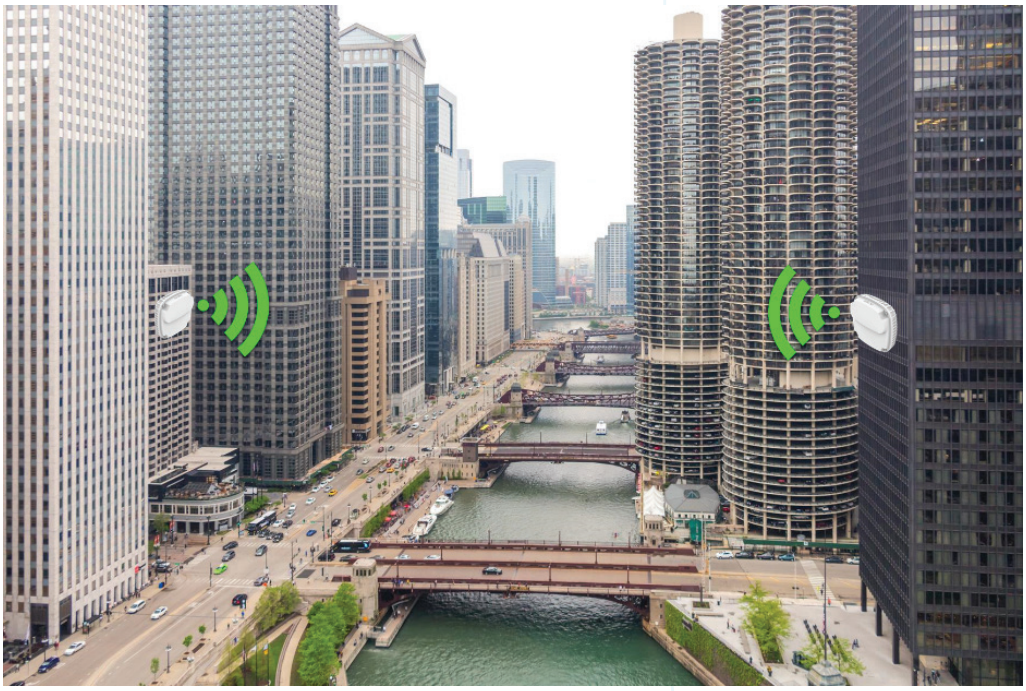

Figure 29: Aruba AP-387 High-Speed Outdoor Point-To-Point Link

MONITORING THE SWITCHING FABRIC TO DETECT SECURITY-IMPACTING IOT ISSUES

As buildings 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.

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 30: 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.

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

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

Figure 31: Meridian-Based Patrocinium Emergency Response Platform

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

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

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

Key benefits include:

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

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

SECURING CONTROL NETWORKS THAT CAN'T PROTECT THEMSELVES

Building plants typically deploy 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 building 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.

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 enterprise, 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 can be 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.

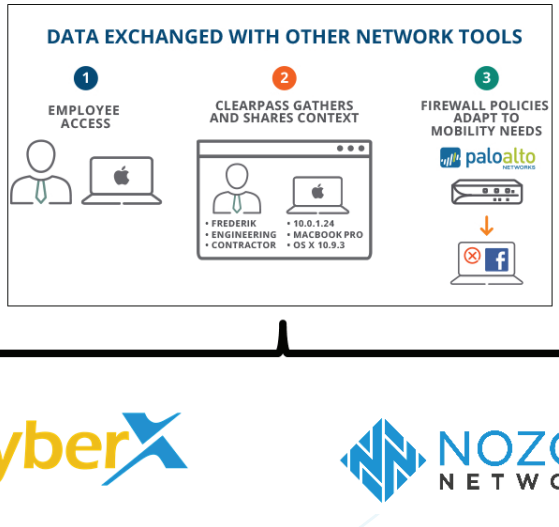

Figure 32: OT Security System Integration With Aruba ClearPass

SUMMARY

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

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

Please contact us for more information on how we can help your facilities make the digital transformation to hyper awareness.

CITATIONS

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

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

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

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

aruba
a Hewlett Packard Enterprise company

WP_Designinghyper-awaresmartbuildings_SK_072420 a00100717enw

Contact Us **Share**