WHITE PAPER

REMOTELY CONNECTED

SECURE REMOTE MONITORING FOR INTERNET OF THINGS APPLICATIONS

aruba
a Hewlett Packard
Enterprise company

TABLE OF CONTENTS

INTRODUCTION

In a provocative 2015 report, Gartner analysts Karamouzis, Jivan, and Notardonato opined that the rise of smart machines, cognitive technologies, and algorithmic business models could render obsolete the competitive advantage of offshoring.[1] Hyper-automation, the analysts argued, will trump labor arbitrage in driving profitability and enhancing productivity. Smart machines will accomplish this by classifying content, finding patterns, and extrapolating generalizations from those patterns. The eyes and ears of smart machines will be the Internet of Things (IoT), the so-called "digital mesh," which will be given voice by secure connectivity infrastructure.[2, 3]

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 control networks that for decades have been running our factories, cities, and critical infrastructure. What is new today with IoT are the number of devices from which we can potentially draw data, the power of the analytics applications that can derive insights from those data, and the impact on our personal lives, businesses, and economies that those insights can spawn.

The first step on that journey is improving visibility into the process, business, and customer data locked inside devices, machines, and infrastructure. Regardless of whether the data are local or remote, we need mechanisms to securely tap into them without compromising end-to-end security. IoT data must be protected and governed in-motion and at-rest throughout their lifecycles to ensure compliance in their use.[4]

Once data visibility and security have been achieved we can begin to reap the business benefits of IoT.[5] For example, IoT data can drive profitability by helping merchants better understand customers and their preferences. IoT can also enhance productivity through process improvement, and the empowerment of the people who run them.[6]

The Internet of Things Value Cycle (Figure 1) shows the interplay between visibility, security, profitability, and productivity. Achieving adequate visibility and security are critical challenges for most IoT deployments and organizations.

A simple case in point shows why. Operational technology (OT) data are rich with insights about processes and device performance. Having access to these data could enhance a variety of applications and services including, among others, supply chain efficiency, inventory management, and predictive maintenance. OT system designers and integrators are specialists in system functionality and reliability, however, they're rarely experts in cybersecurity.[7] OT designers often rely on isolation, including air gaps, to protect OT systems against attack, an approach that has proven ineffective from a security perspective and deprives the enterprise of valuable business insights.[8]

The good news is that we have alternate solutions to walled gardens that both establish a trustful IoT and deliver greater visibility. Aruba's white paper, *Connect-and-Protect: Building A Trust Based Internet Of Things For Business Critical Applications*, introduces the building blocks needed to assert trust. In this paper we'll apply those building blocks to show how Aruba's secure remote monitoring solutions simultaneously address both IoT visibility and security.

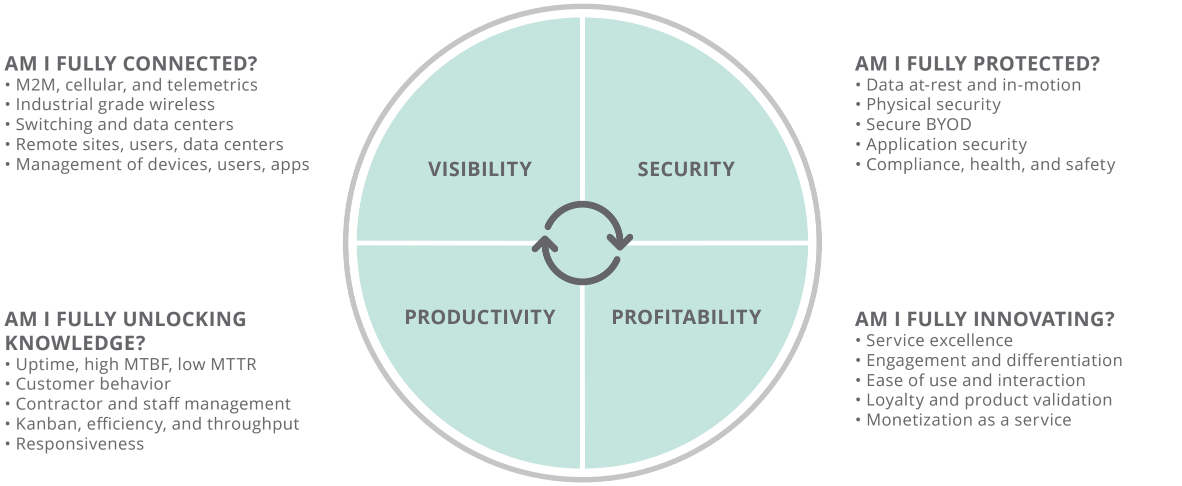

AM I FULLY CONNECTED?
• M2M, cellular, and telemetrics
• Industrial grade wireless
• Switching and data centers
• Remote sites, users, data centers
• Management of devices, users, apps
AM I FULLY PROTECTED?
• Data at-rest and in-motion
• Physical security
• Secure BYOD
• Application security
• Compliance, health, and safety
VISIBILITY
SECURITY
PRODUCTIVITY
PROFITABILITY
AM I FULLY UNLOCKING KNOWLEDGE?
• Uptime, high MTBF, low MTTR
• Customer behavior
• Contractor and staff management
• Kanban, efficiency, and throughput
• Responsiveness
AM I FULLY INNOVATING?
• Service excellence
• Engagement and differentiation
• Ease of use and interaction
• Loyalty and product validation
• Monetization as a service

figure 1.0_092816_iotremotemonitoring-wpa

Figure 1: Internet of Things Value Cycle

ANATOMY OF AN IOT SECURE REMOTE MONITORING SOLUTION

Secure remote monitoring infrastructure includes a few basic building blocks that can be mixed to address different implementation requirements: Intelligent IoT Device, Access Device, Communications Media, IoT Controller, IoT Business and Analytics Application, and Device and Network Management. Let's consider each building block in turn.

Intelligent IoT Device

An Intelligent IoT Device is a machine, or a group of machines, that generate data (e.g., temperature) – or perform a function (e.g., open/close valves) – into which the enterprise wants visibility. Those data could be in analog or digital formats, and may be accessible through discrete inputs and outputs (IO), a serial interface, a control protocol, TCP/IP, cellular, or some other wired or wireless network format. Device communications may be limited to an isolated group of devices, while in other cases — like automotive telematics and demand-side management systems — a centralized data center may serve tens of millions of IoT devices.

Access Device

There are two forms of Access Devices: Gateways and Converged IoT Systems. A Gateway converts data streams from IoT Devices into a secure format that is compatible with the network in use. Gateways are used when an IoT Device lacks the ability to securely with a network (LAN, cellular, Wi-Fi), is unable to run a local VPN client for secure remote access, or has serial, analog, or proprietary inputs/outputs (I/O) that are incompatible with the target network.

Figure 3: Access Devices: Aruba RAP and Edgeline Gateway

A Converged IoT Device has the I/O interfaces and compute power to locally process data from Intelligent IoT Devices. This solution is used to reduce process latency, lower the volume and cost of wide area data communication traffic, process and store local IoT activity, and/or send a remote data center a summary of local IoT activity. Converged IoT Devices accomplish these tasks by locally running machine learning and data analytics engines, and the devices are characterized by their powerful compute engines, ability to ingest analog/digital sensor data and control bus traffic, and remote management capabilities.

Figure 4: Access Devices: Aruba Converged IoT Systems

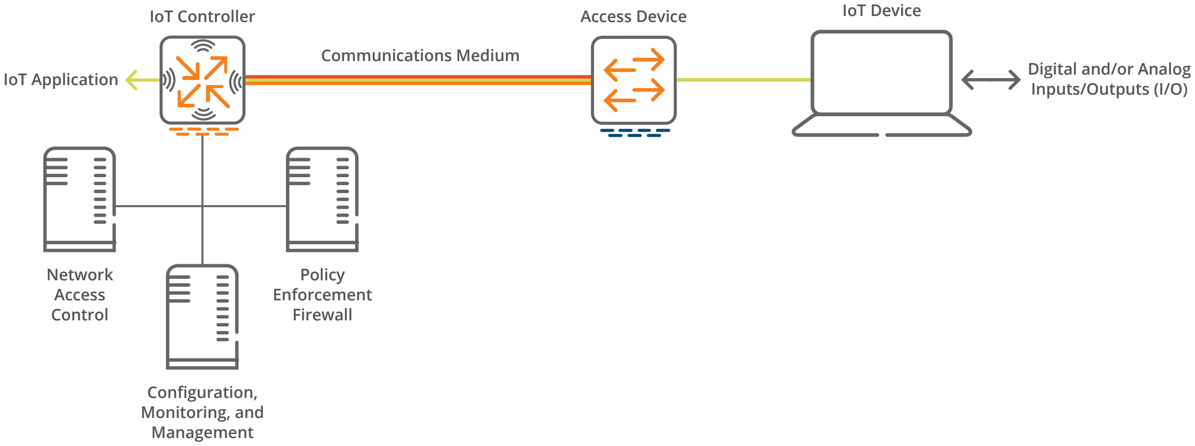

IoT Controller
Access Device
IoT Device
Communications Medium
IoT Application
Digital and/or Analog Inputs/Outputs (I/O)
Network Access Control
Policy Enforcement Firewall
Configuration, Monitoring, and Management

fig.2.0_092816_iotremotemonitoring-wpa

Figure 2: IoT Secure Remote Monitoring Infrastructure Building Blocks

An Access Device may also be needed when data traffic from many IoT devices must be consolidated within a single VPN tunnel or wireless connection, or when the site owner prohibits a connection to their enterprise network. Corporate prohibitions against connecting IoT devices to enterprise networks are not unusual today, and arise out of concerns about IT security, management, and accountability. Corporate data breaches that were launched through IoT infrastructure, Target being the poster child,[9] have given some CISOs pause about comingling IoT and corporate data networks.

Communications Media

The Communications Media used in IoT systems vary considerably, and may include wired Ethernet, Wi-Fi, cellular, or specialized control network physical layers. There are dozens of different control network physical layers, and even more controls protocols that use them. Table 1 presents some of the standard-based control network physical layers, and Table 2 shows the more common control network protocols used in different vertical markets.

Gateways provide physical layer (PHY) and protocol conversion that reformats and tunnels control data over a Communications Media with which they would otherwise be incompatible. This feature enables IoT remote access systems to monitor both new IoT Devices, and ones that use legacy control protocols.

TABLE 1: CONTROL NETWORK PHYSICAL LAYERS

Standard	Medium
IEEE 802.15.1	Bluetooth radio frequency
IMT-2000, ETSILTE	Cellular radio frequency
IEC 61754	Fiber optics
IEEE 11073-30300	Infrared
IEEE 488	Short-haul cable
ISO/IEC 14543-3-6	Twisted pair
IEC 61158-2	Twisted pair
IEEE 11073-30200a	Twisted pair
IEEE 802.3	Twisted pair – Ethernet
ISO/IEC 14908-2	Twisted pair – free topology
ISO 11898-2	Twisted pair – high speed
ISO 11898-3	Twisted pair – low speed
ISO/IEC 14908-3	Power line carrier – narrow band
ISO/IEC 14543-3-5	Power line carier – narrow band
IEEE 1901	Power line carrier – wide band
ISO/IEC 14543-3-7	Radio frequency
IEEE 802.15.4	Radio frequency
ISO/IEC 14543-3-10	Radio frequency – Energy harvesting

TABLE 2: CONTROL NETWORK PROTOCOLS

AS-i	Profinet IO	IEC 60870-5
BSAP	SERCOS	IEC 60870-6
Control Area Network (CAN)	Sinec H1	IEC 61850
CC-Link Industrial Networks	SynqNet	IEC 62351
CIP	TTEthernet	ANSI C12 18
ControlNet	RAPIEnet	DLMS/IEC 62056
DeviceNet	MTConnect	IEC 61107
DF-1	OPC DA	ISO/IEC 14908.1
DirectNet	OPC HDA	M-Bus
EtherCAT	OPC UA	AFDX
Ethernet Global Data (EGD)	BACnet	ARINC 429
Ethernet/IP	C-Bus	ARINC 825
Ethernet Powerlink	DALI	FlexRay
FINS	DSI	FMS
FOUNDATION Fieldbus	Insteon	IEBus
GE SRTP	ISO/IEC 14543-3-1 (KNX)	ISO/IEC 14908.1
HART Protocol	ISO/IEC 14908.1 (LonTalk)	J1587
Honeywell SDS	oBIX	J1708
HostLink	VSCP	Keyword Protocol 2000
InterbusS	X10	LIN
Mechatrolink	xAP	MOST
MelsecNet	xPL	NMEA 2000
Modbus	ZigBee	SAE J1939
Optormux	DNP3	Unified Diagnostic Services
Profibus	IEC 60870	VA

Wide area networks (WANs) may use cellular, satellite, DSL, cable modem, fiber optics, microwave, MPLS, or E1/T1, among others. To prevent the loss of data, high availability applications may require two separate and distinct connections, such as DSL and cellular. If one fails the alternate connection will automatically be selected by the Access Device. Cellular has the advantage of being quickly set up and easily moved, as needed, in the event of a disaster or during adds, moves, and changes. The downside of cellular is the high recurring subscription costs, especially for data heavy applications.

High cellular costs can be addressed by using a Mobile Virtual Network Operator (MVNO) that has pre-negotiated favorable subscription rates for low bandwidth IoT applications such as machine monitoring applications. Pre-processing IoT data on-site using a Converged IoT System with analytics software can also significantly reduce both the volume and cost of cellular in data heavy applications.

Intelligent IoT Devices and Access Devices that use a VPN need security commensurate with the application. Internet Protocol Security (IPsec) ESP encrypts and encapsulates data between two locations, and is commonly used for commercial VPNs that traverse public telecommunications infrastructure, including the Internet. IPsec supports AES 256+ bit key encryption and provides network-level peer authentication, data origin authentication, data integrity, and replay protection. For government IoT applications, Suite B elliptic curve encryption may be required to protect IoT devices associated with foreign releasable information, US-Only information, or Sensitive Compartmented Information (SCI) up to Top Secret classification.

IoT Controller

The IoT Controller terminates VPNs, typically at a data center or an intermediate aggregation point, and hands off the data to an Application for processing. The controller manages network encryption and authentication, and interfaces with firewall, network access control, and policy management applications that enforce application-layer security, packet prioritization, and access rules.

Figure 5: Aruba Controller

IoT data should remain encrypted from source to destination so there's no clear text available to snoop. However, this isn't always possible. Older IoT devices, or ones that lack modern cyber security capabilities, have to rely on a Gateway or Converged IoT System to encrypt the IoT data. The clear text link from the IoT Device presents a vulnerability that needs to be addressed using physical measures, e.g., securely embedding the Access Device inside the IoT Device and monitoring the data link for tampering.

IoT Business Analytics and Applications

Data are the new eye candy – or "bacon" – in the world of business transformation, and it's the Business and Analytics Applications that add sizzle to the process. These applications consume IoT data and use mathematics, statistics, machine learning, and predictive modeling to visualize data, manage operations, detect security violations, and create innovative new services based around contextual data like location. Examples include HPE Vertica, Software AG APAMA, Schneider Wonderware, and GE Predix.

Device and Network Management: Adaptive Trust

IoT Device network access needs to be governed by the same adaptive trust model used for IT devices: trust no IoT Device until proven otherwise. Adaptive trust accomplishes this by using multiple complementary protective mechanisms to assert trust and minimize threat vectors. These mechanisms include:

- Detection – detects or assigns identity when a new IoT device attempts to access the network;
- Profiling – determines whether the devices is safe, unsafe, or unknown;
- Posture – checks continuously if the IoT device's operating system, anti-malware, anti-virus, and other parameters are in compliance with your guidelines;
- Remediation – quarantines or redirects non-compliant devices to a remediation site at which they can be brought into compliance;
- Authentication – assigns identity and validates the authenticity of the IoT device;
- Policy compliance – continuously checks for compliance with defined policies. Works in tandem with policy enforcement firewall, mobile device management (MDM), enterprise mobility management (EMM), security information and event management (SIEM), and north-bound firewall systems;
- Enforcement – determines how policy violations will be handled, i.e., quarantining, monitoring, or redirecting the IoT device.

When a new device attempts to access the network it should not be allowed to connect until it has been identified, its characteristics profiled, and its authenticity validated.

Device and Network Management: Configuration and Monitoring

Device and Network Management tools configure, manage, and monitor IoT systems and their associated networking infrastructure. In line with the separation in responsibilities between OT and IT, it is common practice to use separate tools for managing devices and networks: OT tools manage IoT Devices, and IT tools manage network infrastructure. Presumably as OT and IT responsibilities merge, so, too, will the tool chains merge but today they remain separate in most enterprises.

Configuration tools reduce the workload of administrators by automating what previously were manual processes. Software updates, diagnostics, trouble-shooting, adds, moves, and changes should be remotely managed without requiring a truck role. For example, it should be possible to remotely determine if the source of a problem is local RF interference versus an actual problem in an IoT device. With the proliferation of IoT Devices, labor savings becomes even more critical, and new IoT Devices and Access Devices should be able to roam back to a public or private cloud, authenticate themselves, and then download their configuration over a secure link without any manual intervention.

Monitoring tools identify and react to abnormal conditions, report on device and system performance, and provide analytics engine to device insights from IoT Device data. The ideal monitoring tool offers carrier-grade scalability, availability, and service level agreements (SLAs). It also will securely expose IoT Device data to, and exchange access policies and security violations with, authorized external applications.

ARUBA IOT REMOTE MONITORING SOLUTIONS

Aruba's IoT Remote Monitoring solutions are easier for IT and OT staff to set-up and manage, deliver a uniform experience for IoT Devices and users across all locations, and feature significantly lower total cost of ownership than traditional approaches to remote access. Key unique features include:

- Zero-touch configuration;
- Support for a broad range of IoT protocols and WAN communication options;
- Local analytics and IoT data processing;
- User and Entity Behavioral Analytics (UEBA);
- Role- and policy-based access control;
- Centralized VPN suitable for industrial, commercial, and defense applications;
- On-premise, private-cloud, and public-cloud IoT network management;
- IoT Device monitoring.

These solutions leverage a broad range of Aruba and HPE products including:

- Remote Access Points (RAP);
- VIA VPN Clients (commercial or Suite B);
- Edgeline Gateways;
- Edgeline Converged IoT Systems;
- Aruba Virtual or Hardware Controllers;
- ClearPass IoT Profiler and NAC;
- IntroSpect User and Entity Behavior Analytics (UEBA).

Figure 6 shows where these products fit into the secure remote access path. Each will be discussed in turn in the next sections.

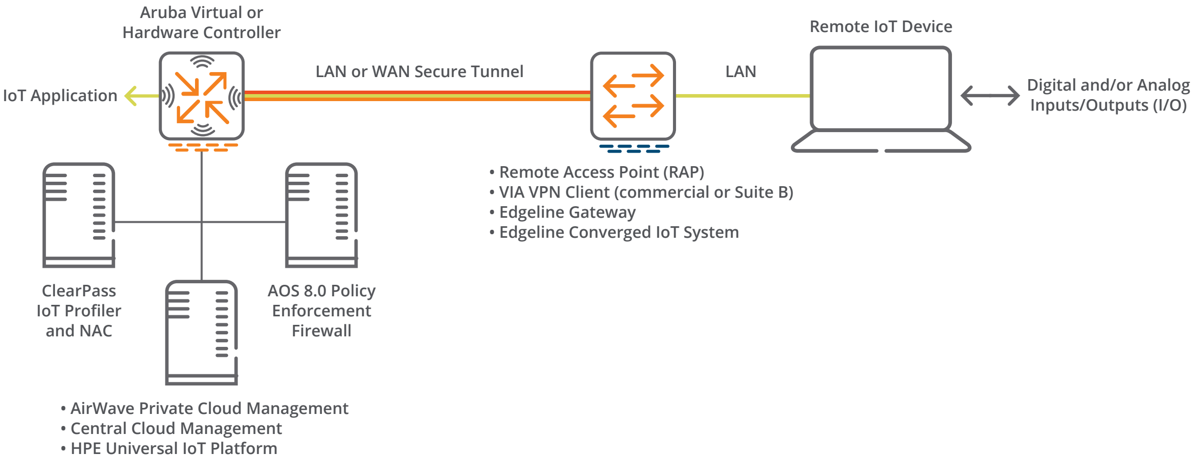

Aruba Virtual or Hardware Controller
IoT Application
LAN or WAN Secure Tunnel
LAN
Remote IoT Device
Digital and/or Analog Inputs/Outputs (I/O)
• Remote Access Point (RAP)
• VIA VPN Client (commercial or Suite B)
• Edgeline Gateway
• Edgeline Converged IoT System
ClearPass IoT Profiler and NAC
AOS 8.0 Policy Enforcement Firewall
• AirWave Private Cloud Management
• Central Cloud Management
• HPE Universal IoT Platform

fig.6.0_092816_iotremotemonitoring-wpa

Figure 6: Aruba and HPE IoT Secure Connectivity Infrastructure

VPNs and Access Devices

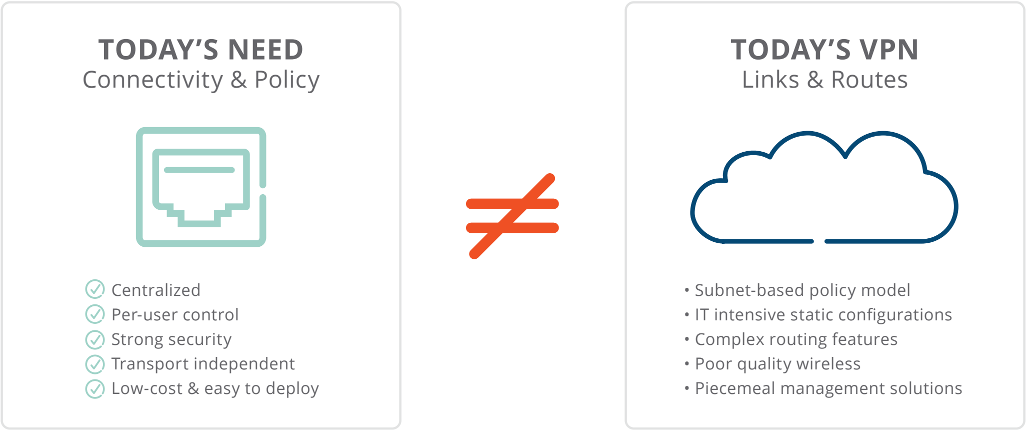
VPN access has historically been both essential for security and vexing to set up: the labor savings that come from centralized VPN management are often offset by the complexity of system configuration and modifications. Additionally, VPNs don't protect endpoints or data at rest, and need to be supplemented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

Aruba addresses these issues by enabling the Access Device to support VPN client functionality while simultaneously sharing access to multiple IoT Devices, say via wired and wireless LAN interfaces. In this scenario the IoT Controller acts like a VPN concentrator, and the Access Device sets up one or more secure, encrypted tunnels with the IoT Controller thru which the IoT Devices communicate. The IoT Controller's role-based firewall then enforces policies on a per-packet, per-flow basis. The result is a remote access solution that blends the simplicity of a centralized, network-based VPN with the flexibility of role-based access control for all IoT Devices

Aruba offers two types of VPN client (commercial and government Suite B) and three types of Access Devices (Remote Access Points, Edgeline Gateways, and Edgeline Converged IoT Systems). The optimum solution for an application will vary according to the IoT Device interface, security requirements, and WAN communication requirements.

IoT Devices that are capable of running VPN clients, can use Aruba VIA or Suite B software clients, as long as they are running Linux, Windows, iOS, OS X, or Android operating system. The VIA VPN client is designed for commercial applications, while Aruba's Suite B VPN client targets high security government, finance, banking, and insurance applications. A hybrid IPsec/SSL VPN, VIA automatically scans and selects the best secure connection to the corporate network. Unlike traditional VPN clients, VIA offers a zero-touch experience. For military grade IoT device security, VIA supports Suite B cryptography when used with a controller running the Aruba OS Advanced Cryptography (ACR) module. ACR supports controlled unclassified, confidential, and classified information.

RAPs provide secure remote connectivity to Ethernet or Wi-Fi based IoT Devices using a WAN and/or cellular connection. IoT Device and technician network access policies are enforced via dissolvable firewall agents: if a RAP be lost or stolen no security information will be compromised. Devices and users are authenticated, and IoT data are encrypted, to commercial or government standards without any client software or manual intervention. Should there be a technical issue, a 1-button debugging feature and 1-button "reset" to default make quick work of troubleshooting without the need to dispatch service personnel. The result is a high security connection that is easily configured, requires no user training, and delivers a plug-and-play IoT monitoring experience.



TODAY'S NEED
Connectivity & Policy

- ✓ Centralized
- ✓ Per-user control
- ✓ Strong security
- ✓ Transport independent
- ✓ Low-cost & easy to deploy

≠

TODAY'S VPN
Links & Routes

- Subnet-based policy model
- IT intensive static configurations
- Complex routing features
- Poor quality wireless
- Piecemeal management solutions

figure 7.0_092816_iotremotemonitoring-wpa

Figure 7: Remote Access Needs do not Align with the Capabilities of Today's VPNs

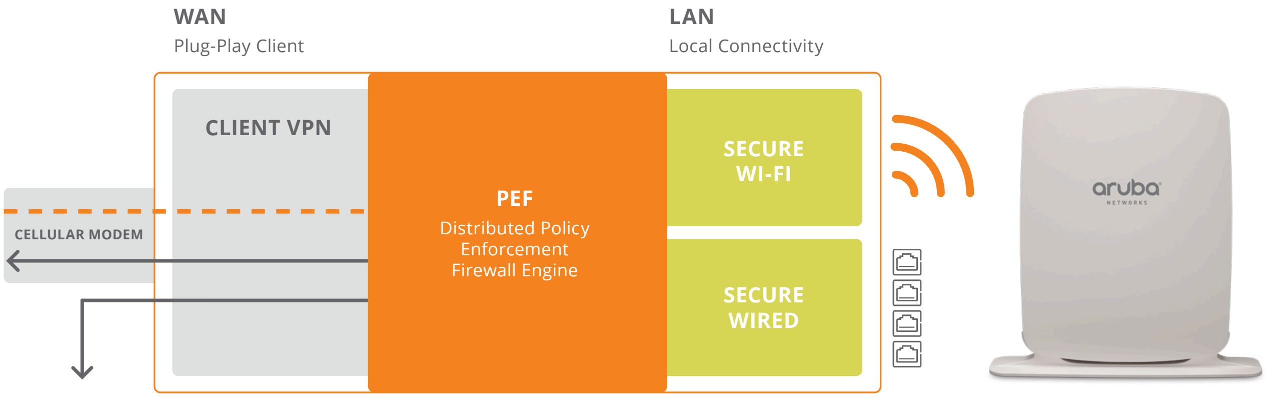


Figure 8: Aruba RAP Architecture and RAP-155

figure 8.0_092816_iotremotemonitoring-wpa

RAPs are available with a wide range of indoor/outdoor mounting and interface configurations. A cellular modem can be used for rapid-deployment applications and sites without a wired WAN. Any Aruba Wi-Fi access point can be software-enabled as a RAP, allowing spare parts inventory to be repurposed between corporate and IoT applications, if required.

Edgeline Gateways are ruggedized, wide temperature IoT edge processors that combine powerful compute platforms with expansive memory, a Trusted Platform Module, Wi-Fi and Ethernet connectivity, cellular modem options, and flexible serial, analog, and digital I/O. Gateways can run software to preprocess data streams in real-time, store results, and interface IoT Devices to remote data centers and/or IoT cloud services.

Edgeline Converged IoT Systems come with data center-grade edge processing power and memory, Trusted Platform Modules, Wi-Fi and Ethernet connectivity, cellular modem options, and PXI serial, analog, digital, and control network I/O interfaces. Supported control networks include CAN and Modbus, among others. The Converged IoT Systems can locally run analytics and machine learning applications for faster time to insights and to preprocess data prior to sending summaries results to remote applications. Table 3 summarized VPN and Access Device options and applications.

TABLE 3: VPN AND ACCESS DEVICE OPTIONS

IoT Device Type	VIA VPN Client	Suite B VPN Client	Remote Access Point	Edgeline Gateway	Edgeline Converged IoT System
Analog, digital, or serial interface				✓	✓
RS-485 control network interface				✓	✓
Modbus or CAN interface				✓	✓
Cloud IoT analytics gateway				✓	✓
VXI compatible interface					✓
Edge analytics/machine learning					✓
Ethernet interface			✓	✓	
Wi-Fi interface			✓		
OS supports VPN client	✓				
FIPS 140-2 or government		✓	✓		
Requires cellular backhaul			✓	✓	

Access Control and Security: Aruba Controller

Aruba controllers running the Aruba Operating System (AOS) terminate VPNs, manage identity assignment, centralize encryption, and run Aruba's unique role-based firewall. Every IoT 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 IoT Devices regardless of how or where they connect to the LAN, wireless LAN, or 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 contextual data such as location, time of day, day of week, and current security posture to provide more granular role based access control.

Since IoT Devices can be both stationary and mobile, or can switch between the two modes. This behavior means there isn't always a fixed port through which an IoT Device always connects, so traditional firewalls that rely on port-based security are ineffective. Additionally, MAC authentication without 802.1X can be spoofed using a replicated MAC address, so role-based control is essential to enforce control over headless IoT Devices.

A role is applied during the authentication process, before the IoT 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 and ensures 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.

Role-based firewall rules can be constructed based on identity, applications in use, source and destination of traffic, service type, time of day, physical location, and device state when using client integrity software. Policy actions can include permit, deny, redirect to external devices or tunnels, logging, or Quality of Services actions such as setting Differentiated Services (DiffServ) bits and placing traffic into high or low priority queues.

Automated denylisting will block network access if firewall rules are violated even a single time. Such a trip-wire is particularly useful for single-function IoT sensors and actuators: if the firewall detects a compromised IoT Device attempting to conduct unauthorized database queries or file server browsing, it can be immediately disconnected from the network and an alert generated.

The heterogeneous nature of IoT Device types, network access methods, and network resource requirements are tailor-made for role-based control. Some of the key benefits of Aruba's approach to role-based control include:

- Allows multiple classes of IoT Devices to share one common network but be treated differently based on role;
- Eliminates excess network privilege normally granted by "one size fits all" fixed networks;
- Locks down the network against unauthorized disclosure or alternation of information;
- Provides accountability through auditing of network infrastructure and activity;
- Protects devices from attack by other devices;
- Blocks the propagation of viruses, worms, and other malware.

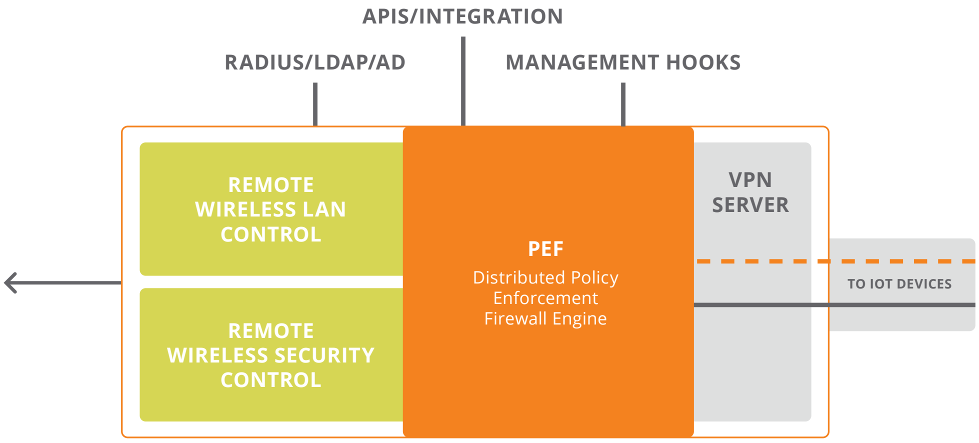

APIS/INTEGRATION
RADIUS/LDAP/AD
MANAGEMENT HOOKS
REMOTE WIRELESS LAN CONTROL
REMOTE WIRELESS SECURITY CONTROL
PEF
Distributed Policy Enforcement Firewall Engine
VPN SERVER
TO IOT DEVICES

figure 9.0_092816_iotremotemonitoring-wpa

Figure 9: Aruba Controller Architecture

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

Access Control and Security: ClearPass Access Control

Access rules and context – collectively called "policies" – determine how, when, and where IoT Devices can access network resources. IoT policy management, network access control, and endpoint compliance for IoT Devices, and the technicians that support them, are handled by Aruba's ClearPass Access Management System.

The ClearPass IoT Device Profiler automatically discovers and classifies IoT Devices, regardless of device type, using a variety of contextual data including MAC OUIs, DHCP fingerprints, and other identity-centric device data. Upon connection, unmanaged non-802.1X devices are classified as known or unknown upon connecting to the network based on the presence of their MAC address in an external or internal database. Stored profiling signatures identify device profile changes and dynamically modify authorization privileges. For example, if a Programmable Logic Controller tries to masquerade as a Windows PC, the policy manager will automatically deny access.

ClearPass posture monitoring uses device health checks based on interactive interrogation of the IoT Device to determine known vulnerabilities, active ports, operating system version, SNMP security, and openSSL vulnerabilities. Posture needs to be routinely verified to ensure compliance, and known good IoT Devices may be denied access if the posture is sub-standard, and even redirected to a remediation site at which patches and updates are available to correct the issue(s).

ClearPass authentication services validate the authenticity of any IoT Device connecting to the network, locally or remotely. Authentication services include:

- 802.1X authentication with RADIUS for centralized authentication, authorization, and accounting management before providing network access;
- MAC authentication to authenticate devices based on their physical MAC addresses;
- MAC authentication followed by 802.1X authentication;
- Captive portal for temporary mobile devices, e.g., industrial tablets used by service personnel.

Authentication can be managed independently by ClearPass or in conjunction with existing AAA resources already in use. Both single and two-factor authentication are supported assuming the IoT Device is capable of responding to a two-factor challenge.

Since attacks can have many origins, a holistic approach to IoT device threat prevention must operate at every level of the network – from profiling IoT Devices to governing when and how they access the network, applications, and northbound Internet traffic. ClearPass achieves this by sharing policies and threat notifications with MDM, EMM, SIEM, and northbound next-gen firewalls. Each platform operates at a different point of enforcement, and working in concert they address IoT threat scenarios at every network level.

This security framework can be extended to additional technologies in the infrastructure. For example, exchanging syslog data flows and using APIs to exchange attributes with MDM, SIEM, and related security services accelerates NAC response to any detected violations. And a violation anywhere can be enforced everywhere. Representative supported technology partners include: Mobile Iron, AirWatch, MaaS360, Citrix, Afaria, SOTI, and Jamf for MDM: Microsoft InTune for EMM; ArcSight for SIEM; and Palo Alto Networks, Checkpoint, and Fortinet for next-gen firewalls.

Being context-based enables ClearPass to have tight control of network access privileges based on variable such as an IoT Device's role, type, MDM attributes, device health, location, and time-of-day. If available, attributes from multiple identity stores can be used within a single policy for the finest-grained control. Examples of identity stores include, Microsoft Active Directory, LDAP-compliant directory, ODBC-compliant SQL database, token servers and internal databases across domains

If a more advanced IoT Device with an operating system is used then ClearPass endpoint posture assessment will ensure compliance with access authorization policies before the device connects, e.g., the device is not allowed to connect unless it has the latest anti-virus, anti-spyware, firewall, and peer-to-peer application policy settings. Automatic remediation services enable non-compliant IoT Devices to become compliant and then connect without manual intervention.

Aruba IntroSpect UEBA

It is no longer enough to assert trust at the time an IoT solution is deployed. The evolution of malware, and the constant threat of insider attacks, mandate the continuous revalidation of trust. The sheer volume of IoT traffic outstrips the ability of human analysts to monitor IoT traffic, so automated user and device behavior analytics must be applied.

IntroSpect detects attacks on IoT devices and associated personnel by spotting small changes in behavior that are often indicative of attacks that have evaded traditional security defenses. The solution integrates advanced artificial intelligence-based machine learning, pinpoint visualizations and instant forensic insight into a single solution. Attacks involving malicious, compromised or negligent users, systems, and devices are found and remediated before they damage IoT infrastructure and operations.

IntroSpect builds baselines of normal behavior for devices, users, and systems. The baselines are built by machine learning models that operate on key data from logs, netflow and packet streams—any data that characterize behavior. These baselines are then used to detect abnormal behavior that, aggregated over time and put into context, indicate a gestating attack. Based on a Spark/Hadoop platform, IntroSpect uniquely integrates both behavioral-based attack detection and forensically-rich incident investigation and response at enterprise scale.

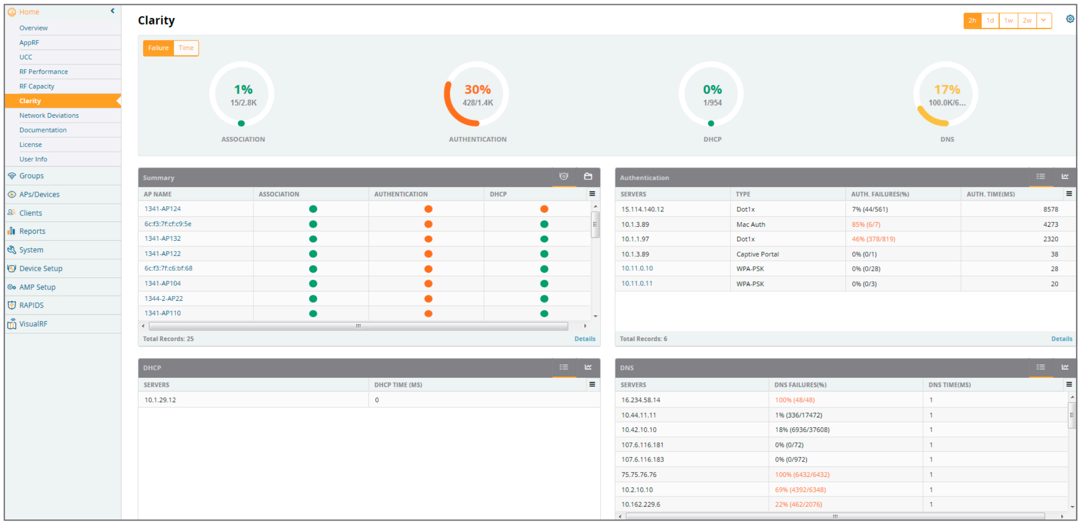
IoT Network Management

IoT network management and IoT Device monitoring are two different specialties, one highly IT and cybersecurity focused, and the other OT- and device-centric. No tools today offer best-in-class support for both areas simultaneously, hence they are split into separate tool chains.

Aruba's AirWave Network Management System provides fine grained visibility into wired, Wi-Fi, and remote access IoT networks. The system proactively monitors the health and performance of infrastructure and devices, and provides insights into applications in use, security violations, and network bandwidth utilization. Designed for use with multi-vendor network infrastructure, AirWave provides a centralized, intuitive, single-pane-of-glass user interface. Real-time monitoring, proactive alerts, trouble ticket generation, and historical reporting shows the health and performance of infrastructure at a glance.

AirWave's intrusion detection systems identifies unauthorized access attempts and devices across both wired and wireless infrastructure. Wireless data are correlated with wired data to identify the most significant and relevant threats while simultaneously reducing false positives.

AirWave can also proactively monitor critical metrics with the Aruba Clarity module. This module monitors the time it takes for a mobile IoT device to associate with a Wi-Fi radio, authenticate to a RADIUS server, gather an IP address through DHCP, or resolve names through DNS services. With custom alerts and simulated client testing, Clarity lets IT take proactive action against future performance problems.



Summary

AP NAME	ASSOCIATION	AUTHENTICATION	DHCP
1341-AP124	●	●	●
6c:f3:7f:cf:c9:5e	●	●	●
1341-AP132	●	●	●
1341-AP122	●	●	●
6c:f3:7f:c6:bf:68	●	●	●
1341-AP104	●	●	●
1344-2-AP22	●	●	●
1341-AP110	●	●	●

Total Records: 25 Details

Authentication

SERVERS	TYPE	AUTH. FAILURES(%)	AUTH. TIME(MS)
15.114.140.12	Dot1x	7% (44/561)	8578
10.1.3.89	Mac Auth	85% (6/7)	4273
10.1.1.97	Dot1x	46% (378/819)	2320
10.1.3.89	Captive Portal	0% (0/1)	38
10.11.0.10	WPA-PSK	0% (0/28)	28
10.11.0.11	WPA-PSK	0% (0/3)	20

Total Records: 6 Details

DHCP

SERVERS	DHCP TIME (MS)
10.1.29.12	0

DNS

SERVERS	DNS FAILURES(%)	DNS TIME(MS)
16.234.58.14	100% (48/48)	1
10.44.11.11	1% (336/17472)	1
10.42.10.10	18% (6936/37608)	1
107.6.116.181	0% (0/72)	1
107.6.116.183	0% (0/972)	1
75.75.76.76	100% (6432/6432)	1
10.2.10.10	69% (4392/6348)	1
10.162.229.6	22% (462/2076)	1

Figure 10: AirWave Clarity Display

IoT Device Monitoring

IoT Device monitoring tools need to support a broad range of device types, protocols, and communications media. They also need to provide powerful analytics form assessing IoT Device data, and interfaces to share those data with complementary applications.

HPE's Universal IoT Platform (UIoT) is designed from the ground up for IoT Device monitoring, and includes a range of services to accommodate these requirements. UIoT services include:

- APIs through which data may be consumed by client applications;
- Digital services through which new applications, micro services, and algorithms can be quickly introduced;
- Data acquisition from virtually any IoT protocol via open source message brokering;
- Robust predictive analytics with pre-built algorithms and ready to use templates;
- Alignment with oneM2M or equivalent data structure standard and built-in protocol libraries for commonly used control protocols;
- Message queuing through open standard messaging bus including both device and subscription management.

UIoT aligns IoT Device support with the oneM2M industry standard, enhancing flexibility by ensuring that the system is industry, vertical, and vendor agnostic. The oneM2M data model supports access to different IoT devices and networks, as well as a wide variety of IoT applications and processes. This capability enables UIoT to easily support new services, IoT Devices, and IoT protocols. It also allows new applications to be rapidly instantiated on a large scale, including device discovery, configuration and control of IoT traffic (outside of traditional voice and data traffic) on the same private or hybrid cloud platform.

USE CASES

In this section we will consider five different remote monitoring scenarios including:

- Office equipment;
- Industrial chiller;
- Smart building controller;
- Service personnel wayfinding and tracking; and
- Off-shore oil platform telemetry.

Each scenario includes a table showing the different options, followed by a diagram outlining the workflow.

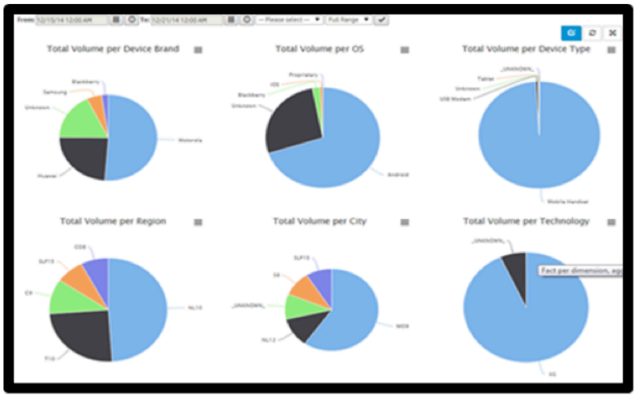
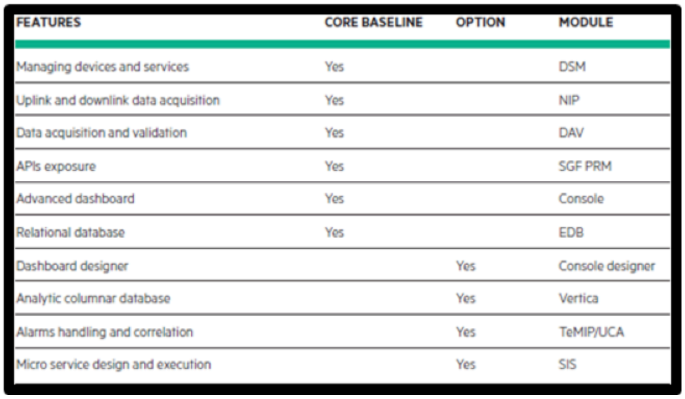


Figure 11: UIoT IoT Device Monitoring System



FEATURES	CORE BASELINE	OPTION	MODULE
Managing devices and services	Yes		DSM
Uplink and downlink data acquisition	Yes		NIP
Data acquisition and validation	Yes		DAV
APIs exposure	Yes		SGF PRM
Advanced dashboard	Yes		Console
Relational database	Yes		EDB
Dashboard designer		Yes	Console designer
Analytic columnar database		Yes	Vertica
Alarms handling and correlation		Yes	TeMIP/UCA
Micro service design and execution		Yes	SIS

Enterprise: Office Machine Monitoring

Objective

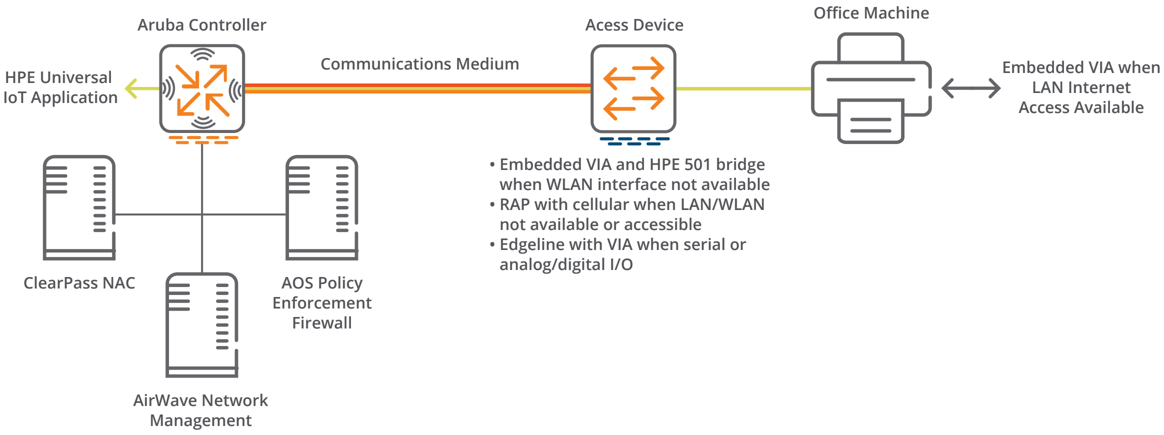
- Customer wants to improve client services by managing their office equipment including remote code updates, and toner, paper, and fault monitoring

Challenges

- Machine may lack a secure VPN capability or a Wi-Fi interface
- Access to local network forbidden by site owner and require cellular broadband
- Access to local network may permitted but subnet may not have access to the Internet

TABLE 4: OFFICE MACHINE MONITORING OPTIONS

Machine Capabilities	Local LAN Access	Local WLAN Access	No Local LAN/WLAN Access
VIA can be used, Ethernet port	VIA client	VIA and HP 501 Bridge	RAP with cellular modem
VIA cannot be used, Ethernet port	RAP	RAP	RAP with cellular modem
Serial port	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
Analog or digital I/O	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem


Aruba Controller
HPE Universal IoT Application
Communications Medium
Acess Device
Office Machine
Embedded VIA when LAN Internet Access Available
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management

- Embedded VIA and HPE 501 bridge when WLAN interface not available
- RAP with cellular when LAN/WLAN not available or accessible
- Edgeline with VIA when serial or analog/digital I/O

fig.12.0_092816_iotremotemonitoring-wpa

Figure 12: Office Machine Monitoring Diagram

Building Automation: Chiller Monitoring

Objective

- Customer wants to reduce energy bills and conduct preventive maintenance before breakdown by using remote performance and diagnostics monitoring

Challenges

- Machine may lack a native VPN capability or a Wi-Fi interface
- Access to local network forbidden by site owner and require cellular broadband
- Access to local network may permitted but subnet may not have access to the Internet
- Government customers need FIPS 140-2 and Suite B

TABLE 5: CHILLER MONITORING OPTIONS

Machine Capabilities	Local LAN Access	Local WLAN Access	No Local LAN/WLAN Access
VIA can be used, Ethernet port	VIA client, FIPS/Suite B option	VIA and HP 501 Bridge, FIPS/Suite B option	RAP with cellular modem, FIPS/Suite B option
VIA cannot be used, Ethernet port	RAP, FIPS/Suite B option	RAP, FIPS/Suite B option	RAP with cellular modem, FIPS/Suite B option
Serial port	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
Analog or digital I/O	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
Modbus or CAN	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
BACnet, LONWORKS, or other control protocol	Protocol converter and RAP, FIPS/Suite B option	Protocol converter and RAP, FIPS/Suite B option	Protocol converter and RAP with cellular modem, FIPS/Suite B option

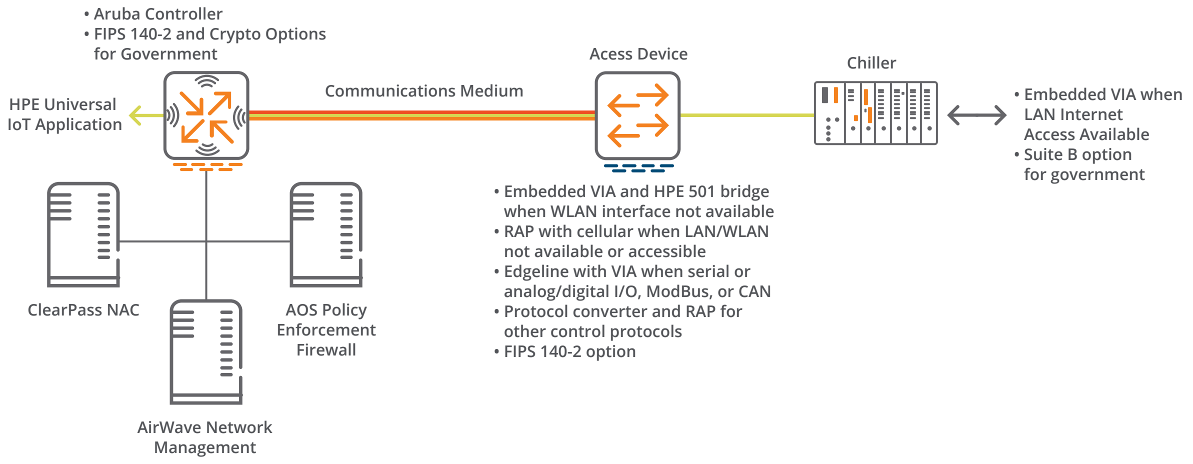

• Aruba Controller
• FIPS 140-2 and Crypto Options for Government
HPE Universal IoT Application
Communications Medium
Acess Device
Chiller
• Embedded VIA when LAN Internet Access Available
• Suite B option for government
• Embedded VIA and HPE 501 bridge when WLAN interface not available
• RAP with cellular when LAN/WLAN not available or accessible
• Edgeline with VIA when serial or analog/digital I/O, ModBus, or CAN
• Protocol converter and RAP for other control protocols
• FIPS 140-2 option
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management

fig.13.0_092816_iotremotemonitoring-wpa

Figure 13: Chiller Monitoring Diagram

Building Automation: Building Controller Monitoring

Objective

- Customer wants to reduce truck rolls by remotely accessing the building automation controller for log access and preventive maintenance

Challenges

- Machine may lack native VPN capability
- Access to local network forbidden by site owner and require cellular broadband
- Access to local network may be permitted but subnet may not have access to the Internet
- Government customers need FIPS 140-2 and Suite B

TABLE 6: BUILDING CONTROLLER MONITORING OPTIONS

Machine Capabilities	Local LAN Access	Local WLAN Access	No Local LAN/WLAN Access
VIA can be used, Ethernet port	VIA client, FIPS/Suite B option	VIA and HP 501 Bridge, FIPS/Suite B option	RAP with cellular modem, FIPS/Suite B option
VIA cannot be used, Ethernet port	RAP, FIPS/Suite B option	RAP, FIPS/Suite B option	RAP with cellular modem, FIPS/Suite B option
Serial port	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
Analog or digital I/O	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
Modbus or CAN	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and cellular modem
BACnet, LONWORKS, or other control protocol	Protocol converter and RAP, FIPS/Suite B option	Protocol converter and RAP, FIPS/Suite B option	Protocol converter and RAP with cellular modem, FIPS/Suite B option

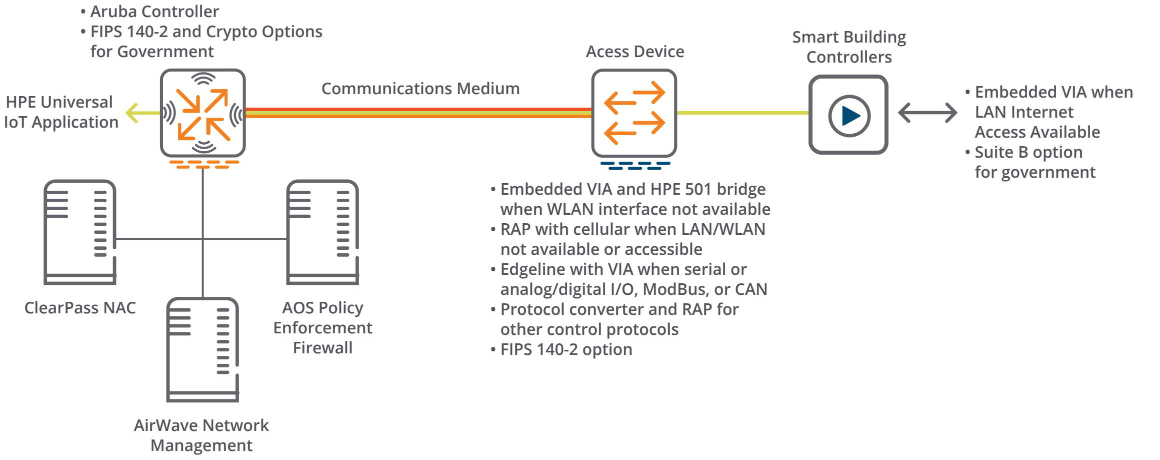

• Aruba Controller
• FIPS 140-2 and Crypto Options for Government
HPE Universal IoT Application
Communications Medium
Acess Device
Smart Building Controllers
• Embedded VIA when LAN Internet Access Available
• Suite B option for government
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management
• Embedded VIA and HPE 501 bridge when WLAN interface not available
• RAP with cellular when LAN/WLAN not available or accessible
• Edgeline with VIA when serial or analog/digital I/O, ModBus, or CAN
• Protocol converter and RAP for other control protocols
• FIPS 140-2 option

fig.14.0_092816_iotremotemonitoring-wpa

Figure 14: Building Controller Monitoring Diagram

Service Monitoring: Personnel Wayfinding and Tracking

Objective

- Customer wants to improve operational efficiency and reduce incorrect labor fees by using wayfinding to expeditiously guide service personnel to machines in need of service, reduce mean time to repair by automatically calling up service records and manuals when machines are approached, and validate service costs and labor utilization based on actual travel and on-site time

Challenges

- Large sites are difficult to navigate
- Service personnel may need to run application on personally owned smartphone or tablet
- Customer may have non-Aruba network infrastructure

TABLE 7: PERSONNEL WAYFINDING AND TRACKING MONITORING OPTIONS

Site Capabilities	Beacon Type	Beacon Interface	Client Type
Aruba WLAN deployed	Integrated in access point, battery, USB, Aruba Sensor	Aruba access point, Aruba Sensor	Meridian Client, Meridian SDK for 3rd party client
Non-Aruba WLAN deployed	Battery, USB, Aruba Sensor	Aruba Sensor	Meridian Client, Meridian SDK for 3rd party client

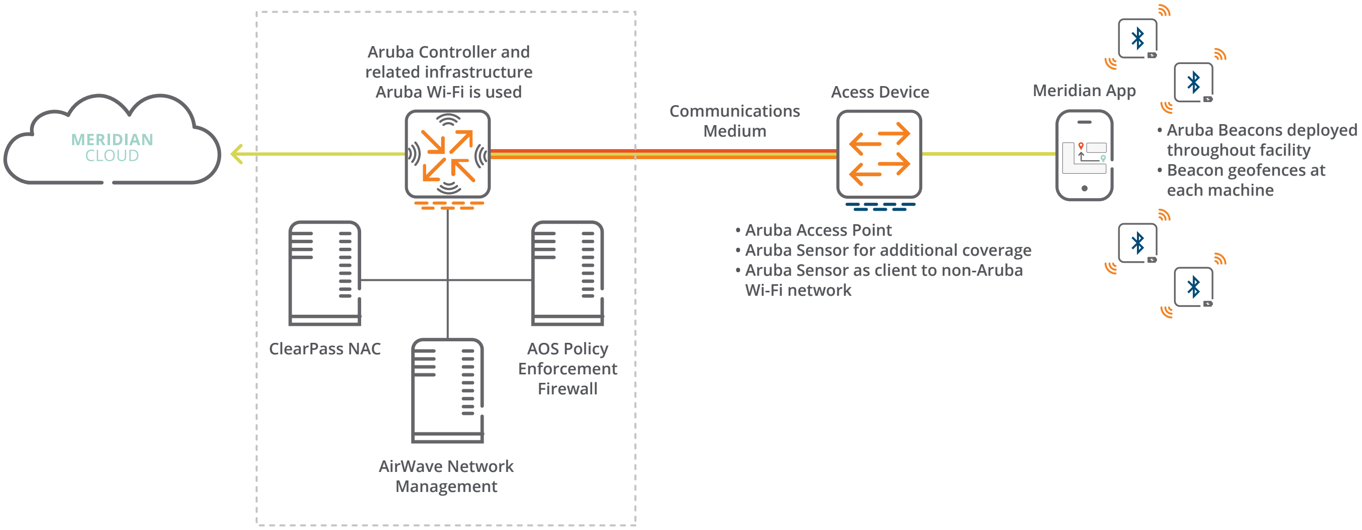

MERIDIAN CLOUD
Aruba Controller and related infrastructure Aruba Wi-Fi is used
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management
Communications Medium
Acess Device
Meridian App
• Aruba Beacons deployed throughout facility
• Beacon geofences at each machine
• Aruba Access Point
• Aruba Sensor for additional coverage
• Aruba Sensor as client to non-Aruba Wi-Fi network

fig.15.0_092816_iotremotemonitoring-wpa

Figure 15: Personnel Wayfinding and Tracking Monitoring Diagram

Industrial: Offshore Oil Platform Telemetry

Objective

- Customer wants to lower wide-area network costs and increase well-head productivity by locally processing data from >100,000 sensors at the platform before sending a summary of results to a remote data center

Challenges

- Local analytics requires data center-grade computing power and storage
- Rugged environmental conditions
- WAN expenses for large data transmissions
- Combination of analog and digital I/O
- Modbus and other protocols

TABLE 8: OFFSHORE OIL PLATFORM TELEMETRY MONITORING OPTIONS

Machine Capabilities	Local LAN Access	Local WLAN Access	No Local LAN/WLAN Access
Analog or digital I/O	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and broadband wireless or fiber optic connection
Modbus or CAN	Edgeline with VIA client	Edgeline with VIA client	Edgeline with VIA client and broadband wireless or fiber optic connection
ProfiBus, ProfiNet, or other control protocol	Protocol converter and Edgeline with VIA client	Protocol converter and Edgeline with VIA client	Protocol converter and Edgeline with VIA client and broadband wireless or fiber optic connection

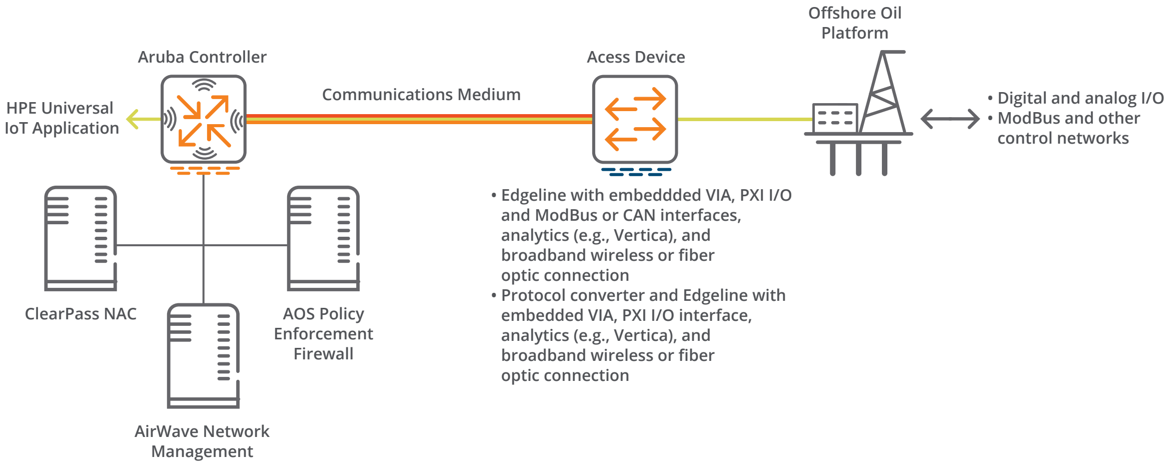

Offshore Oil Platform
Aruba Controller
Acess Device
Communications Medium
HPE Universal IoT Application
• Digital and analog I/O
• ModBus and other control networks
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management
• Edgeline with embeddded VIA, PXI I/O and ModBus or CAN interfaces, analytics (e.g., Vertica), and broadband wireless or fiber optic connection
• Protocol converter and Edgeline with embedded VIA, PXI I/O interface, analytics (e.g., Vertica), and broadband wireless or fiber optic connection

fig.16.0_092816_iotremotemonitoring-wpa

Figure 16: Offshore Oil Platform Telemetry Monitoring Diagram

CONCLUSION

No longer do companies need to isolate OT data for fear of expanding security vulnerabilities. Instead they can design and use secure remote access solutions to address both visibility and security, and unlock the true potential and economic value of the Internet of Things.

Secure connectivity solutions transform untrustworthy devices into trusted data sources. By securely delivering those data from remotely location IoT devices to analytics, machine learning, and business intelligence applications, Aruba helps improve efficiency, productivity, and customer/employee experiences.

REFERENCES

1. Frances Karamouzis, Ruby Jivan, and Sandra Notardonato, *Predicts 2016: The Rise of the Machine Leads to Obsolescence of Offshoring for Competitive Advantage*, Gartner, 4 December 2015
2. Tom Austin, Bettina Tratz-Ryan, Frances Karamouzis, Whit Andrews, and Alexander Linden, *Entering the Smart-Machine Age*, Gartner, 21 October 2015
3. Mike J. Walker, David W. Cearley, and Brian Burke, *Top 10 Strategic Technology Trends for 2016: Information of Everything*, Garter, 26 February 2016
4. Ruggero Contu and Earl Perkins, *How the Internet of Things Will Impact Cybersecurity*, Gartner, 26 April 2016
5. Bettina Tratz-Ryan and Pam Fitzpatrick, *Predicts 2016: The Internet of Things as an Enabler for Energy Efficiency and Sustainable Business Acumen*, Gartner, 21 March 2016
6. Colin Fletcher and Sanjit Ganguli, *Enhance IT Operations Management With IoT Derived Context and Data*, Gartner, 7 January 2016
7. John Girard, Eric Ahlm, and Jeremy D'Hoinne, *Market Guide for Enterprise Infrastructure VPNs*, Gartner, 8 March 2016
8. John Pescatore and Earl Perkins, *Don't Think Targeted Attacks Like Stuxnet Can't Hit You*, Gartner, 23 September 2010
9. http://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/#109482774b29

aruba
a Hewlett Packard
Enterprise company