SOLUTION OVERVIEW

aruba
a Hewlett Packard Enterprise company

Smart Digital Federal Government

Solutions to address today's work and operational challenges

The mission of Federal Government agencies leaves little room for error. Employees and contractors depend on a wide range of cloud and on-premises services brought on by new hybrid work requirements.

This digital acceleration has left Federal IT teams the challenging requirement to adapt network and security architecture for initiatives like work-from-home, return to office, and other cloud-enabled solutions.

As Federal IT teams adapt, connecting more users, devices, applications and locations than ever, the traditional human-driven approach to assuring great experiences and air-tight security may seem daunting. Automation is needed to reduce time-consuming network processes. Smart digital tools, leveraging IoT and other technologies, is key to improving operations and emergency management, equipment maintenance, logistics and tactical operations.

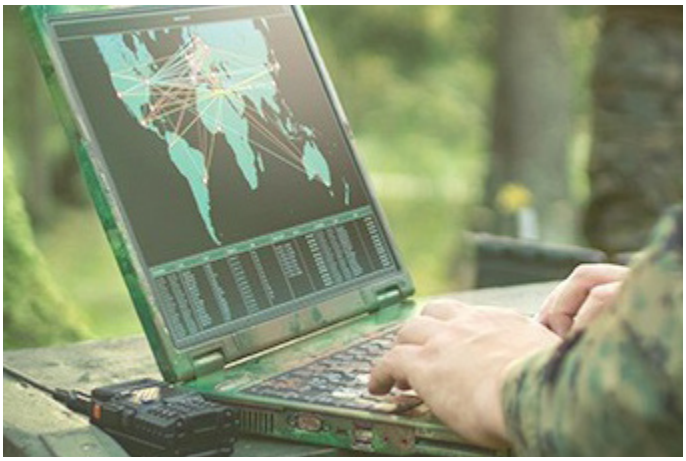
As Federal Government agencies look to change the way they serve citizens, customers, and employees, they are transforming their work practices and operations to do more. This transformation requires digital tools, data processing right where users and devices are, and leveraging artificial intelligence and machine learning to improve IT processes and drive outcomes.

As Federal Government looks to innovate, Aruba can help.

FEDERAL GOVERNMENT USE CASES

An adaptable and agile network supports use cases for today and the future.

- Always-on secure access to critical and classified services, on-premises or in the cloud (FedRAMP)
- Highly enabled mobile employees
- Always-on device and application connectivity
- Frictionless visitor check-in
- Analytics to understand employee and visitor location, physical distancing and contact tracing
- Quick deployment of remote or pop-up sites
- Support of data-demanding research projects
- Sensors to detect water levels, machine faults, earthquakes, or human temperatures
- Improve operations with robots, voice-commands, and driverless forklifts



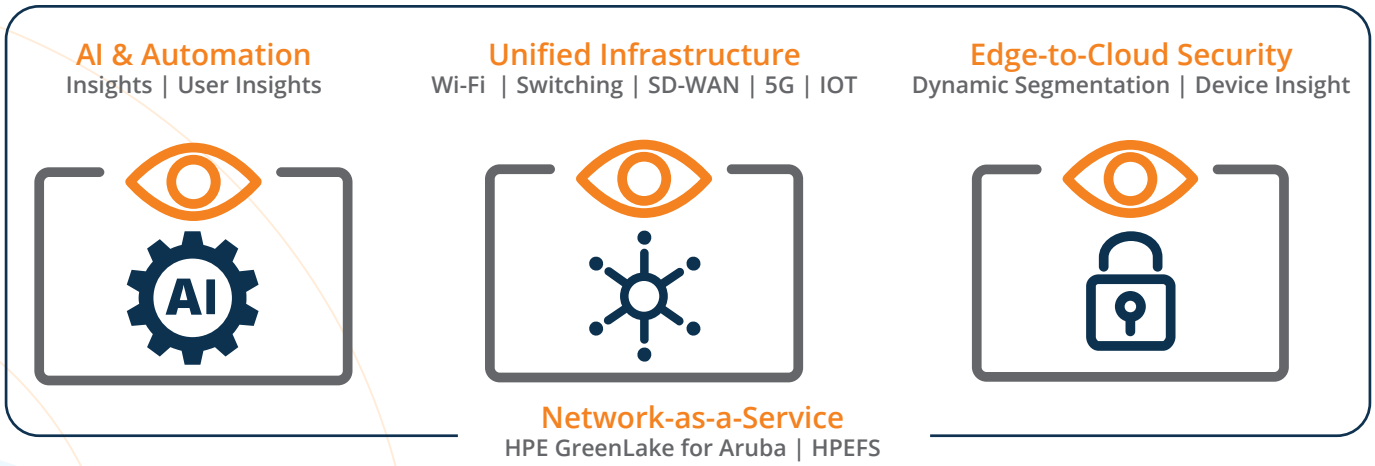
ARUBA'S FEDERAL GOVERNMENT SOLUTIONS

Aruba's solutions enable Federal Government to deliver critical services to their customers and improve operations. Agencies can deploy high-performance networking and security across any location – office spaces, courts, health departments , outdoor locations, and teleworker home offices. Aruba's Edge Services Platform (ESP) uniquely integrates management and policy enforcement across Wi-Fi, wired, and wide area networks (WAN) to right-size network infrastructure and ensure end-to-end mobility.

Aruba ESP is the industry's first AI-powered architecture designed to automate, unify and protect the edge for businesses of any size or type and includes attributes of Unified Infrastructure, Edge-to-Cloud Security with Zero Trust and SASE, AI Powered Operations (AIOps), and Flexible Consumption/Financing Models. These attributes are designed for the unique challenges facing federal government, including being able to adapt quickly for unknown future use cases and meet the secure networking needs of federal entities. A Unified Infrastructure provides a single management source for wired, wireless, & SD-Branch to facilitate any location. Zero-Trust Security ensures that all devices are profiled and correctly assigned network access. AIOps enable network automation, proactive problem resolution, and provides robust management tools for network operators.

KEY FEDERAL INSTALLATIONS

- Pentagon wireless & switching
- DHA LAN/WLAN Refresh Program
- WIN-T tactical deployment
- Navy NGEN NMCI Enterprise Mobility & shipboard CSfC WLAN
- USAF CITS/BITI program
- CDC
- DoE (multiple labs)
- DoJ: Executive Office of the U.S. Attorney (EOUSA)
- FTC WLAN Guest Networks and Network Authentication
- IRS WLAN Guest Networks and Network Authentication
- NASA WLAN Guest Networks and Network Authentication
- Veterans Affairs WLAN Guest Networks
- U.S. Air Force
- U.S. Army



UNIFIED INFRASTRUCTURE FOR ALWAYS-ON CONNECTIVITY

APPROVED PRODUCT LISTS
DODIN APL
NSA CSfC APL

Performance of the network, whether on-premises or in the cloud, must always deliver reliable connectivity and exceptional experiences. As mobility has shifted from supporting logistics to being a part of most aspects of service delivery, zero-downtime is paramount to omitting impacts to mission critical work. When agencies can rely on the network to perform at an optimal level, with consistent FIPS/TAA compliant infrastructure at all sites, it increases the ability to focus on customers and operations, not on how device connectivity might impact services.

Seamlessly connect employees or visitors to Wi-Fi

The first step to productivity or service delivery is ensuring network connectivity. Using a self-registration guest portal delivered by Aruba Central or Aruba ClearPass, you can ensure a seamless guest onboarding experience. Employees, contractors, or customers will appreciate the ease of connecting and you'll gain immediate insights. With data gathered at the point of entry, rather than after an individual initiates a connection, new data streams on traffic patterns and network usage can be delivered. Building operations can position digital or other signage to communicate while network insights and usage can help IT understand where there might be connectivity issues so that network alterations can be made to deliver the best experiences.

Delivery always-on mobility with high-performance Wi-Fi

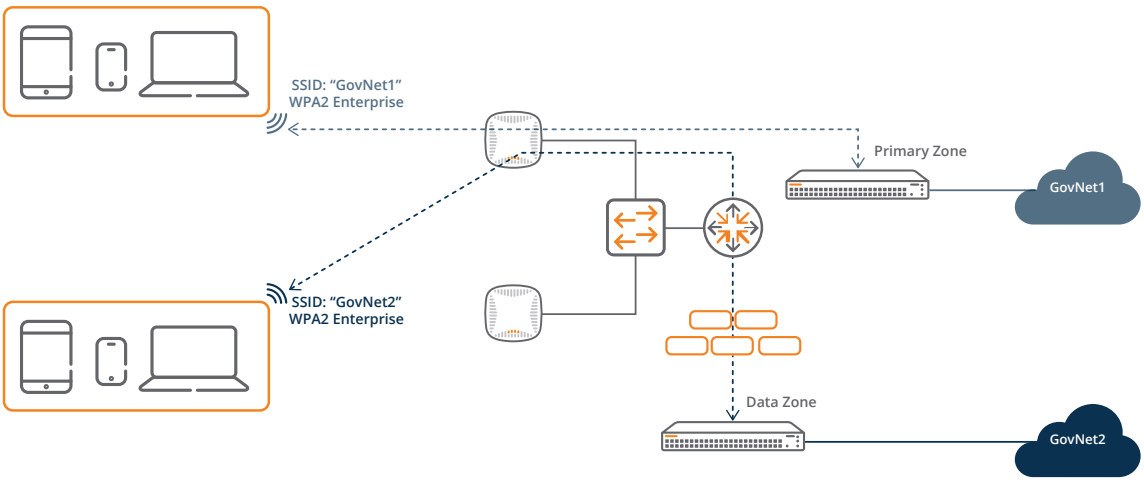
Aruba's Wi-Fi 6 and Wi-Fi 6E infrastructure is designed to support hundreds of devices simultaneously without impacting Wi-Fi quality. Employees, contractors, visitors, or even Wi-Fi enabled robotics can move through a facility with consistently great performance. Critical applications can be prioritized so they can perform at their peak, not impacting services or visitor experiences. These always-on experiences are powered by Aruba technology that auto-adapts to changing environments and applications, ensuring uninterrupted operation. Technologies include ClientMatch, that optimizes roaming performance; AppRF that optimizes the performance of critical applications such as record systems; AirMatch enhances and adapts radio performance; and Air Slice manages bandwidth allocation to enhance specific applications. Hitless upgrades and hitless failover to support C2 and critical missions with zero downtime, ensure that the network can stay current with the latest security updates, tolerate faults, and be available whenever needed. No test interruptions, no lost data, no dropped connections or transactions.

AUTHORIZATION TO OPERATE

- Defense Information Systems Agency (DISA)
- Naval Nuclear Propulsion Information (NNPI)
- U.S. Air Force Combat Information Transport System (CITS)
- U.S. Air Force Concept of Operations (CONOPS)
- U.S. Army Enterprise
- U.S. Army Warfighter Information Network - Tactical (WIN-T)
- U.S. Marine Corps
- U.S. Navy Next Generation Enterprise Network (NGEN)

Send your non-public facing workers home

Federal Government has traditionally been a worksite dependent industry – but with the need to follow social distancing and self-quarantine guidelines, it has become essential to enable workers to be productive at home. Aruba Remote Access Points (RAPs) extend the same network services and security policy to an employee's home, just as if they were in an office. Use the same authentication credentials to gain access and dynamically apply and enforce access policies based on the user's role.



Simply enable multi-classification networks

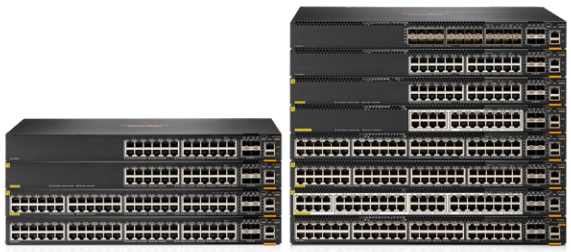
Aruba's centralized architecture makes it possible to provide additional separation and security by designing and creating separate "zones" for each separation instance. Examples where this kind of separation is needed includes Federal unclassified networks vs classified networks, separate operating networks (unclassified or classified) within a single environment, or department/contractor/visitor/guest access. Aruba Multizone enables administration of multiple secure access control classifications from a single access point to terminate on physically diverse controllers. This feature eliminates frequency challenges, improves security, and reduces physical cabling and access points required.

Expanded services and coverage.

Many agencies have the need to deploy pop-up facilities or extend their indoor services outside. These environments can be challenging, but the primary network can easily – and securely – extend outside with the same connectivity reliability and security posture at the main facility. Additionally, with the use of Aruba's Zero-Touch Provisioning, a network can be installed and configured without IT being physically involved.

Smart switches from edge to core.

Mobility enabled wireless solutions is a priority and the wired network plays a critical role to support a variety of wired only and IoT use cases. Multi-gigabit switches support high density APs and new IoT devices, delivering enhanced performance and improved security by segmenting traffic.

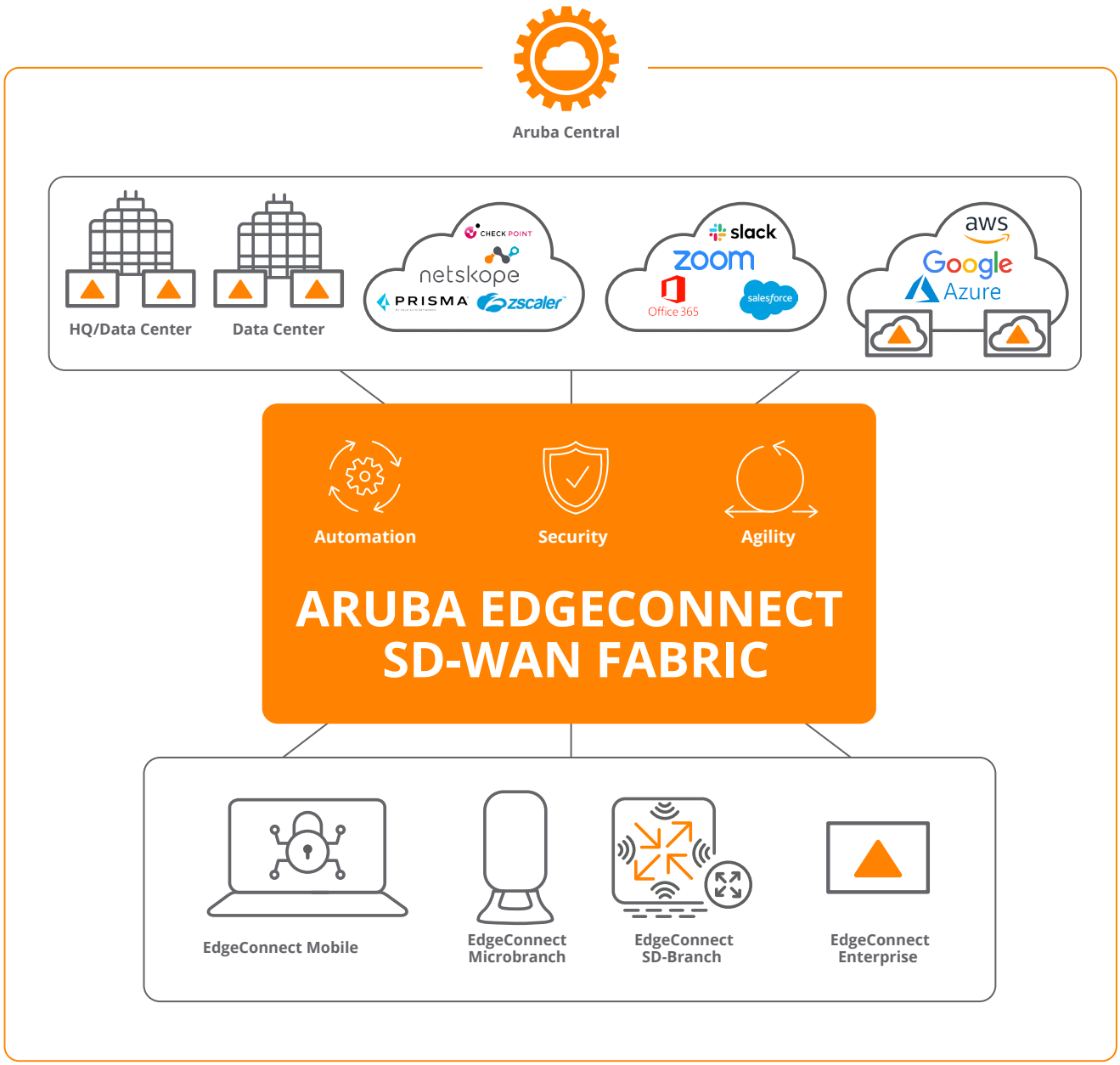


In addition to Smart Rate PoE, Aruba provides auto-negotiation between switch and access point to determine the needed throughput for devices and applications, ensuring great performance. The Aruba AOS-CX operating system includes many features including intuitive software-defined management tools, built-in analytics, and programmable scripting that can deliver insights into network and system performance to help IT stay ahead of issues. Similar to the wireless network, upgrades and updates can also be easily enabled, reversed, and changed without impacting the network or the customers, warehouse workers, and devices that rely on it always on access. Aruba switches deliver the performance and actionable insights IT administrators need to handle the massive amounts of data now being generated at the network edge.

Business-driven, Advanced SD-WAN

By deploying the Aruba EdgeConnect Enterprise SD-WAN platform, application performance, security and routing are dictated by top-down business policies, not bottoms-up technology constraints. Federal IT ensures that the priorities of their business are always reflected in the way the network delivers applications to users. Business intent dictates application QoS and security policies. Business intent also drives the way network resources are applied to match the business criticality of every application.

The Aruba EdgeConnect Enterprise SD-WAN architectural model utilizes virtual WAN overlays based on business requirements (business intent overlays) for every class of application. Once overlays and their associated policies have been defined via Aruba Orchestrator, configurations are pushed to all sites across the network. At that point, traffic handling is fully automated to optimally route — or steer — applications based on pre-configured parameters. Aruba EdgeConnect Enterprise continuously learns about any network condition changes and automatically adapts traffic handling to maintain continuous compliance to application QoS and security application QoS and security policies.



Architecture of the Aruba EdgeConnect SD-WAN Fabric

ZERO-TRUST SECURITY FROM END-TO-END

CERTIFICATIONS
- FIPS 140-2
- Common Criteria
- DODIN APL
- UNH IPv6/USGv6

No industry has more unique security requirements than the U.S. federal government. Commercial and enterprise organizations are adopting the concept of Zero-Trust Security – trust no one or no thing – and this has been the longstanding perspective for sensitive government missions. Most traditional security solutions focus on securing the perimeter by detecting known attacks and malware by their patterns or signatures. Yet never before seen threats, mutated threats, and advanced targeted attacks can often bypass these types of traditional solutions.

Today's innovations rely on IoT and cloud, amplifying the need for Zero Trust Security. Aruba's networking solutions have successfully designed and maintained hundreds of large government deployments including unclassified and classified environments. Solutions include profiling, posturing, and access control required by high-security agencies including the Department of Defense, Department of Homeland Security, the U.S. Air Force, and the Pentagon. Aruba's advanced suite of cryptographic protocols enable commercially available mobile devices to be used for unclassified, confidential, and classified network access, whether inside trusted government facilities or in hotel rooms.

"Zero Trust" network access

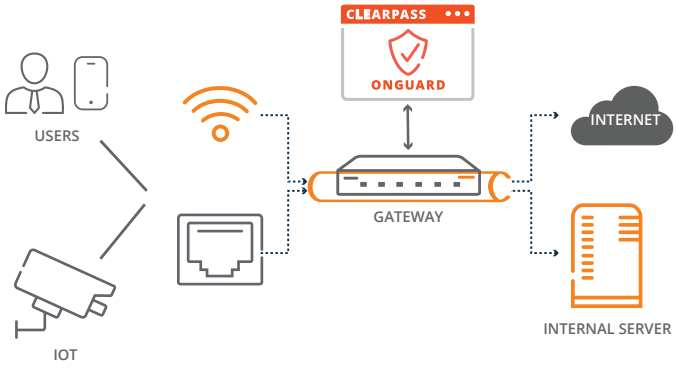
Once devices are identified, ClearPass Policy Manager uses role-based policies and profiles, authenticates, authorizes, and tightly manages network access using granular, policy-based access controls. Users and devices have restricted access across network domains to only those network, IT, and application resources for which they have been approved. Every application flow and every user engagement is treated individually, authenticated and encrypted.

FedRAMP AUTHORIZATION

Aruba Central is the first unified network management solution to be FedRAMP authorized by the Federal Risk and Authorization Management Program (FedRAMP).

Separate employee, IoT and visitor traffic

Various agencies can feel confident in supporting a highly-secure use cases and applications without reducing the security posture. Aruba's Dynamic Segmentation delivers the micro-segmentation needed for traffic on wired, wireless and the WAN using granular user/device/connectivity information. Policies are carried across the network end-to-end, ensuring that sensitive government information can only be accessed by authorized personnel while keeping visitor network traffic kept separate, regardless of the location of the user or device or the switch port carrying the traffic.



Mobile and IoT Friendly Point-of-Access Firewall

As networks become the catalyst for digital transformation, traditional perimeter security defenses no longer suffice. Mobile and IoT devices are being connected by employees, partners, customers and guests everywhere within an organization, driving the need for improved segmentation of traffic based on specific IT access permissions. No longer are standard security firewall rules and physical network configuration based on IP addresses adequate. Organizations now require edge-based protection that is dynamically enforced regardless of user role, device type or location. Enforcing firewall rules at the point of connectivity provides a simple way to control user and IoT access anywhere within an environment and eliminates the cost and complexity of configuring VLANs, ACLs, and subnets at every hop in the network.

Aruba pioneered the use of a comprehensive role-based access control solution called the Policy Enforcement Firewall (PEF) that specifically helps solve this problem. This proven technology is the only user- and device-centric firewall that provides a "zero trust" boundary at the point of access and carries the Cyber Catalyst℠ by Marsh designation for reducing risk.

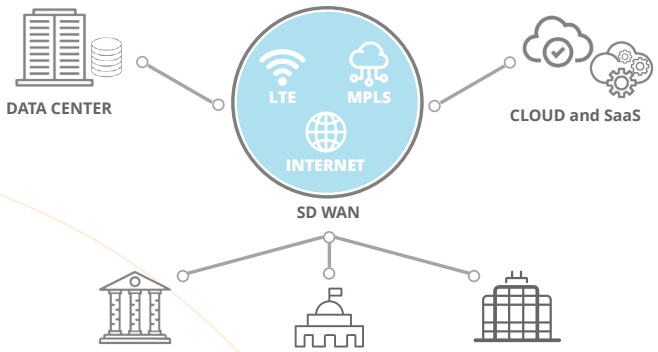
Meet and Exceed PCI Requirements

Aruba provides multiple levels of protection to allow government agencies who handle purchasing transactions to meet and even exceed PCI requirements. Strong authentication and authorization, WIPs, role-based access controls and advanced encryption ensure adherence to the stringent mandates of PCI DSS, even in the most challenging environments. Features such as the stateful Policy Enforcement Firewall™ (PEF™) allows organizations to securely enable customers, employees and credit card transactions to share the same network and feel confident that data is safe.

ACT QUICKLY WITH INTUITIVE AI-POWERED MANAGEMENT TOOLS

The amount of data generated at a civilian or military agency can challenge the very fabric of network operations. Aruba's Edge Services Platform (Aruba ESP) includes assurance and orchestration features to maximize up-time, optimize user experiences, and reduce the time to

Optimize remote site visibility and management



The continued migration of applications and infrastructure to the cloud, and the increase of remote workers are fueling the need to transform traditional wide area network (WAN) and security architectures. Aruba and Silver Peak are taking an end-to-end approach to help government agencies modernize and secure their cloud architectures while significantly reducing costs. Software-defined WAN is a new way to orchestrate routing over wide geographical areas with any mix of WAN connections - like broadband, MPLS and LTE. It improves your Total Cost of Ownership and makes the WAN much easier to deploy and manage. IT can remotely monitor, manage, and troubleshoot the wired, wireless, and SD-WAN infrastructure from anywhere. Aruba's SD-Branch solutions addresses LAN and WAN complexity with a single-pane-of-glass providing unified management, AIOps, and security across wired, wireless, and SD-WAN.

Assurances for optimized network and mission critical application performance

Mobile devices, IoT, VoIP, and UCC have become mission critical for the digital business and must be always-on with real-time access to applications and network services. But traditional methods of performance monitoring need to adapt to current deployment and application needs. One way to ensure those who are working directly with customers receive a quality network experience is by using Aruba User Experience Insight (UXI). Aruba UXI provides user and IoT device application assurance and rapid troubleshooting through easy-to-deploy sensors and a user-friendly cloud-based console. By simulating end-user activities with admin-defined frequency, UXI sensors continuously perform user-centric application testing, allowing resolution of issues before a service ticket is opened. These powerful tools bring much-needed help to enable already overwhelmed IT staff to take necessary action and stay ahead of issues.

LEVERAGE ANALYTICS AND LOCATION FOR IMPROVED EXPERIENCES AND OPERATIONS

High-performing networks should do more than provide secure connectivity – they should leverage additional solutions to meet staff and visitor expectations, and drive better outcomes. Ecosystem partner solutions can automatically gather data from multiple sources - access points, people counters, mobile devices, and other IoT – and turn them into insights that can be leveraged by many business units. These solutions allow civilian and military agencies the opportunity to understand how users leverage the network, where and how they move through physical spaces, and in some instances, offer pre-emptive intelligence to fix machinery before it breaks.

Access Points as IoT Platforms

We are accustomed to thinking about Wi-Fi access points in the context of secure wireless network access, and for many years that was their primary function. Not so today. Aruba Wi-Fi 6 access points include radios for wayfinding, location tracking, sensor monitoring, gun-shot detection, and a multitude of other uses cases. These capabilities transform Aruba access points into secure, multi-purpose communication systems, eliminating the need for additional gateways, reducing cost, and simplifying IT operations.

With some of the industry's best technology partners and app developers, Aruba is helping to deliver innovative solutions that connect the dots between today's business and IT priorities. These solutions provide tested and proven integrations to support everything from staff communications, surveillance, first responder communications to predictive machine maintenance. To learn more, visit our list of ArubaEdge Partners.

A PARTNER YOU CAN TRUST

Aruba's mission is to harness and secure data at the edge, enabling Federal Government agencies of all sizes to deliver mobility-centric networks, security and management services that are tailored to the needs of their civilian and military agencies. Aruba delivers on performance, providing the confidence that infrastructure investments will scale to meet the simultaneous demands of all operations will helping departments meet their goals. With Aruba, agencies have the flexibility to choose the infrastructure and network management approach that best fits their mission.

Learn more by contacting your local Aruba salesperson or reseller today.

CONTRACT PURCHASING

- SEWP
- EIS

SO_SmartDigitalFederalGovernment_RVK_073022 a00108199enw

Contact us at www.arubanetworks.com/contact