aruba
a Hewlett Packard Enterprise company

TECH BRIEF

CLOUD DATA PRIVACY AND PROTECTION

Aruba Central

ARUBA AND PRIVACY

Aruba, a Hewlett Packard Enterprise company, respects the privacy of customers, employees, partners and other stakeholders. Ensuring privacy is a core value of Aruba and is integral to the way we do business. We are committed to accountability and seek to maintain a robust privacy program globally.

With investments in cloud-based networking increasing throughout the 2020s[1], data protection and data privacy are increasingly important when designing and deploying network architecture. Aruba Central and the network infrastructure it manages are engineered to faciliate strict compliance with the requirements of international and industry standards bodies.

WHAT IS ARUBA CENTRAL?

Aruba Central, the single pane of glass for Aruba's Edge Services Platform (Aruba ESP), is an AI-powered network management, operations, analytics, and security command center for Aruba's cloud-based networking solutions. Performance, diagnostics, and analytics are enhanced using a modern, microservices-based cloud architecture designed with scalability and resiliency in mind.

Geographic Availability, Scalability, and Resiliency

Aruba Central maintains points of presence (POPs) worldwide, enabling the segmentation of customer information based on region.

KEY FEATURES

- Role-based access control (RBAC)
- Native Aruba hardware authentication
- Ethical Hacking by Aruba Threat Labs
- Deployed in AWS, Azure, and private clusters
- FedRAMP Authorized (U.S. market only)

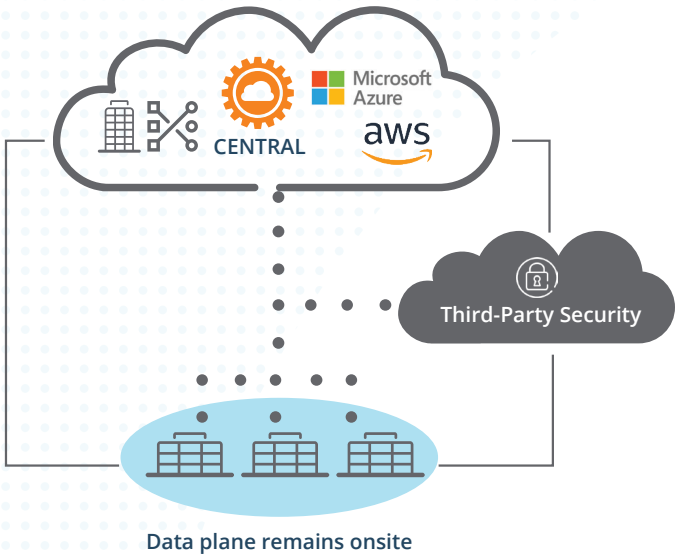

Figure 1: Cloud deployment mockup

[1] Hybrid Workplace Report, July 2020, https://www.arubanetworks.com/assets/eo/Hybrid-Workplace-Report.pdf

ARUBA SECURE INFRASTRUCTURE

In order to protect user data, Aruba Central and managed network infrastructure like access points, switches, gateways, and sensors are designed with advanced security protections to provide role-based access control, device impersonation prevention, intrusion prevention and more.

Role-based Access Control

Aruba Central management consoles can be federated with identity provider (IDP) solutions for SSO. This allows customers to use standard authentication and password policies to enforce requirements for users. Aruba Central then enforce role-based management privileges based on each users' permissions.

Security Audits

Access to Aruba Central by your IT administrators is logged, including CLI sessions, saved changes, login and logout events. This usage data can then be exported and used in support of internal audit processes.

Data Encryption

All data in transit to and from Aruba Central is encrypted end-to-end using at least TLS 1.2. This includes connectivity to Aruba Central, on-premises network devices, and management interfaces accessed by Aruba employees (e.g. support services). Persistent AWS data stores are encrypted using at least AES-256.

Native Aruba Hardware Authentication

Network devices can be automatically added to Aruba Central management using Aruba Activate. Aruba Activate correlates network devices with shipment orders, Point of Sale (POS) orders, customer name, and manufacturing records to place devices into a customer's Aruba Central console. Additionally, Trusted Platform Module (TPM) technology is used by Aruba Activate to validate the secure boot of an onsite device identity before allowing the device on the network.

Aruba Activate provides:

- Zero-touch provisioning (ZTP) for all Aruba network devices (APs, switches, and gateways)
- Device and firmware inventory
- Device ownership management
- Correlation for network devices with shipment orders, Point of Sale (POS) orders, customer name, and manufacturing records to place devices into a customer's Aruba Central console

Learn more about Aruba Activate here:
https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/EntryId/10838/Default.aspx

COMPLIANCE PROGRAMS

FedRAMP Authorized

Aruba Central is currently fully FedRAMP authorized to enable U.S. federal agencies to deploy Aruba Central to securely manage and maintain their Aruba infrastructure. This is based on NIST 800.53 control framework and third party audit. To confirm eligibility, please visit:
https://connect.arubanetworks.com/FedRAMP_Contact-us

For more information about FedRAMP, please visit
https://www.arubanetworks.com/faq/what-is-fedramp/.

PCI, HIPAA and Other Regulations

In order to help enterprises secure IT applications and infrastructure to meet functional and regulatory requirements, Aruba networks can be architected with multiple levels of protection. Learn more about how Aruba Central and other solutions can be designed to support retail, healthcare and government requirements:
https://www.arubanetworks.com/regulatory-compliance

SECURITY OPERATIONS (CLOUDOPS/SECOPS)

In addition to being hosted on one of the most secure cloud platforms available on the market, Aruba Central is continuously monitored and tested for security threats, using automated tools and people resources from the Aruba SecOps team and independent third parties. SecOps runs in-house tools, defines procedures, and performs monitoring of Aruba Central. SecOps works closely with the HPE Cyber Defense Center (CDC) and the Aruba Threat Labs to perform advanced threat detection.

Security Framework

Aruba Central's security framework has been developed using policies and procedures promulgated by HPE Cyber Security Governance, which is based on industry standards such as NIST 800.53 and ISO 27000. Controls are implemented in various categories such as access control, change management, infrastructure security, communication security, vulnerability management, patch management, backups, personnel security, and physical security.

Access to Management Functions

An Aruba employee's access to management interfaces is managed using single sign-on (SSO) with two-factor authentication (2FA). Access is granted on a "least privileged principle" and only as needed to perform job duties. In addition, all Aruba employees undergo background checks and sign Non-Disclosure Agreements (NDAs) before being granted access to the environment. Actions performed on management interfaces are logged and the logs are regularly reviewed.

Independent Vulnerability Assessments

Third party penetration tests are performed to identify and close any potential vulnerabilities. Third party assessments are also performed for security compliance attestations.

Additional Testing and Ethical Hacking

Aruba Threat Labs, part of Aruba's CTO office, exists to find and eliminate security vulnerabilities in Aruba products. This includes a talented group of information security professionals who conduct additional hardware, software, and cloud security assessments, perform red team operations, exercise applied security research, promote and drive security into the software development lifecycle (SDLC) of our solutions, manage a bug bounty program, and coordinate with Aruba Security Incident Response Team (Aruba-SIRT) and HPE's Fusion Center.

PROVEN CLOUD HOSTING PROVIDERS

AWS and Azure, as Aruba Central's cloud hosting providers, participate in extensive audit and certification programs to help maintain security and compliance in the data center. They provide Aruba with SOC2 Type 2 audit reports and extensive information on other compliance activities. These materials are also available directly to other customers. Aruba reviews these certifications on a regular basis to confirm that any identified vulnerabilities are resolved.

These cloud providers are available globally and can be segmented by governments, industry, geographic region and more.

Cloud Providers Compliance and Security Programs

The cloud providers Compliance Programs and documents provide Aruba with validation for the robust controls in place. Those could be found at https://aws.amazon.com/compliance/programs/ and https://docs.microsoft.com/en-us/azure/compliance/.

The service providers Security team provides Aruba with information on their security posture and back up documents: https://aws.amazon.com/security/ and https://docs.microsoft.com/en-us/azure/security/

RESOURCES

Please see below for additional information about Aruba's privacy policy, compliance, and terms and conditions:

- Blog: Addressing Cloud Security Challenges, Part 1: https://blogs.arubanetworks.com/Solutions/addressing-cloud-security-challenges-in-aruba-central-secure-by-design/
- Blog: Addressing Cloud Security Challenges, Part 2: https://blogs.arubanetworks.com/solutions/cloud/addressing-cloud-security-challenges-in-aruba-central-data-security/
- Blog: Aruba's Security CTO on the Future of Cloud Security: https://blogs.arubanetworks.com/solutions/arubas-security-cto-on-the-future-of-cloud-security/
- Aruba Data Privacy Overview and Commitments: https://www.arubanetworks.com/dataprivacy/
- Aruba GDPR White Paper: https://www.arubanetworks.com/assets/wp/WP_SecuritySolutionsGDPR.pdf
- Aruba Retail, Healthcare, and Federal Compliance: https://www.arubanetworks.com/regulatory-compliance/
- Aruba PCI Compliance White Paper: https://www.arubanetworks.com/assets/wp/WP_PCIDSS.pdf

- Aruba Central Terms and Conditions: https://www.arubanetworks.com/products/networking/management/central/terms-conditions/
- HPE Privacy Policy: https://www.hpe.com/us/en/legal/privacy.html
- NIST Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Cloud Security Alliance Registry: https://cloudsecurityalliance.org/star/registry/aruba-a-hpe-company/
- HPE Security Consulting Services: https://www.hpe.com/us/en/services/consulting/security.html

TB_CloudDataPrivacyAndProtection_SK_012523 a00105609enw

Contact us at www.arubanetworks.com/contact