PRODUCT DATA SHEET

SUPPLEMENTS THE HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

	Aruba ClearPass Device Insight
Aruba* performs the following services:	Aruba ClearPass Device Insight (CPDI) provides a full spectrum of visibility across the network to understand the context for connected devices. Contextual information may include device type, vendor, hardware version, and behavior, including applications and resources accessed. CPDI uses machine learning to better recognize devices across the network. CPDI can provide this information to ClearPass Policy Manager or through Aruba Central to attach and enforce security and compliance to each end point device. Data collectors are available as a hardware appliance or a virtual appliance. Collected data is provided to the Aruba Central cloud environment for matching to known devices and creating new classes of devices.
Customer Personal Data:	Data collected as part of CPDI includes: MAC OUI (Media Access Control, Organizationally Unique Identifier) DHCP (Dynamic Host Configuration Protocol) • DORA Options (Discover, Offer, Response, Acknowledge) o DHCP Option 12 – Host Name • DHCP Option 50 – Address Request • DHCP Option 55 – Parameter List • DHCP Option 60 – PXE Server ID User Agent Information including information for all applications SNMP (Simple Network Management Protocol) based on configuration NMAP (Network Mapped) based on configuration • Open Ports • Banner Information SPAN Port • Communication Protocols • Applications accessed • Destination IP and port mappings • Destination URL information • Domain name lookups • SNI information WMI (Windows Management Instrumentation) • Operating System information • Service pack information CDP/LLDP (Cisco Discovery Protocol/Link Layer Discovery Protocol) • Discovery of neighbor devices via seed switch discovery • CAM and ARP table dump from Layer 2/Layer 3 devices
Data subjects to whom Customer Personal Data pertains are:	Customer's client / end-user / employee / contractor and temporary worker / visitor

With respect to Customer Personal Data, Customer is acting as:	Controller
Aruba shall process Customer Personal Data only as follows:	**Provisioning Services:** The information gathered and stored by the product is the minimum required to ensure secure access to the portal, and essential to performing its function. All session logs about a user will be automatically purged after 90 days. **Support Services:** Access to customer environment and data for troubleshooting is provided to Aruba support services based on customer agreements and permissions. **Device Insight Services:** Contextual information on end point devices is gathered at the data collector and compared against previously defined devices to determine the nature of the device. If the device is not matched, new device information is reviewed and added to Aruba's defined device characteristics database to better identify device types.

*Aruba, a Hewlett Packard Enterprise company, is referred throughout this document as Aruba

	CPDI Information within Aruba Central Clusters
Security and Encryption:	**Product Security Features:** • **Physical Security:** Aruba Central is hosted in the most widely adopted IaaS platform-Amazon Web Services (AWS) that offers the most comprehensive security and compliance features. AWS has put in place security measures around all critical areas including perimeter, infrastructure, data and environment layers. • **Network Security:** Our network security ensures that the physical and virtual network on which the application and data resides is secure. We use services and tools that the IaaS provider offers and some 3rd party solutions to make sure our production environment is as secure as it can be from external threats and internal vulnerabilities. Aruba operates separate instances of internal and production environments. The internal environment is focused on development and testing, while the production environment is solely reserved for our customers. Having this physical and logical separation of our production environment from other running instances helps us offer the best quality software deployment to our customers and ensures their data is always confined to one environment. • **Application Architecture and Security:** All traffic that is exchanged between the Central application and the outside world is done using HTTPS over SSL. All traffic flow is encrypted using AES encryption technology. Different application tiers such as web, app and database are designed to operate in a whitelist framework. Only necessary and required communication paths are allowed between tiers. Each instance within a tier is protected by firewall rules to prevent any unauthorized or malicious access. • **Data Security:** All data exchange between the application and devices and users happens using HTTPs. Data at rest is encrypted and stored. Data backup occurs on a regular basis and backup data is stored in

a redundant manner. From an organization perspective, we have a DevOps team that manages all security and operational aspects of the app.

- **Geographic Availability:**

  Aruba Central is available in multiple locations worldwide, allowing customers to choose in which region to establish an account. Many factors can influence this decision. For example, an organization may require all data to reside in a given region or impose regulatory restrictions on how data can be processed and stored.

  Aruba Central is deployed on clusters in selected Amazon Web Services (AWS) Data Centers, with AWS providing the compute and storage infrastructure. The following table provides a detailed listing of Aruba Central Clusters and the supporting AWS Regions:

ARUBA CENTRAL CLUSTER	AWS REGION (City where Cluster is based)	SIGN UP URL
US-2	US West (Oregon), us-west-2	https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/
EU-1	EU (Frankfurt), eu-central-1	https://portal-eu.central.arubanetworks.com/signup

Aruba Central's Cloud Platform is a global, multi-tenant application where all data is stored based on a tenant ID that prevents any given customer from accessing the data associated with other customers. All data is indexed based on the tenant ID and cannot be cross-proliferated in any part of the application. Data for each customer is retained for 90 days. Customers will also have the option to delete data from the UI and back-end data stores. Some of this data is also used for machine learning modeling. The data used for machine learning models will be deleted after 90 days, except for the sample trained model that will be retained for a longer period of time.

Third Party Security Certifications:	None
Privacy-Specific Certifications:	None

(rev. 06//30/2020)