PRODUCT DATA SHEET

SUPPLEMENTS THE HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

	Aruba ClearPass
Aruba* performs the following Services:	Services provides network access control (NAC) to secure wired, wireless, and virtual private network connections. It is an "on premise" solution that runs in the end users' networks.
Customer Personal Data	Data collected includes: • MAC addresses • IP addresses • Connection information (start time, end time, data transferred) • Usernames • Passwords • Email addresses • Mobile phone numbers • Endpoint Operating System (OS) profiling information • Web browser information • Social network or cloud-based login service user profiles • Installed/running endpoint applications • Information such as group membership or authorization lists obtained through external device queries
Data subjects to whom Customer Personal Data pertains are	Customer's client /end user /employee /contractor and temporary worker
With respect to Customer Personal Data, Customer is acting as	Controller
Aruba shall process Customer Personal Data only as follows:	Aruba and its affiliates will (i) have access to customer personal data hosted in Aruba's VPC as part of the proof of concept services, and (ii) during the provision of support services through the receipt of data dumps or remote access to customer systems. **Support Services:** Aruba TAC CRM is certified compliant with the highest independent, international, industry-accepted privacy standards. **Skyhook Services:** Limited ClearPass Extensions may require the use of Skyhook Service to broker communication between client and external cloud hosted services. Processing is offered as a service only to customer who accept the Aruba SaaS agreement to register for the Skyhook service with the Extension.

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

	Aruba ClearPass
Security and encryption	**Product**: The product itself is a security product used to control network access on customer networks. Access controls are defined by the customer security policy and requirements. • All data is stored within an AES128-bit encrypted database within the access-controlled management interface of the product. • There is a SIRT group that follows security advisories for externally reported vulnerabilities, including 3rd party open source code, as well as internally identified issues. • Security updates are regularly released in a timely manner. **Technical Security features:** • The product uses firewall to only open specific network ports that need to be open for product usage • All credentials are stored in encrypted format • Product minimizes programs and processes running as root
Third Party Security Certifications:	Common Criteria validated against CPP_ND_V1.0 and PP_NDCPP_APP_AUTHSVR_EP_V1.0 (VID#10814) FIPS140-2 Level 1 certificate #2577
Privacy-specific certifications:	None today