PRODUCT DATA SHEET

SUPPLEMENTS THE HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

	Aruba Introspect
Aruba* performs the following Services:	Services provide user and entity behavioral analytics. This is a security solution that helps customers detect intrusions into their network from internal and external threat actors. It detects attacks by spotting small changes in behavior that are often indicative of attacks that have evaded traditional security defenses. It is an "on premise" solution that runs in the end users' networks.
Customer Personal Data	Data collected includes data related to: • Network activity behavior of customer end users of customer network including applications used, and data exchanged by internet facing/internal facing usage • Data exchanged by internet-facing and/or internal-facing usage includes, but is not limited to: • Contact Information: names, email addresses and phone numbers • System Asset/Usage Device Information: IP address and tracking/analytics data • Tracking/Analytic Information: IP addresses.
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. **Proof of Concept Services:** the data is deleted when the compute instance is deleted. AWS does not retain a copy of the data but has the ability to access personal data while the instance is running. **Support Services:** Aruba TAC CRM is certified compliant with the highest independent, international, industry-accepted privacy standards.

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

	Aruba Introspect
Security and encryption	**Product Security Features:** the product is itself a security product as it helps customers detect intrusions into their network from internal and external threat actors. The product has certain security features. These include: Organization security features: • Access control is implemented at various levels so only specific individuals have access to perform their job functions • There is a SIRT group that follows security advisories found internally, reported externally and responds diligently • Security updates to products are provided on a regular and 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 **Obfuscating Personally Identifiable Information (PII):** IntroSpect stores and displays a user's PII, such as a user's full name and department, in clear text. For privacy reasons, it is sometimes necessary to obfuscate a user's PII. For example, a help desk person should not be able to see a user's PII, but a senior threat investigator should. IntroSpect 2.2 and later enables obfuscation of PII for an analyst whose role is assigned as an "Obfuscated Analyst". An obfuscated analyst sees user Jane Doe as randomized set of characters, such as *aaxxbbee*, instead of *Jane Doe* and cannot correlate this randomized set of characters to Jane Doe. In contrast, a "Senior Analyst", does not have Jane Doe's PII obfuscated and can see the user as *Jane Doe*. **Proof of Concept Services:** AWS security standards. Access to the customer instance is limited to Aruba personnel supporting the proof of concept services. All access is logged in an audit trail and can be provided to the customer if required. **Aruba Security Measures:** The support services used to support Introspect customers is provided by the Technical Assistance Group (TAC) within Aruba business unit. Aruba implements and maintains physical, technical and organizational security measures set out in to protect Customer Personal Data and Business Contact Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. Only where necessary to provide the Services, Aruba will provide its affiliates and subcontractors with access to Customer Personal Data.
Third Party Security Certifications:	None today
Privacy-specific certifications:	None today

3333 Scott Blvd. | Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com