HPE Aruba Networking IntroSpect

Annex II: Description of the processing

1.	Description of processing	Services provide user and entity behavioral analytics. This is a security solution that helps Controller detect into their network from internal and external threats. 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-premises" solution that runs in the Controller's networks. Processor and its affiliates will (i) have access to Controller personal data hosted in Processor's HPE Aruba Networking VPC as part of proof of concept services, and (ii) during provision of support services through the receipt of data dumps or remote access to Controller systems. Proof of concept: 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 service: Processor's HPE Aruba Networking TAC CRM is certified complaint with the highest independent, international, industry-accepted privacy standards.
2.	Type of personal data processed	Personal data collected includes data related to: a. Network activity behavior of Controller end users of Controller network including applications used, and data exchanged by internet-facing/internal facing usage. b. Data exchanged by internet-facing and/or internal-facing usage includes, but is not limited to: i. Contact Information: Names, email addresses, and phone numbers ii. System Asset/Usage Device Information: IP address and tracking/analytics data iii. Tracking/Analytic Information: IP address
3.	Categories of personal data processed	Controller's client, end user, employee, contractor, and temporary workers.
4.	Duration of processing	Processor shall process Controller personal data for the duration of the Agreement and/or any applicable transaction document.
5.	Technical & Organizational Measures	Processor shall maintain the information and physical security program for the protection of Controller personal data as detailed in Annex III below.

Annex III: Technical and organizational measures including technical and organizational measures to ensure the security of the data

1. **Product Security Features:** The product is a security product which helps the Controller to detect intrusions into Controller's network from internal and external threat actors. The product has certain security features. These include:

   Organization Security Features:

   a. Access control is implemented at various levels so only specific individuals have access to perform their job functions.

   b. There is an SIRT group that follows security advisories found internally, reported externally and responds diligently.

   c. Security updates to products are provided on a regular and timely manner.

   Technical Security Features:

   a. The product uses firewall to only open specific network ports that need to be open for product usage.

   b. All credentials are stored in encrypted format.

   c. Product minimizes programs and processes running as root.

2. **Obfuscating Personal Data:** IntroSpect stores and displays a user's personal data, such as user's name and department in clear text. For privacy reasons, it is sometimes necessary to obfuscate a user's personal data. For example, a help desk person should not be able to see a user's personal data, but a senior threat investigator should. IntroSpect 2.2 and later enables obfuscation of personal data 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 personal data obfuscated and can see the user as Jane Doe.

3. **Proof of Concept:** Amazon Web Services (AWS) security standards. Access to the Controller's instance is limited to Processor personnel supporting proof of concept services. All access is logged in an audit trail and can be provided to the Controller if required.

4. **Processor Security Measures:** The support services used to support IntroSpect customers (Controller) is provided by the Technical Assistance Group (TAC) within Processor's HPE Aruba Networking business unit. Processor implements and maintains physical, technical and organizational security measures set out to protect Controller personal data and business contact data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosures or access. Only where necessary to provide the services, Processor will provide its affiliates and subcontractors with access to Controller personal data.

a50009463ENW