Data sheet

HPE ARUBA NETWORKING SECURITY SERVICE EDGE (SSE)

Annex II: Description of the processing

1.	Description of processing	Processor's HPE SSE helps businesses better support their modern workplace through secure connectivity with its cloud-delivered platform, Atmos. Short for "Atmosphere," Atmos is a security service edge (SSE) platform that offers a modern alternative to traditional network security technologies. With over 350 global edge locations, Atmos enables IT teams to easily provide end users with granular zero trust access to private applications, SaaS applications, and the internet anywhere work needs to be done and anywhere it can be done based on defined policies based on user role, permissions, geographic location, and other parameters. The platform artfully integrates Atmos ZTNA, Atmos SWG, Atmos CASB and Atmos Digital Experience into one, cloud-delivered, platform that feels weightless, and is controlled by a single pane of glass. In addition, Atmos provides users with filtering capabilities of the content using Data Leakage Prevention and Anti-Malware capabilities, processing the data itself.
2.	Type of personal data processed	Personal data collected as part of network management and related applications include: a. Device MAC b. Device IP c. Device Operating System d. Device model e. Device Type f. Device Hostname g. Username h. User Id i. Email (in case it's used as a user ID) j. Location of user k. GEO Location l. Display Name / Group Membership / Title
3.	Categories of personal data processed	Controller's end-user, employee, contractor, and temporary worker.
4.	Duration of processing	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. The content itself is purged immediately after processing.
5.	Technical & Organizational Measures	Processor shall maintain the information security program for the protection of Controller personal data as detailed in Annex III below. The program is certified against different standards, including ISO 27001:2022, ISO 27017:2015, ISO 27018, and SOC 2 Type 2 with a Privacy Extension.

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

1. **Product Security Features:**

   a. **Physical Security:** HPE Networking SSE is deployed on leading hyperscale cloud service providers, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform™ (GCP™), and inherits the physical security controls implemented and maintained by these providers.

   As part of our cloud security program every 6 months we review relevant Cloud Service Provider (CSP) reports to ensure that security level remains the same.

   b. **Network Security:** Processor network security ensures that the physical and virtual network on which the application and data reside is secure. We use services and tools that the IaaS provider offers and some third-party solutions to make sure our production environment is as secure as it can be from external threats and internal vulnerabilities. Processor 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 (Controller). 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 (Controller) and ensures their data is always confined to one environment.

   c. **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 an allowlist 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.

   d. **Data Security:** All data exchange between the application and devices and users happen using HTTPS. Data at rest is encrypted. Furthermore, the data retention period is strictly aligned with the contract requirements, varying from immediate deletion to 90 days. Data backup occurs on a regular basis, and backup data is stored in a redundant manner. From an organization perspective, we have a SecOps team that manages all security and operational aspects of the app.

   e. **Geographic Availability:** HPE Networking SSE is available in multiple locations worldwide, allowing Controller 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 each region or impose regulatory restrictions on how data can be processed and stored.

HPE SSE is deployed on clusters in several regions that are primarily used to store and process data.

HPE SSE Cluster	AWS region (City where cluster is based)
UK (London)	London, England, United Kingdom (eu-west-2)
US East (N. Virginia)	Northern Virginia, USA (us-east-1)
EU (Frankfurt)	Frankfurt, Germany (eu-central-1)

Additionally, HPE Networking SSE operates multiple Points of Presence (PoPs) globally, functioning as intermediaries between the selected region and the applications. This PoPs are designed for routing data In-transit only and do not store any data. PoP Is selected automatically and can be changed per customer request.

HPE SSE Point of Presence	AWS region (City where cluster is based)
UK (London)	London, England, United Kingdom (eu-west-2)
Asia Pacific (Hong Kong)	Hong Kong (ap-east-1)
EU (Spain)	Spain (eu-south-2)
Middle East (Israel)	Tel-Aviv, Israel (il-central-1)
Asia Pacific (Sydney)	Sydney, Australia (ap-southeast-2)
US East (N. Virginia)	Northern Virginia, USA (us-east-1)
Asia Pacific (Singapore)	Singapore (ap-southeast-1)
Asia Pacific (Mumbai)	Mumbai, India (ap-south-1)
South America (São Paulo)	São Paulo, Brazil (sa-east-1)
EU (Frankfurt)	Frankfurt, Germany (eu-central-1)
Africa (Cape Town)	Cape Town, South Africa (af-south-1)
US West (N. California)	Northern California, USA (us-west-1)
Asia Pacific (Tokyo)	Tokyo, Japan (ap-northeast-1)
Asia Pacific (Jakarta)	Jakarta, Indonesia (ap-southeast-2)
Middle East (UAE)	UAE (me-central-1)
Milano (Italy)	Milan, Italy (eu-south-1)
Paris (France)	Paris, France (eu-west-3)
Asia Pacific (Seoul)	Seoul, South Korea (ap-northeast-2)
US West (Oregon)	Oregon, USA (us-west-2)
NA (Canada)	Montreal, Canada (ca-central-1)
EU (Spain)	Zaragoza, Spain (eu-south-2)
Asia Pacific (India)	Hyderabad, India (ap-south-2)
EU (Stockholm)	Stockholm, Sweden (eu-north-1)
Asia Pacific (Australia)	Melbourne, Australia (ap-southeast-4)
North America (Mexico)	Central Region, Mexico (mx-central-1)
EU (Switzerland)	Zurich, Switzerland (eu-central-2)

HPE SSE Point of Presence	Azure region (City where cluster is based)
UK (Cardiff)	Cardiff, United Kingdom (uk-west)
US Central (Texas)	Texas, USA (South-Central US)
US Central (Iowa)	Iowa, USA (Central US)
Asia Pacific (New Zealand)	Auckland, New Zealand (New Zealand-north)
NA (Canada)	Toronto, Canada (Canada Central)

HPE SSE Point of Presence	GCP region (City where cluster is based)
South America (Santiago)	Santiago, Chile (South America-west1)
EU (Netherlands)	Groningen, Netherlands (Europe-west4)
Asia Pacific (Taiwan)	Taiwan (Asia-east1)
EU (Poland)	Warsaw, Poland (Europe-central2)
EMEA (Saudi Arabia)	Dammam, Saudi Arabia (me-central2)

All activities related to a Controller terminate in the chosen cluster, including network statistics and telemetry data pushed over HTTPS connections.

All data (including personal data) corresponding to the customer's network activities (i.e., Web Access logs) and any other user data is stored on databases within the same cluster.

— **Security Measures:**

Processor shall maintain the following information and physical security program for the protection of Controller personal data (the "Processor Security Program"):

- Processor infrastructure has reasonable up-to-date versions of system security software which may include host firewalls, anti-virus protection, and up-to-date patches and virus definitions. Processor maintains logs of events involving the infrastructure, including intrusion detection systems to monitor, detect, and report misuse patterns, suspicious activities, unauthorized users, and other security risks.

- Employees and contractors are trained in Processor's privacy and security policies and made aware of their responsibilities with regard to privacy and security practices. Processor employees and contractors are contractually bound to maintain the confidence of Controller personal data and comply with applicable Processor policies, standards, or requirements in relation to the processing of Controller personal data. Failure to comply with those policies, standards, or requirements will be subject to investigation which may result in disciplinary action up to and including termination of employment or engagement by Processor.

- If Controller becomes aware of a personal data breach incident that affects the services, the Controller shall promptly notify the Processor of such and inform the Processor of the scope of the personal data breach. Notice shall be provided to Processor Security Operations Center via email at Cloudops@axissecurity.com.

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

GCP and Google Cloud Platform are registered trademarks of Google LLC. Azure and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All third-party marks are property of their respective owners.

a00138898ENW, Rev. 5

HEWLETT PACKARD ENTERPRISE

hpe.com