Privacy Datasheet

Prisma AIRS

The purpose of this document is to provide customers of Palo Alto Networks with information needed to assess the impact of this service on their overall privacy posture by detailing how Personal Data is captured, processed, and stored by and within the Prisma AIRS solution when Palo Alto Networks is acting as a Processor.

1. Product Summary

Prisma AIRS is a platform to secure customers' AI applications, models, and agents from supply chain to runtime. It includes multiple components, including runtime security, model security, agent security, and red teaming.

2. Personal Data Processed by Prisma AIRS

The table below lists the Personal Data used by Prisma AIRS and describes what Personal Data is processed and why.

Table 1: Personal Data Processed by Prisma AIRS

Type of Personal Data	Example(s)	Purpose of Processing
AI Runtime Security		
[API & AI Firewall] Unknown personal data and metadata in LLM & tool inputs and outputs	*“This is Mark. Can you summarize my logs from the past 7 days?”*	● Threat prevention ● Support
[API & AI Firewall] Administrative user ID	jsmith@company.com; jsmith	● Reporting
AI Model Security		
Administrative user ID	JSmith; jsmith@company.com	● Authentication ● Reporting
Individual email (when used for service accounts)	jdoe-testing@company.com	● Reporting
AI Red Teaming		
Administrative user ID	Jsmith; jsmith@company.com	● Authentication ● Reporting
Unknown personal data in LLM & tool outputs	*“The following users are logged in: ….”*	● Threat analysis ● Reporting

	AI Agent Security		
	User IDs/email of users accessing AI agents	jdoe-testing@company.com	• Reporting

If you request customer support, more information on Personal Data processed is available in the Support Services, Customer Success and Focused Services Privacy Data Sheet.

3. Access to Personal Data

Access by Customers

The Prisma AIRS management console is hosted in the cloud allowing customer administrators to view and manage data related to the entire AI ecosystem. The data available to the customer includes all Personal Data listed in Table 1. Administrators have access to reports that detail the LLM/tool input and output payloads.

Data can be accessed directly through the administrative console (the front end) or programmatically via the Prisma AIRS APIs. This API-first approach allows customers to query and retrieve all data stored by the product for Model Security and AI Red Team functions, enabling seamless integration with existing systems.

Access by Palo Alto Networks

Access by Palo Alto Networks to Personal Data is restricted to:

1. Customer support teams,
2. Product development teams,
3. Threat research analytics teams, and
4. Managed threat hunting/detection/response service teams (if the customer has procured such services).

All access is recorded and audited. Access privileges are managed by Palo Alto Networks engineering leadership.

4. Processing Locations

Data Centers and Third Party Service Providers

Palo Alto Networks engages third-party providers that act as sub processors in order to provide Prisma AIRS. These suppliers are required to provide an equivalent level of protection of data as Palo Alto Network provides.

Table 2: Sub-processors in Prisma AIRS			
Sub-processor Name	**Personal Data Processed**	**Service Type**	**Location**
AI Runtime Security			

GCP	Unknown personal data in LLM & tool inputs and outputs Administrative user ID	IaaS/PaaS	United States, United Kingdom, Canada, India, Germany, Singapore
AI Model Security			
GCP	Administrative user ID Individual emails used for service accounts	IaaS/PaaS	United States
AI Red Teaming			
GCP	Administrative user ID Unknown personal data in LLM & tool outputs	IaaS/PaaS	United States
AI Agent Security			
GCP	User ID/email of users accessing AI Agents	IaaS/PaaS	United States, Canada, Germany, United Kingdom, Singapore, India, Australia, Japan, France

Customer Support Locations

Customer support for Prisma AIRS will be provided from various locations around the globe. For more information on these locations, please refer to the Support Services, Customer Success and Focused Services Privacy Data Sheet.

Affiliates Processing Locations

Palo Alto Networks may process Personal Data in any of the locations of its Sub-processor Affiliates identified in its List of Sub-processors.

5. Compliance with Privacy Regulations

Palo Alto Networks captures, processes, stores, and protects Personal Data in Prisma AIRS in accordance with the terms in (i) Palo Alto Networks Privacy Policy, (ii) for our customers, the applicable Data Processing Addendum, and (iii) this Privacy Datasheet. Our Trust Center, Palo Alto Networks one stop-shop for everything privacy and security related, provides numerous resources, including information on how our privacy practices comply with existing and applicable privacy legislations around the globe. For more information, please visit the Privacy section in the Trust Center.

Cross-Border Data Transfer

As part of the provision of the Prisma AIRS service and/or purchased support services, Palo Alto Networks may be required to transfer Personal Data to other countries outside of the country/region where the customer is located. To the extent that we need to transfer such data, we will do so in compliance with applicable requirements for transfer of Personal Data, which include the EU Standard Contractual Clauses, as approved by the European Commission and/or other legally binding instruments.

Data Subject Rights

Users whose Personal Data is processed by Prisma AIRS have the right to request access, rectification, suspension of processing, or deletion of the Personal Data processed by the service. Users can open a request via Palo Alto Networks Individual Rights Form.

Palo Alto Networks will confirm identification before responding to the request. Please note that if, for whatever reason, we cannot comply with the request, we will provide an explanation. For all users whose employer is a Palo Alto Networks customer, such users may be redirected to the relevant customer/employer for a response.

6. Data Portability

Customer administrators can forward logs that may contain the administrative user ID to Palo Alto Networks or third-party products for collection and review. On the user interface, customer administrators can also view the LLM/tool input and output payloads that may contain unknown Personal Data.

For the AI Runtime API, customer administrators can query a report that contains the LLM/tool input and output payloads.

For Model Security and for Red Team, Customers can call public APIs to retrieve all the data stored by the product.

7. Retention and Deletion of Personal Data

Table 3: Retention and Deletion of Personal Data

	Categories of Personal Data	Retention/Deletion Period
AI Runtime, AI Model Security, AI Red Teaming		
During the term of your subscription	Benign LLM/tool input and output payloads	Up to 14 days

	Malicious LLM/tool input and output payloads	Up to 10 years
	Administrative user ID	During the term of subscription
After the termination of your subscription	Benign LLM/tool input and output payloads	Up to 14 days
	Malicious LLM/tool input and output payloads	Up to 10 years
	Administrative user ID	30 Days
AI Agent Security		
During the term of your subscription	Users accessing AI agents	90 days
After the termination of your subscription	Users accessing AI agents	90 days

8. Security of Personal Data

Securing Personal Data

Palo Alto Networks supports a defense-in-depth security model to help protect the customer's data at all stages of its lifecycle, in transit, in memory, and at rest, as well as through key management.

- The Trust 360 Program details the corporate-wide security, compliance, and privacy controls in place to protect our customers' most sensitive data.
- Palo Alto Networks Information Security Measures document details the technical and organizational measures that will be implemented by us to secure systems, processes and data. This document forms part of Palo Alto Networks Data Processing Addendum.

9. Resources

For more general information about Palo Alto Networks Privacy and Security Practices, please visit our Trust Center.

About This Datasheet

Please note that the information provided with this Datasheet may be subject to change, provided however that such change will not result in a material degradation of the security posture of the platform. Information concerning warranties and compliance with applicable laws may be found in Palo Alto Networks End User License Agreement.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com