Prisma Access Privacy Datasheet

The purpose of this document is to provide Palo Alto Networks customers with the information needed to assess the impact of this service on their overall privacy posture by detailing how personal information may be captured, processed[1], and stored by and within the service.

Product Summary

Prisma Access provides network security for off-premises and branch offices, allowing remote and mobile users to securely connect to the internet, the cloud, SaaS, and data center applications. Using cloud-based security infrastructure as an alternative to installing or managing firewalls around the world, it eliminates the need to backhaul cloud traffic to a central firewall. It consistently inspects all traffic across all ports, leveraging built-in threat prevention, malware prevention, URL filtering, SSL decryption, and application-based policy capabilities to provide the same level of security no matter where users are or what resources they are accessing.

Information Processed by Prisma Access

The types of personal information processed by Prisma Access are limited to the minimum necessary to fulfill our business purposes in providing our customers with Prisma Access. Categories of information processed by Prisma Access that may contain personal information include:

- **Configuration, customer security policies, and operational data:** These policies and data are received, stored, and processed through the Panorama interface or Prisma Access app on the hub. Policies may include information about the host state, User-Ids, and the applications, as well as content that users or user groups are allowed to access. When using the ADEM add-on, information used for detecting applications and their usage on the network may include user geolocation data (city and state level), user device, and Wi-Fi details, for a complete list of data collected, please refer to the ADEM Admin Guide. The Host Information Profile data is also collected for any mobile user device when it matches a configured asset policy, such as when the device does not have antivirus programs installed.
- **Network traffic:** This may contain source and destination IP addresses. For support requests, the customer controls permissions for packet capture. SSL/SSH decryption enables inspection of encrypted network traffic. The customer establishes and manages decryption policies to enforce security policies, control access to applications, and stop malicious content.
- **User identification:** When enabled, Prisma Access employs User-ID™ technology on remote networks and mobile users to provide the customer's organization with user and user group identification, for instance, by retrieving it from Active Directory to map security policies to network activities. It may include information that may be considered personal, individually or in

[1] In this document, we adopt the broad definition of "processing" that appears at Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …", which includes, but is not limited to the following non-exhaustive series of examples: "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

combination, such as: User-Id, User Device Details, Wi-Fi SSID Name and Other Wi-Fi details, User Location, ISP Information, IP Addresses, and LAN details.

- **Malicious file content:** When detected, this content may include information that could be considered personal, individually or in combination, such as: sender, recipient, and subject lines, URLs associated with unknown files, and application/User that transmitted the unknown files.
- **Sensitive file content:** Prisma Access with DLP service inspects file content in motion to detect and protect sensitive data defined by data patterns and data profiles based on corporate policy, including any type of personal information contained in the file.
- **URLs:** URL users interact with are inspected, blocked, and logged in accordance with the customer's security policies and may contain personal information personal, such as User-Ids

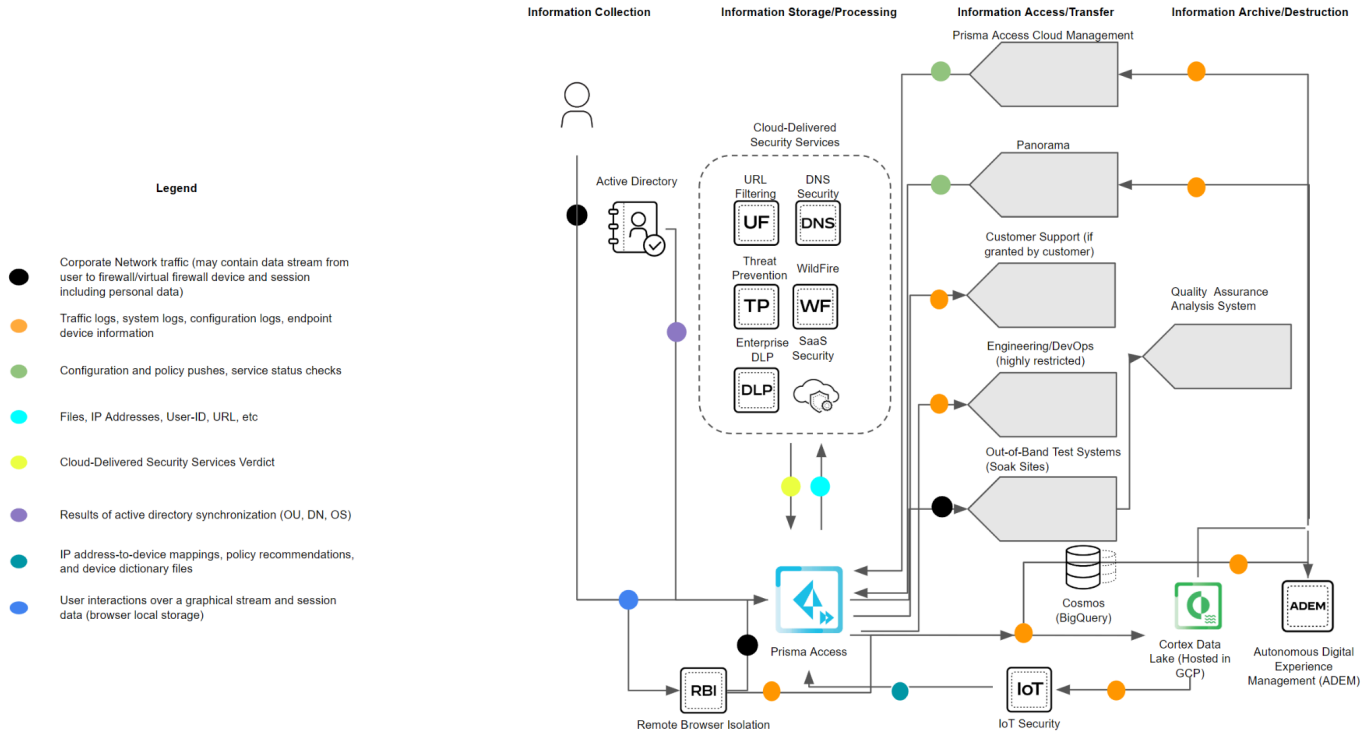
Purpose of Information Processed by Prisma Access and Add-ons

Palo Alto Networks processes information through Prisma Access in order to secure network traffic and prevent unauthorized access. The processing activities involved include, but are not limited to:

- Inspecting network traffic that goes through the firewall and generating traffic, URL filtering, data filtering, and threat logs, and pcaps (APIs used to process live network packet data).
- Blocking known threats, monitoring performance, and monitoring and preventing transfers of sensitive data based on policy.
- Authenticating users that connect to a network either from a mobile device or from a branch office that does not operate its own firewall.
- Sending unknown files to the WildFire cloud for further inspection and analysis.
- Transferring logs to Cortex Data Lake for storage and analysis.
- Conducting security research and quality improvement purposes, including by using Soak Sites.
- Providing customers with optimal user experience, application performance metrics, and identifying service/app malperformance for remediating user experience issues.
- Transfer Internet browsing activity away from their employee devices and corporate networks to Palo Alto Networks cloud for Remote Browser Isolation, to secure and isolate potential malicious code.

Data Flow Diagram

Prisma Access interacts with several Palo Alto Networks products and applications. The key data flows associated with the information processing activities described in this document are shown below.



Our Privacy Practices

Palo Alto Networks captures, processes, stores, and protects personal information in accordance with our Privacy Policy and product Privacy Data Sheets. Our Trust Center provides numerous privacy resources, including descriptions of our privacy practices related to the California Consumer Privacy Act (CCPA), the European Union's General Data Protection Regulation (GDPR), our subprocessors, and our U.S. Cloud Act Frequently Asked Questions (FAQ). For further information about the ways in which our products support customer GDPR compliance, please visit: https://www.paloaltonetworks.com/legal-notices/gdpr.

The Palo Alto Networks platform 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. Please refer to the Trust 360 white paper for further information.

Subprocessors

Security compute locations may be hosted in Amazon Web Services (AWS®) or Google Cloud Platform (GCP®). Prisma Access is hosted in AWS and GCP public cloud data centers. Twilio Inc. (SendGrid) in the United States may be used to send email alerts to customer administrators if elected by customer.

Customer Privacy Options

Palo Alto Networks designs its products to support our customers' compliance with global data protection and compliance obligations.

Whereas Prisma Access for remote networks leverages cloud locations that are in proximity to the branch or remote office, Prisma Access for mobile users can rely on cloud locations deployed worldwide so that customers can benefit from network security everywhere, with minimal latency. When onboarding, customers can choose a deployment region associated with a security compute location for processing traffic.

Customers can control access to the data processed by Prisma Access by applying the business need-to-know rule through Panorama. Customer controls and access privileges also apply to the ADEM application. When configuring the service, customers can determine what information gets logged and sent to Cortex Data Lake. The logs created by the firewall may be accessed by Palo Alto Networks support teams to investigate a support case initiated by a customer.

Access and Disclosure

Access by the Customer

Customers can access information related to Prisma Access through the Panorama interface, the Prisma Access Cloud Management interface, or the Prisma Access app on the hub. The customer's system administrator controls access to Panorama by granting appropriate privileges to authorized users. To use the Prisma Access app on the hub, the customer's system administrator must have an account on the Palo Alto Networks Customer Support Portal with an app administrator role.

Access by Palo Alto Networks

Data processing by Prisma Access is mostly automated. Access is restricted to (a) product development teams, (b) Site Reliability Engineers (SREs), (c) Threat Research Analytics teams, and (d) Customer Support teams. Selective mirroring access by Palo Alto Networks occurs when required to troubleshoot a customer support inquiry or address issues related to the service. All access privileges are managed by Palo Alto Networks Customer Support and Engineering leadership and audited for privilege access violations.

Prisma Access is able to collect contact information to enable us to directly reach out to our customers, if required, for service-related matters. It is stored in conformance with our Privacy Policy and customers may exercise their applicable privacy rights with respect to their contact information.

Palo Alto Networks may disclose or use aggregated or de-identified personal information for any lawful purpose in accordance with our privacy policies and other privacy disclosures.

Cross-Border Data Transfer

In the event of a need to share personal information with Palo Alto Networks personnel in regions outside of those identified in the Locations of Processing section above, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission and/or other legal instruments, recognized by EU data protection laws. For a more detailed assessment of our international data transfers, please refer to our GDPR Data Transfer Impact Assessment.

Retention

Logs from Prisma Access are temporarily stored in the cloud service before being transferred to Cortex Data Lake. See the Cortex Data Lake Privacy datasheet for details on the controls and processes related to retention of logs.

Data consumed by Prisma Access Insights is retained for 15 months and data collected by the ADEM add-on is retained for 30 days.

Through Prisma Access Insights, customers' administrators will have access to 30 days' worth of data concerning: service and network health, including Prisma Access, Prisma Access locations, and customer deployment; customer network configuration/setup-related information, including tunnel details and status, remote network health, bandwidth consumption, regions of deployment, number of security processing nodes, types of nodes, etc.; usage metrics, including license consumption, bandwidth consumption, mobile user connections (IP and location), behavior, and trends; and alerts, including all aforementioned metrics and combinations of metrics. Administrators will also see alerts when a tunnel or node goes down or when issues are resolved. When enabled, Prisma Access employs User-ID™ technology that may include user group information that may be retained by the cloud service as long as the customer's subscription is active.

Security

AWS and GCP provide the physical and environmental security controls for the Prisma Access infrastructure. The controls of AWS and GCP are excluded from the scope of this privacy datasheet. For information about security protections in the data centers where Prisma Access data resides, please see the Google Compliance resource center at https://cloud.google.com/security/compliance and the AWS Compliance resource center at https://aws.amazon.com/compliance/.

Palo Alto Networks also has achieved SOC 2 Type II Plus and ISO 27001 certification for Prisma Access to demonstrate its strong security policies and internal controls. For more information, visit paloaltonetworks.com/legal-notices/trust-center/soc2. Please visit Palo Alto Networks' technical certifications page to learn more about the full range of ISO and other certifications that apply to Prisma Access: https://www.paloaltonetworks.com/legal-notices/trust-center/tech-certs.

The Trust 360 Program details the security, compliance, and privacy controls in place to protect our customers' most sensitive data. Further information about Palo Alto Networks' security safeguards is available here. These safeguards include firewall technology, an intrusion detection system, and network segmentation. Each respective customer is responsible for ensuring physical, technical, and administrative security measures are in place to protect data and must meet all applicable privacy and security standards required by their organizations.

Locations of Processing

Palo Alto Networks regional clouds provide options to address customers' data location preferences. Prisma Access offers a local experience in more than 100 locations worldwide.[2] Each location is mapped to a security compute location based on optimized performance and latency. ADEM and Prisma Access Insights locations are automatically mapped to CDL locations as shown below in Table 1.

[2] Explicit proxy currently available in 25 locations.

Table 2 shows the list of Prisma Access compute locations where security processing occurs. A mapping of local country locations to the associated compute locations can be found at Prisma Access Locations. System administrators can select and deselect the countries in the configuration menu in order to select the associated compute location indicated in the list. Please review the Prisma Access Administrator's Guide for more information. Palo Alto Networks reserves the right to update these country-to-compute mappings from time-to-time and such changes will be reflected at the link above, and displayed to the administrator in the configuration menu.

Table 1: Management, Insights, ADEM and IoT Security Location Mapping to CDL

CDL	**Cloud Management**	**Prisma Access Insights Data**	**ADEM Data (ADEM portal)**	**IoT Security** (add-on)
United Kingdom	United Kingdom	United Kingdom	United Kingdom	United Kingdom
Netherlands	Germany	Netherlands	Netherlands	Germany
Germany	Germany	Germany	Germany	Germany
Switzerland	Germany	Switzerland	Switzerland	Switzerland
France	Germany	France	France	Germany
Singapore	Singapore	Singapore	Singapore	Singapore
India	India	India	India	Singapore
Japan	United States	Japan	Japan	Japan
Canada	United States	Canada	Canada	Canada
United States	United States	United States	United States	United States
Australia	Australia	Australia	Australia	Australia

Table 2: Prisma Access Mapping to Prisma Access Compute, WildFire Locations

Prisma Access Compute Location	WildFire Location
Japan Central	Japan
India West	India
Indonesia	Indonesia
Singapore	Singapore
Australia South	Australia
Australia Southeast	Australia
Australia West (Perth)	Australia
Bahrain	Netherlands
Belgium	Netherlands
Canada East	Canada
Canada Central	Canada
Canada West	Canada
Germany Central	Germany
Poland	Poland
Finland	Netherlands
Sweden	Netherlands
United Kingdom	United Kingdom
France	France
Italy	Netherlands
Spain	Netherlands
Netherlands Central	Netherlands
Hong Kong	Japan
India North	India

Ireland	Netherlands
Japan South	Japan
Qatar	Netherlands
United Arab Emirates	Netherlands
Israel	Israel
Nigeria (Lagos)	Netherlands
New Zealand (Auckland)	Australia
South Africa Central	Netherlands
South Africa West	Netherlands
Brazil South	United States
Chile	United States
Saudi Arabia	Netherlands
South America West (Lima)	United States
South Korea	Japan
Switzerland	Switzerland
Taiwan	Taiwan
US Central	United States
US-Central (Chicago)	United States
US Central West	United States
US East	United States
US Northwest	United States
US South	United States
US Southeast	United States
US Southeast (Miami)	United States

US Southwest	United States

For the DNS Security, URL filtering, and the DLP and SaaS Security add-ons, Prisma Access uses dynamic location mapping rather than static mapping. The data for each of the four services will be processed in that service's data center that has the lowest latency and the best performance with the Prisma Access security compute data center. The current data center locations for each service is as follows:

DNS Security: Japan, Singapore, Australia, Hong Kong, India, United Kingdom, Germany, Netherlands, France, United States (West, East, and Central), Canada, Brazil, South Africa, Bahrain
URL Filtering: Japan, Australia, Singapore, India, Netherlands, Germany, Switzerland, France, United Kingdom, United States (West, East and Central), Canada
DLP: Australia, Singapore, India, United Kingdom, Germany, United States
SaaS Security: United States, Singapore, India, Germany

Resources

You may visit this directory of all of our available product privacy data sheets or view other selected product resources below:

- Cortex Data Lake resource page: paloaltonetworks.com/cortex/cortex-data-lake
- Prisma Access resource page: paloaltonetworks.com/prisma/access
- WildFire resource page: paloaltonetworks.com/products/secure-the-network/wildfire
- Enterprise DLP resource page: paloaltonetworks.com/enterprise-data-loss-prevention
- Cloud-Delivered Security Services (CDSS) resource page: https://www.paloaltonetworks.com/network-security/security-subscriptions
- ADEM add-on resource page: https://docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-in-prisma-access.html

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

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