Privacy Datasheet
Enterprise DLP and Email DLP

The purpose of this document is to provide customers of Palo Alto Networks with the 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 Enterprise Data Loss Prevention ("DLP") and the Email DLP services.

Palo Alto Networks Data Loss Prevention (DLP) is a cloud service that scans data flowing through various Palo Alto Networks products, helping provide consistent data protection across the entire organization. It allows organizations to discover, monitor, govern, and secure sensitive data and supports an organization's data protection and compliance efforts in a simplified, cost-effective manner.

1. Product Summary

DLP is integrated with Palo Alto Networks products (hereinafter called "channels") such as SaaS Security, Prisma® Access, Prisma Cloud Data Security, and NGFWs to provide data security at various enforcement points. The channels send files to DLP via APIs. DLP scans the files, performs analysis to detect sensitive information in the files for any policy violation, and returns a verdict and other data to the channel. The channel then uses this information to take remediation action to protect sensitive data at risk.

2. Personal Data Processed by Data Loss Prevention

Palo Alto Networks DLP (both Enterprise DLP and Email DLP) discovers and protects sensitive information in data at rest stored in software-as-a-service (SaaS) apps—such as Microsoft 365™, Google Workspace, Slack, and Box—and in data in motion over the networks.

DLP scans files against predefined or customer-defined data patterns. Customers create or use pre-defined data patterns corresponding to the information type they want to protect. The machine learning-based classifier can also analyze a file for sensitive information.

For example, suppose the customer wants to protect credit card numbers from loss or exfiltration. In that case, DLP will scan the files against the credit card data pattern and provide visibility and actionable verdicts. The results of these scans are made available to the customer through reporting features offered in each channel's user interface. The results, called "snippets," are provided to the administrator on request through the channel's UI. The customer administrator can configure the information displayed in the snippet for specific channels. Logs generated by DLP across all channels show information about the occurrences of policy violations, the file metadata, and the risk assessment summary.

Enterprise DLP and Email DLP process Personal Data described in Tables 1-A and 1-B.

Table 1-A: Personal Data Processed by Enterprise Data Loss Prevention			
Category of Personal Data	**Type of Personal Data**	**Example(s)**	**Purpose of Processing**
User information (employee of the customer)	Name	John Doe, Jane Smith	• User identification • Tracking Incident records • Channel admin for monitor and remediation
	Email address	jdoe@company.com	• User identification • Tracking Incident records • Enable customers to monitor and remediate
Network information	IP addresses	34.107.151.202	• User identification • Policy matching and enforcement
Customer files	Data in Files where data pattern is matched	Social security numbers, credit card numbers, name of a medicine	• Detection of predefined or customer-defined data patterns- snip
User Activity	Service used by the end-user	end URL/domain information	• policy and enforcement

Table 1-B: Personal Data Processed by Email Data Loss Prevention			
Category of Personal Data	**Type of Personal Data**	**Example(s)**	**Purpose of Processing**
Information in Emails	Sender/recipient email addresses	To: jonedoe@example.com From: Jane@organization.com	• User identification • Detection by predefined or customer-defined data patterns
	Personal data in email subject line	Subject: User Tom with ID ABC010101, last 4 of SSN is 0909	• Detection by predefined or customer-defined data patterns
	Personal data in email body if any personal data is attached in an email attachment	SaraLee's medication information or SSN	• Detection by predefined or customer-defined data patterns

3. Access to Personal Data

Access by Customers for Enterprise DLP

The customer's administrative users will have access to the following:

- Name.
- Email address.
- IP Address.
- Data where the pattern is matched.

A customer's administrative users can use all of the above information to determine the service usage by individuals and to take further administrative actions, such as policy enforcement and deletion of associated session data. Customer's administrative users can view snippets and logs through each channel's user interface.

Access by Customers for Email DLP

Customer's administrative users can access the following data in the product:

- Email metadata, which includes the following information:
  - Sender & recipient email address on the incidents page
  - Email subject, which may contain sensitive content on the incidents page
  - Email addresses on the Email DLP policy
- Name
- IP Address
- Data where the pattern is matched

Additionally, the customer's administrator can configure the product to transfer the full email or file that has violated the customer's defined criteria into the customer's chosen cloud storage provider.

A customer's administrative users can use all of the above information to determine the service usage by individuals and to take further administrative actions, such as policy enforcement and deletion of associated session data. Customer administrative users can view snippets and logs through each channel's user interface.

Access by Palo Alto Networks

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

1. Customer support teams,
2. Product development teams, and
3. Threat research analytics teams.

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 to provide Enterprise Data Loss Prevention. These sub-processors are required to provide an equivalent level of data protection to that of Palo Alto Networks.

Palo Alto Networks engages Amazon Web Services (AWS®) and Google Cloud Platform (GCP®) for hosting of DLP and MongoDB® Atlas for configuration management. DLP processes the Personal Data in the locations in Tables 2-A and 2-B that have the best performance and lowest latency to the

individual user. The result logs from DLP processing (but not snippets) will be consolidated for reporting purposes in the region selected by the customer in onboarding.

Table 2-A: Sub-processors in Enterprise Data Loss Prevention			
Sub-processor Name	**Personal Data Processed**	**Service Type**	**Location**
AWS	All Types of Personal Data listed in Table 1-A	IaaS Provider	USA, Canada, Germany, United Kingdom, Singapore, India, Australia, Japan, France
GCP	All Types of Personal Data listed in Table 1-A	IaaS Provider	USA, Canada, Germany, United Kingdom, Singapore, India, Australia, Japan, France
Atlas Mongo	Customer administrator email address (of administrator that creates configuration)	IaaS Provider	USA

Table 2-B: Sub-processors in Email DLP			
Sub-processor Name	**Personal Data Processed**	**Service type**	**Location**
GCP	All Types of Personal Data listed in Table 1-B	IaaS Provider	USA, Germany, Singapore
AWS	All Types of Personal Data listed in Table 1-B	IaaS Provider	USA, Germany, Singapore

Customer Support Locations

Customer support for Enterprise and Email Data Loss Prevention 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 Enterprise Data Loss Prevention by the terms in (i) Palo Alto Networks Privacy Policy, (ii) for our customers, the applicable Data Protection Addendum, and (iii) this Privacy Datasheet. Our Palo Alto Networks Trust Center is a one-stop shop for everything related to privacy and security and provides numerous resources, including

information on how our privacy practices comply with existing and applicable privacy legislation around the globe. For more information, please visit the Privacy section in the Trust Center.

Cross-Border Data Transfer

As part of the Enterprise Data Loss Prevention service provision 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 comply with applicable requirements for the 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 Enterprise Data Loss Prevention 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 explain. 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. Retention and Deletion of Personal Data

For Enterprise DLP

Depending upon the channel, DLP may store snippets and logs in addition to configurations. The data retention policy for snippets and logs is as follows:

- SaaS Security: SaaS Security stores the metadata about the data pattern (i.e., how many violations the file contains). When the customer requests snippets through the UI, the file is in the SaaS vendor cloud and scanned again for sensitive content. Newly generated snippets are stored in SaaS Security (API Scan)for 12 months.
- Prisma Cloud Data Security, Prisma Access, and NGFWs: Snippets and logs are stored in DLP for 90 days.
- Customers can turn off the snippets feature altogether, in which case no snippets data is stored.
    - Such configuration can be found at Data Loss Prevention -> Settings. The Snippets can be disabled.
- Upon expiration of the DLP and channel license, data will remain available for customer access for 90 days, after which it will be deleted.
- Extracted text for inspection is stored for 24 hours
- Snippets, reports, and incident data are stored for 90 days.

For Email DLP

- Email metadata for incidents and email audit logs in Spanner DB (Google-managed DB) is stored for 90 days.
- Email content data is stored in the Google Cloud bucket managed by Palo Alto Networks for 7 days.

7. 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 to protect our customers' most sensitive data.
- The Palo Alto Networks Information Security Measures document details the technical and organizational measures we will implement to secure systems, processes, and data. This document forms part of the Palo Alto Networks Data Protection Addendum.

8. Resources

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

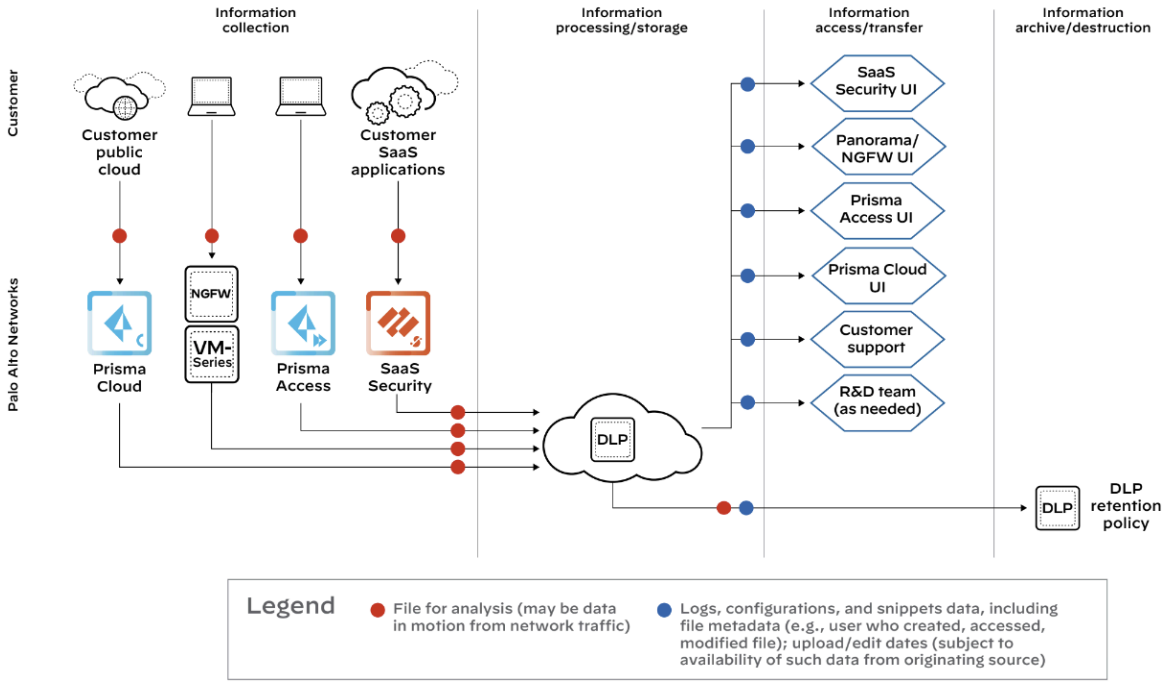

Figure 1: Data flow diagram

About This Datasheet

Please note that the information in this datasheet may be subject to change, provided that such change does not result in a material degradation of the platform's security posture. 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