# Enterprise Data Loss Prevention (DLP) Privacy

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 information may be captured, processed, and stored by and within the service.

Palo Alto Networks Enterprise 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.

## Product Summary

DLP is integrated with Palo Alto Networks products (hereinafter called "channels") such as Prisma™ SaaS, 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 in order to protect sensitive data that is at risk.

## Information Processed by DLP

Palo Alto Networks DLP discovers and protects sensitive information in data at rest stored in software-as-a-service (SaaS) apps—such as Office 365®/Microsoft 365™, GSuite®, and Box—and in data in motion over the networks.

DLP scans files against predefined or customer-defined data patterns. Each data pattern corresponds to a type of information that a customer is looking to detect and protect. For example, there is a data pattern for US Social Security numbers and one for credit card numbers. There are also machine learning-based classifiers that are used to determine whether files contain other types of sensitive data. Verdicts are used to take remediation action on a per-channel basis.

DLP analyzes files to detect violations of customer-enabled policies. For example, if the customer wants to protect credit card numbers from loss or exfiltration, DLP will scan the files against the credit card data pattern and provide visibility as well as 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. For certain channels, the customer administrator can configure the information displayed in the snippet.

Logs generated by DLP, across all channels, show information including but not limited to occurrences of policy violations, the file metadata, and risk assessment summaries.

## Purpose of Information Processed by DLP

The purpose of processing information through DLP is to detect sensitive information such as Social Security numbers, national IDs, credit card numbers, etc., and to prevent that data from being exfiltrated, if possible. For additional details, please consult the technical documentation in the Resources section at the end of this document.

## How DLP Addresses EU Data Protection

Processing personal data to ensure network and information security, including through a cloud-based data processor, is broadly recognized as a "legitimate interest" and specifically called out as such in the EU General Data Protection Regulation:

*(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.*

Where a service provider, such as Palo Alto Networks, processes personal data to ensure data security, this is a legitimate interest of the service provider and its customers, providing a basis for the processing of personal data by Palo Alto Networks under EU data protection laws.

This legitimate interest generally also provides a basis for customers scanning personal data in the cloud or monitoring network traffic for exposure of sensitive data, in accordance with privacy or regulatory requirements.

## How Palo Alto Networks Complies with Data Protection Rules

Palo Alto Networks is committed to protecting personal data processed by DLP. Data stored on or processed by Palo Alto Networks systems is secured with state-of-the-art technologies, and Palo Alto Networks operates rigorous technical and organizational security

controls. As Palo Alto Networks is a multinational company, there may be a need, in some cases, to share information with Palo Alto Networks offices in other regions. We will do so in compliance with applicable requirements for transfer of personal data, including the EU Standard Contractual Clauses as approved by the European Commission, or other legal instruments for the transfer of personal data, provided for in EU data protection law.

## Subprocessors

DLP utilizes Amazon Web Services (AWS®) and Google Cloud Platform (GCP®) for hosting, and MongoDB® Atlas for configuration management. DLP logs and snippets are stored in the same region selected by the customer for the channel with which DLP integrates. Configurations are stored centrally.

## Privacy Options

Customers' system administrators can configure which users can be authorized to view data and logs through the respective channel's user interface.

## Access to Data

### Customer Access

Customer users can view snippets and logs through each channel's user interface.

### Palo Alto Networks Access

Data stored within the customer's DLP instance can only be accessed by the customer's administrator or by users authorized by the administrator through the channel DLP is protecting. When a support case is opened, access to the data may be requested for the purposes of troubleshooting, solving issues, and improving the effectiveness of security protections. Additionally, Palo Alto Networks applies a business-need-to-know policy to maintain privacy and protect confidentiality.

## Retention

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:

- **Prisma SaaS**: Prisma SaaS 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 located in the SaaS vendor cloud and scanned again for sensitive content. Newly generated snippets are stored in Prisma SaaS for a period of 30 days.
- **Prisma Cloud Data Security, Prisma Access, and NGFWs**: Snippets and logs are stored in DLP for a period of 90 days. Sensitive content is masked by default, but this is configurable. Customers have the ability to turn off the snippets feature altogether, in which case no snippets data is stored.

Upon expiration of the DLP and channel license, data will remain available for customer access for 90 days, after which it will be removed.

## Security

Palo Alto Networks operates rigorous technical and organizational security controls. Data in transit from the channel to the DLP service is encrypted via TLS. Data stored in MongoDB Atlas is encrypted at rest. Palo Alto Networks has achieved SOC 2 Type II and ISO 27001 certification for DLP to demonstrate its strong security policies and internal controls environment.

## Resources

- DLP Resource Page
- DLP Documentation
- Palo Alto Networks Product Privacy Datasheets

## 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.

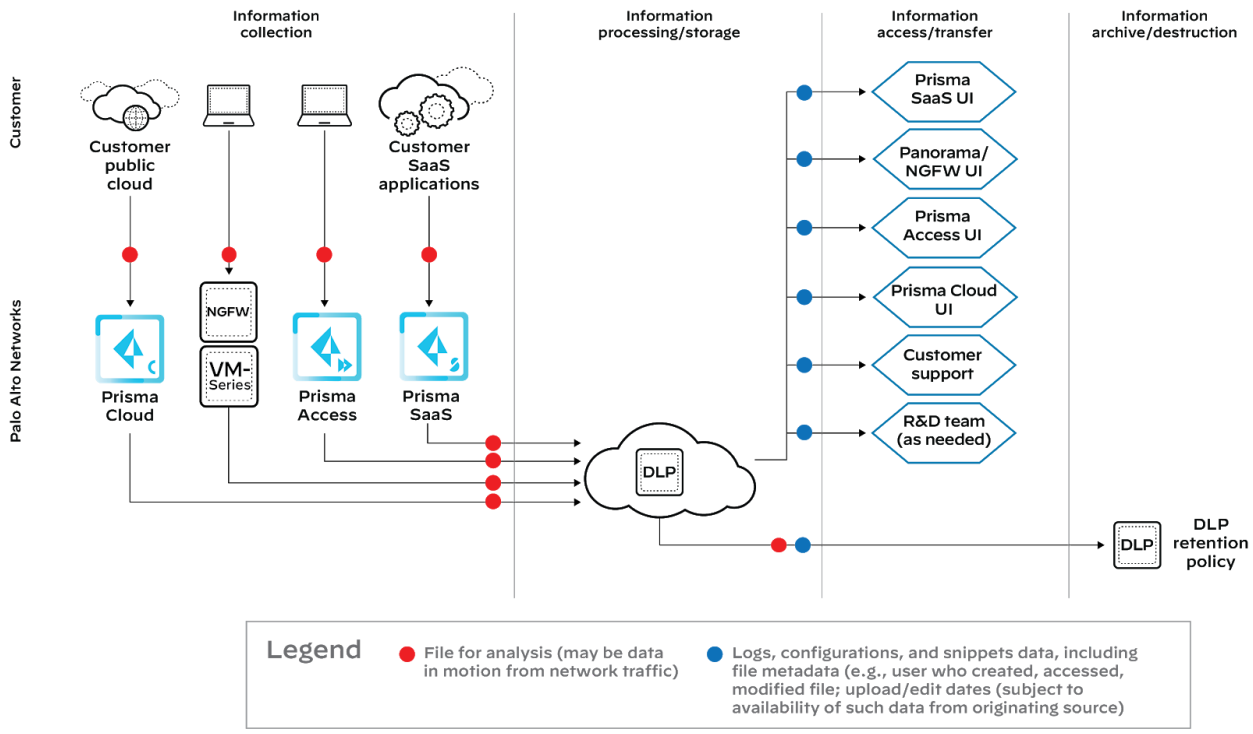


**Figure 1:** Data flow diagram