# APERTURE – PRIVACY DATASHEET

Palo Alto Networks® engaged independent data privacy risk management provider TRUSTe® to review and document the data flows and practices described in this datasheet. 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.

## PRODUCT SUMMARY

Aperture™ SaaS security service provides cloud-based security within SaaS applications (e.g., Box®, Google® Drive, Salesforce®). Aperture scans the files stored in the SaaS applications, in accordance with rules and policies determined by the customer, and monitors them for unauthorized or inappropriate disclosure or handling of information as well as for malware activity.

### Information Processed By Aperture

Aperture makes a temporary copy of all data stored in SaaS services to which the customer has enabled access. Aperture copies the files for analysis in secure multi-tenant environment hosted in Amazon Web Services (AWS) cloud.

Aperture analyzes the files to detect violations of the customer's policies. The results of the scan for each file are stored in Aperture and made available to the customer through reporting features in the interface. Aperture stores the results of each file's analysis, along with any metadata about that file, such as file creation and access dates and the usernames of those who created and accessed the file. The specific metadata available for capture by Aperture varies based on the metadata made available by the SaaS service.

Aperture looks for known patterns of data, such as Social Security and credit card numbers or other violations of the policies determined by the customer. If the analysis identifies a violation of policy, a snapshot example of the data found, with approximately 100 bytes of data adjacent to the identified content, is captured and logged in the Aperture system. Sensitive data, such as Social Security numbers, are masked by default.[1]

### Customer Privacy Options

Customers configure Aperture to access the SaaS services they want to monitor. Customers' systems administrators determine which users can be authorized to view data and reports in the Aperture interface.

### Access to Data

Each customer's system administrator controls access to Aperture reports and stored metadata, and access is limited to users who are authorized by the administrator. Data contained within the customer's Aperture environment may be accessed by Palo Alto Networks Customer Support teams exclusively for troubleshooting purposes and only if the customer's administrator enables access. All such access is logged and can be reviewed by the customer. The customer's administrators have the option to unmask sensitive data.

[1] A complete list of data elements masked by default includes: Credit card numbers, magnetic stripe data, international bank account numbers (IBAN), US Tax ID, Australian Tax ID, UK Tax ID, German Tax ID, US Social Security Number, Canada Social Insurance Number.

## Retention

The temporary copying of files analyzed by Aperture is deleted within 48 hours. User-activity data logged in the Aperture system is retained by Palo Alto Networks for 90 days. Metadata about analyzed files is retained, as long as the customer keeps the service active. Palo Alto Networks deletes data collected during an Aperture trial or proof-of-concept account upon the expiration of the trial account (90 days), or within 24 hours if the account is proactively canceled by the customer.

## Security of Data in Aperture

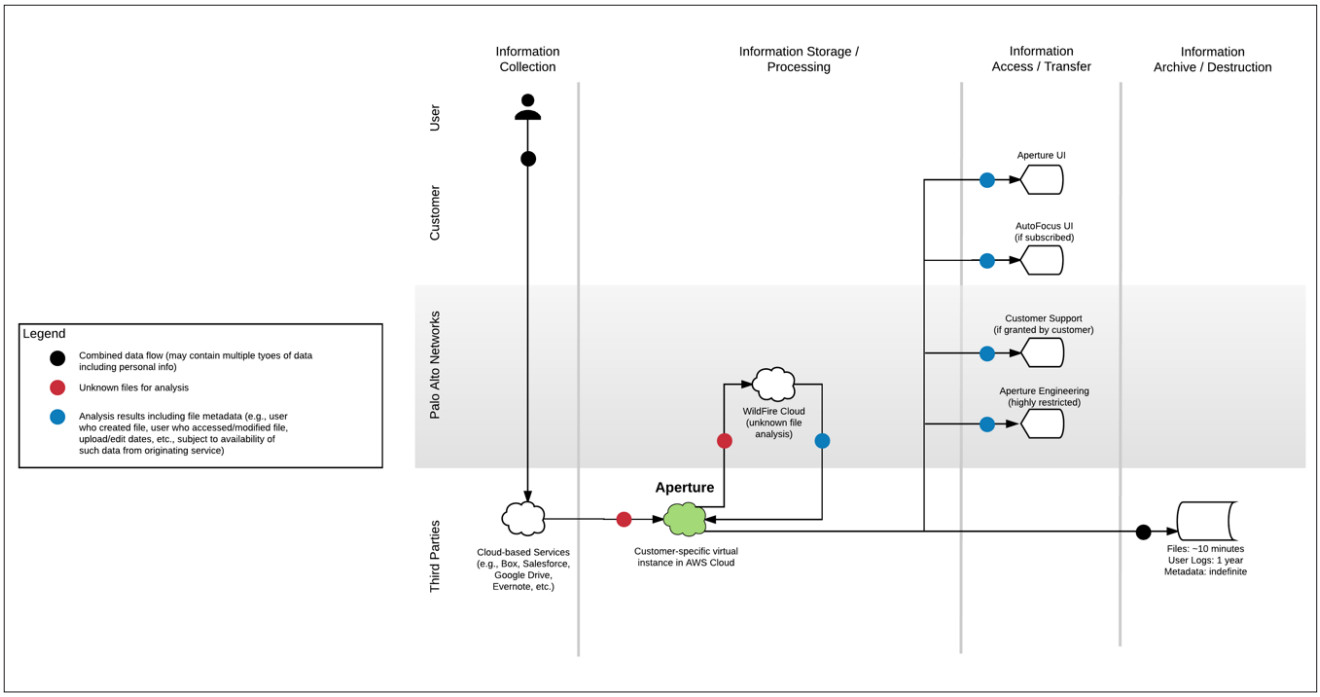
Metadata and scan results are encrypted while in the Aperture environment. Each customer has a unique and exclusive key to encrypt and decrypt such data, and all processing occurs in a virtual environment dedicated exclusively to that customer. Data is transferred from SaaS applications to the Aperture environment using SSL/TLS to the extent enabled by those applications. All data stored within the customer's Aperture instance can only be accessed by the customer's administrator or users authorized by the administrator.

## Resources

Additional information about Aperture is available in the following resources:

- **Aperture At A Glance** - https://www.paloaltonetworks.com/resources/datasheets/aperture-at-glance
- **Aperture Solution Brief** - https://www.paloaltonetworks.com/resources/techbriefs/aperture
- **Aperture Lightboard Video** - https://www.paloaltonetworks.com/resources/demos/aperture-lightboard-demo
- **Technical Documentation** - https://www.paloaltonetworks.com/documentation/

*Dataflow*




## About This Datasheet

*The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TRUSTe has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, 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.*


4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com