Cisco Secure Network Analytics

(formerly, Cisco Stealthwatch Enterprise)

This Privacy Data Sheet describes the processing of personal data (or personal identifiable information) by Cisco Secure Network Analytics (formerly, Cisco Stealthwatch Enterprise).

Secure Network Analytics is an on-premise solution and is not hosted or operated by Cisco and therefore, Cisco does not access or process any personal data from it except as provided in this privacy data sheet (if any) or unless it is provided to Cisco by the customer.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

Secure Network Analytics is an on-premise offer included in the Cisco Secure Analytics portfolio. Secure Network Analytics provides visibility and security analytics that leverages enterprise telemetry from the customer's existing network infrastructure. It provides advanced threat detection, accelerated threat response and simplified network segmentation using multi-layer machine learning and advanced behavioral modeling, all across the extended network. With Secure Network Analytics, customers get real-time visibility that helps to gain better insight into activities occurring within the network. At the core of Secure Network Analytics are the Flow Rate License, the Flow Collector, Management Console and Flow Sensor.

Secure Network Analytics is Smart License enabled. Personal data may be provided to Cisco in the form of a user credential to associate it with a related Cisco.com account (i.e. CCO) or Smart License account. For more information regarding Smart License account and related data collection, please refer to the Smart Software Licensing Privacy Data Sheet.

Global Threat Alerts (formerly, Cognitive Intelligence), a cloud-based malware behavioral analysis feature, is available on an opt-in basis to Secure Network Analytics customers with their license. In addition, Secure Cloud Analytics (formerly, Stealthwatch Cloud) is available to Secure Network Analytics to trial on an opt-in basis. Please refer to the Cisco Privacy Data Sheets for Global Threat Alerts (formerly, Cognitive Intelligence) and Secure Cloud Analytics (formerly, Stealthwatch Cloud) for a list of the data categories and types of personal data collected, processed and stored by these cloud-based services.

2. Personal Data Processing

Cisco does not collect personal data from Secure Network Analytics (except in connection with the optional cloud-based services referenced above). For personal data used by Secure Network Analytics but retained on-premise under a customer's control, please see the table below. The personal data used by Secure Network Analytics but retained under customer's control may change from time to time so please see the product documentation for updates.

Personal Data Category	Types of Personal Data	Purpose of Processing
User Account Information (Collected and stored within the on-premise Secure Network Analytics appliance)	• Name • Email Address • User ID/name	Authentication of customer's users.

By default, Cisco collects non-personally-identifiable usage data to assist Cisco with understanding product usage, enable product improvements, and assist our customers with their product adoption. For more information on how Cisco uses this type of usage data, please see the Systems Information Data Brief. Some non-personal usage data may be shared with Google Analytics. Customers may opt-out of sharing this data with Google Analytics within the configuration settings of the product (go to Central Management / SMC Appliance / Edit Appliance Configuration / General tab / External services).

3. Data Center Locations

Secure Network Analytics is not hosted or operated by Cisco. It is an on-premise solution. Location of data centers is determined by Customer.

4. Cross-Border Transfers

Secure Network Analytics is not hosted or operated by Cisco. Data transfer mechanisms, if required, are the responsibility of the Customer.

5. Access Control

Secure Network Analytics is not hosted or operated by Cisco and therefore, it is the Customer's responsibility to determine who has access to what personal data and for what purposes access is granted.

6. Data Portability

Data Portability requirements do not apply to Secure Network Analytics.

7. Data Deletion and Retention

Secure Network Analytics is not hosted or operated by Cisco and therefore, it is the Customer's responsibility to determine the length of time that data needs to be retained, and why it is retained.

8. Personal Data Security

Secure Network Analytics is not hosted or operated by Cisco and therefore, it is the Customer's responsibility to determine security requirements

9. Sub-processors

Secure Network Analytics is an on-premise product and therefore use of sub-processors is determined by the Customer.

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco's

response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The Cisco Security Center details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber's relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Requirements

The Security and Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The product is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to privacy and information security, including:

- Binding Corporate Rules
- EU-US Privacy Shield Framework
- Swiss-US Privacy Shield Framework
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors

12. Exercising Data Subject Rights

Means and method to respond to Data Subject Rights requests is determined and managed by the Customer. Secure Network Analytics is an on-premise solution and is not hosted or operated by Cisco, nor does Cisco have access to the personal data it processes.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy Program please visit The Cisco Trust Center.

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the Personal Data Privacy section of the Cisco Trust Center.