

Corelight Sensor Privacy Datasheet

This Privacy Datasheet document describes the personal data that may be processed by Corelight's Sensor products. Corelight Sensors are deployed as on-premise appliances or within customer-hosted virtual systems and/or cloud environments.

Corelight Sensor Overview

By default, all processing and storage occurs on Corelight Sensors, local to the customer's environment. Corelight does not process, store, or access any data unless the Sensor's Corelight Cloud Service ("CCS") features are enabled (i.e., "call home" functionality). If a Sensor's CCS features are enabled, then Corelight processes certain categories of health information, functional configuration and performance data pertaining to the Corelight Sensor (collectively, "Usage Data") as outlined below.

Categories of personal data processed and stored by Corelight CCS features

Data Source	Data Elements	Categories of Personal Data	Purpose of Processing
By default, all processing and storage occurs on Corelight Sensors, local to the customer's environment. If a Sensor's optional CCS features are enabled, then Corelight processes and stores:			
Usage Data	<u>Health Information</u> Includes the Sensor's disk status, operating temperatures, power supplies system logs (which contain operating system status messages and mirrors of diagnostic syslog messages). <u>Functional Configuration</u> Includes the Sensor's hostname and IP address, basic system information, virtual sizing (CPU, memory and disk), service status, installed Zeek packages, installed licenses, names of Zeek logs and any custom OS installed packages <u>Performance Data</u> Aggregated statistics derived from the network traffic monitored by the Sensor (such as data volume and packet drops). This statistical data <i>does not</i> include any payload information or identify entities in network traffic).	Usage Data is typically non-personal data but may include limited categories of personal data: IP addresses Hostnames Username	To (i) provide support services and resolve technical issues; (ii) monitor product health and operation; (iii) optimize and improve the performance of Corelight products and services.

Access to the personal data processed by Corelight CCS features

The table below outlines who can access personal data and the purpose of the access.

Personal Data Source	Who Has Access	Purpose of the Access
If a Sensor's optional CCS features are enabled:		
Usage Data	Corelight*	To (i) provide support services and resolve technical issues; (ii) monitor product health and operation; (iii) optimize and improve the performance of Corelight products and services.

**Only specific authorized Corelight personnel have access to the Usage Data through authenticated, audited, and controlled access.*

How Corelight protects personal data

When a customer elects to enable the Sensor's optional CCS features, Corelight protects the personal data provided as part of the Usage Data by implementing technical and organizational security measures designed to protect the confidentiality, integrity and availability of such personal data.

Personal Data Source	Security Measures
If a Sensor's optional CCS features are enabled:	
Usage Data	Data in transit is encrypted using TLS-encrypted transmission. Data at rest is encrypted using cryptographic service provider techniques.

Retention and deletion of personal data

The personal data retention practices and the purpose of such retention are outlined below.

Personal Data Source	Retention Period	Purpose of Retention
If a Sensor's optional CCS features are enabled:		
Usage Data	Corelight retains Usage Data for the lifecycle of each Corelight Sensor.	To (i) provide support services and resolve technical issues; (ii) monitor product health and operation; (iii) optimize and improve the performance of Corelight products and services.

Portability of personal data processed by Corelight CCS features

Corelight does not provide customers with API access to Usage Data. Some data made available in connection with certain Corelight offerings (e.g., Corelight's Health Check Service) may be released pursuant to the confidentiality obligations set forth in the [Corelight Customer Agreement](#).

Data center locations where Corelight processes personal data

Usage Data will only be processed by Corelight when a customer elects to enable the Sensor's optional CCS features. In such case, the Usage Data processed by Corelight is stored within a managed IaaS infrastructure within the continental United States.

Personal Data Source	Data Center Provider	Data Center Location
If a Sensor's optional CCS features are enabled:		
Usage Data	Amazon Web Services, Inc.	United States