Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Data Loss Prevention (DLP) - Information Centric Analytics (ICA)

This Privacy Transparency Notice describes how Data Loss Prevention (DLP) - Information Centric Analytics (ICA) ("Product") collects and processes Personal Data. Its purpose is to provide You (our current or prospective "Customer") the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

Information Centric Analytics (ICA) is a software solution that leverages advanced analytics to provide an integrated, contextually-enriched view of cyber risk across the enterprise by ingesting, aggregating and analyzing Data Loss Prevention (DLP) incident data. ICA builds on the data generated by DLP to deliver a prioritized list of entities whose behaviors indicate elevated cyber risk with automated investigation and remediation capabilities, along with a consistent, top-down view of security and risk for application across IT teams, line of business leaders, and the C-suite.

Further information about the Product is available at:

https://www.symantec.com/products/information-centric-analytics

2. Personal Data Collection And Processing

Sources of Data

ICA integrates directly with DLP to provide the analytics and visibility necessary to isolate those activities that represent real-world risks. The telemetry and data is collected by the DLP systems and analyzed by the ICA software within the Customer environment.

Respective Roles of Symantec and Customer

With respect to Personal Data collected by the Product during its use, the Customer is the Controller. The use of the Product does not involve Symantec as a Data Processor.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Individual identifiers, online identifiers and trackers, network activity data, communications data	Customer employees, contractors, visitors and other business contacts who conduct network-based communications in or from the customer's protected environment	To detect violations of customer-defined DLP policies
Any categories of Personal Data, potentially including Special Categories, which the customer configures to protect in its policies	Customer employees and contractors and any other individuals whose personal data is protected by the customer's DLP policies	To enable the analysis, reporting, investigation and remediation of violations of customer-defined DLP policies

Personal Data Retention Schedule

As the Controller, the Customer is solely responsible for defining and implementing the retention policies and periods applicable to Personal Data collected through the use of the Product. The use of the Product does not involve Symantec as a Data Processor.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and, if applicable, external recipients (third party sub-processors), in the facilitation or provision of the Product. The list of Symantec affiliated entities and their geographical locations are available on the Symantec Privacy - GDPR Portal.

Third-Party Sub-Processors

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

As the Controller, the Customer is solely responsible for complying with any rules applicable to the international transfers of Personal Data that the Customer collects by using the Product. The use of the Product does not involve Symantec as a Data Processor.

4. Exercise Of Data Subject Rights

As the Controller, the Customer is solely responsible for complying with any rules applicable to the exercise of Data Subject Rights related to Personal Data that the Customer collects by using the Product. The use of the Product does not involve Symantec as a Data Processor.

5. Information Security

Technical and Organizational Measures

As the Controller, the Customer is solely responsible for complying with any rules applicable to the security of the processing of Personal Data that the Customer collects by using the Product. The use of the Product does not involve Symantec as a Data Processor.

Security documentation about the Product itself is available on the Symantec Customer Trust Portal.

Applicable Information Security Certifications

1.) The Product is FIPS 140-2 compliant by leveraging the following two cryptography modules:

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2606

https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2605

2.) The Product implements U.S. NIST approved crypto controls to protect sensitive data

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.