Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec™ Endpoint Threat Defense for Active Directory

This Privacy Transparency Notice describes how Symantec™ Endpoint Threat Defense for Active Directory ("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

The Product is designed to protect computers and servers against credentials theft, reconnaissance and lateral movement in a domain environment. This is achieved by obfuscating the Microsoft Active Directory (AD) structure.

Further information about the Product is available at:

https://www.symantec.com/products/endpoint-protection

2. Personal Data Collection And Processing

Sources of Data

The Product collects domain data (information about machines, users, AD sites and segments) from the Domain Controller using GSSAPI (*Generic Security Service Application Program Interface*) encrypted LDAP (*Lightweight Directory Access Protocol*) protocol. It utilizes this information in machine learning to generate obfuscated data tailored for the data collected from the Active Directory.

The Product collects forensics data from a computer or server in the organization which generated an alert. The data is collected from the endpoint, using a secure line of communication over SMB (*Server Message Block*).

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
Online identifiers, network and system location data	Customer employees, contractors and other users present in the Active Directory of the Customer's protected environment	Product configuration, administration and management
Network activity and electronic communication metadata	Customer employees, contractors and other users present in the Active Directory of the Customer's protected environment	Incident forensics (unless disabled by the Customer)

The Product does not need and is not meant to collect or process any Special Categories of Personal Data. However the Product has machine learning capabilities to conduct automated analytics in order to determine normal usage and behavior profiles so as to detect suspicious actions, events or behaviors that may lead to, or constitute incidents. Customers should seek qualified legal advice and assistance on the regulatory and other requirements that may be applicable to the deployment and use of such technologies in their I.T. environment.

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

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.

For the purposes of the Product, every user role, as assigned by the Customer, has access to view forensics data and export it from the web console without Symantec intervention. Admin role, as assigned by the Customer, has the ability to delete certain data elements, specifically forensic details of an endpoint in an incident.

5. Information Security

Technical and Organizational Measures

The data collected and stored by the Product can only be accessed using valid credentials in the Product's web console. The access to the data in the web console happens through HTTPS. The collection of data is encrypted either using GSSAPI Kerberos encrypted LDAP, or on encrypted SMB channel. By default every user who has access to the web console has access to all of the information as well, unless otherwise configured by the Customer.

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.