Symantec Advanced Threat Protection Platform with Network and Endpoint Privacy Notice

Effective: September 14, 2016

Purpose and Scope

This Privacy Notice explains what data Symantec collects or processes from You and what we do with this data when You use Symantec Advanced Threat Protection Platform with Network and Endpoint ("ATP"), and applies to data collected through or related to Your use of the Symantec ATP. Unless otherwise specified, this Privacy Notice does not apply to any other products/services or to data collected in any other way (online or offline) or for any other purpose.

Automatically Collected and Transmitted Information ("Transmitted Information")

ATP collects from Your environment, and automatically transmits to Symantec, data, which may include, without limitation:

- All information collected by Symantec Endpoint Protection;
- Administrator contact information, email address and portal password;
- Software configuration, product details, installation status;
- System and content update information;
- License file, name, version, language and status, license entitlement information, license ID and license usage;
- Device name, Machine Name, host name type, OS version, language, location, browser type and version, IP address and ID;
- File reputation metadata, including hash, URL and digital signature information;
- Android app (APK) reputation metadata including hash, package name and signer information;
- Network detection event information, including file samples sent for analysis and file analysis results;
- Log files of all network inspection events;
- Information on potential security risks and URLs of websites contacted deemed to be potentially fraudulent (such URLs could contain personal information that a potentially fraudulent website is attempting to obtain without Your permission), portable executable files and files with executable content that are identified as malware, and which may contain personal information, including information on the actions taken by such files at the time of installation;
- For files identified as potential malware: metadata including hash, file MIME type, IP address, as well as corresponding URL, HTTP headers, FTP domain/path, java applet tags and the full file;
- For optional diagnostic features: Failure data including failure reports, crash dump information, log files, as well as the temporary files, configuration files and database tables related to the failure;
- For optional telemetry features:
  - LiveUpdate error metadata (for further information see below);
  - File scan error metadata;
  - Conviction metadata including timestamp, machine ID, conviction threshold, severity rating, action taken, config version, host name, local and remote IP and ports, URL, Referrer URL, conviction classification, malicious file metadata, blacklist classification, malware signature information, confidence score and virus metadata;
  - Device statistics on number queries, average and maximum latency, cancellations, convictions, clean findings, errors, total numbers of files scanned and files convicted, system health metadata, certificate metadata and aggregated network failure and usage statistics;
- For optional event correlation features: relevant appliance IP and internal network IP ranges covered, malware conviction related metadata (as above), and metadata of emails blocked by Email Security Service including envelop information and attachment conviction metadata;
- For optional support features: files You share with Support;
- Personal Information provided by You during configuration of the Service or any other subsequent service call.

Transmission of certain of the above Transmitted Information may be deactivated during and after installation by following the instructions in the documentation for ATP. Submission of the Transmitted Information is not required and You will be able to use ATP even if You do not submit the Transmitted Information to Symantec. You may elect to request that Symantec delete files submitted for inspection by following the instructions in the documentation for ATP.

In addition, certain information listed above is only transmitted in the event You choose to do so and have enabled certain optional features of this product or related products such as Symantec Endpoint Protection Management.

ATP utilizes the LiveUpdate functionality. For information about the LiveUpdate functionality, please refer to the LiveUpdate Privacy Notice.

For purposes of this Privacy Statement, "personal information" means information that can be used to reasonably identify an individual. We may also collect Your personal information when You contact us about any Symantec product or service, such as for technical support.

Automatically Collected and Stored Data ("Stored Data")

ATP collects from Your environment, and stores in Your environment, data, which may include, without limitation:

- Locally quarantined files
- Conviction metadata as per the above

The above Stored Data is used to enable the functionality of ATP, is not transmitted back to Symantec and, by itself, is anonymous.

ServiceNow Application

The ServiceNow Application synchronizes incidents and incident-related events from the ATP appliance to the ServiceNow cloud platform and transfers data which may include, without limitation, Transmitted Information.

How We Use Your Transmitted Data or Personal Information (collectively, "Information")

Transmitted Information may be used as follows:

- Enabling and optimizing the performance of ATP;
- Limiting damage done by installed malware;
- Providing support or debugging assistance;
- Sending You or others promotional information, in accordance with Your permission, as required by applicable law;
- Deriving statistics from Your data to track and publish reports on security risks/trends;
- Research and development, such as improving Symantec's products or services (e.g., to better protect You, such as by using data analytics to protect Your network/data);
- License administration;
- Combating fraud or any other criminal activity;
- For any other purpose with Your consent; and/or
- In an anonymized and/or aggregated form for the general security research purposes of:
  - Improving the detection of malware;
  - File sample analysis to discover advanced malware; and/or
  - Internal research and development, including improving Symantec's products and services; and/or

- Statistical analysis of product deployment, including analysis of trends and comparisons in our aggregated install base.

How We Transfer, Store and Disclose Your Transmitted Information

We are a global organization and may transfer Your Information to other countries, including countries that may have less protective data protection laws than the country in which You are located (including the European Union). For the purposes described in this privacy statement, Your Information (i) may be stored and processed manually and/or electronically through global systems and tools, (ii) may be disclosed to vendors or third parties that process data on behalf of Symantec, (iii) may be disclosed in connection with any proposed or actual sale or other transfer of some or all assets of Symantec in the event of a reorganization, merger, acquisition, or sale of our assets; and/or (iv) may be disclosed as otherwise permitted by You.

To promote research, awareness, detection or prevention of security risks, Symantec may disclose Information to relevant public and private entities such as cybersecurity research organizations and security software vendors. In such cases, we will endeavor to anonymize such information or to minimize any personal information in it to the extent reasonably possible without defeating purposes of security risk research, awareness, detection or prevention.

Subject to applicable laws, Symantec reserves the right to cooperate with any legal process, or any law enforcement or other government inquiry, related to Your use of ATP, including disclosing Information if relevant to a court subpoena or to a law enforcement or other government investigation, or as otherwise required by our legal obligations.

How We Protect Your Information

To protect Information, we have taken reasonable and appropriate administrative, technical, organizational and physical security and risk management measures, in accordance with applicable laws.

Your Obligation to Personal Information

It is Your responsibility to ensure that any disclosure by You to Symantec of personal information of Your users or third parties is in compliance with applicable privacy and data security laws, including informing users and third parties that You are providing their personal information to Symantec, informing them of how it will be transferred, used or processed, and gathering appropriate consents and other legal measures required for such transfer, use or processing.

Data Access

Under certain circumstances, You may be able to request to access, update, correct or remove personal information we have about You. We may retain certain Information if necessary to prevent fraud or future abuse, or as otherwise required or permitted by law.

Contact Us

Please contact us at privacyteam@symantec.com if You have any questions.

Changes To This Privacy Notice

We reserve the right to revise or modify this Privacy Notice, and will note the date of its most recent revision above. If we make significant changes to this Privacy Notice, and where required by applicable law, we will either notify You either by prominently posting a notice of such changes prior to implementing the changes or by directly sending You a notification.