Tanium Engage Privacy Datasheet

What Is Tanium Engage?

With Tanium Engage, you can create surveys to collect qualitative feedback from endpoint users and deploy remediations to correct problems on the endpoints. The questions in a survey can be unique to that survey, or they can be copied from template questions that you can create. Each question is multiple choice and can have one response.

Organizations use Engage to monitor, manage, and improve their employees' digital work experience at scale with self-service automation.

What Data Privacy Issues Relate to Tanium Engage?

Tanium Engage in its default configuration uses username and endpoint name identifiers in collecting survey responses from end users. An organization may configure Engage to collect additional sensitive and/or personal data as part of custom survey questions, and such information may be made visible in the Engage dashboard to an organization's authorized users, and in limited circumstances to Tanium personnel as part of operations and troubleshooting support.

What Types of Personal Data Does Engage Detect?

Tanium Engage collects endpoint name and survey participant username in collecting user responses to survey questions. Data is collected from the endpoint via Engage specific platform sensors. These sensor results are stored in the organization's Tanium Could instance. Survey results can optionally be anonymized depending on the organization's configuration on a per-survey basis—username and endpoint name are not collected when this option is enabled. Username and endpoint data is visible to the organization's authorized users in the Engage workbench when viewing the survey details pages and via the "Engage - Survey Results" platform sensors. Further, the Tanium Directory Query Service (DQS) can optionally be configured by the organization. If DQS is configured, additional user metadata such as email addresses and department will be visible via the Engage workbench.

When Might Engage Identify Sensitive Data?

In its default configuration, Tanium Engage does not collect sensitive data. Organizations may create custom Engage surveys that ask questions pertaining to sensitive.

Does Engage Store Personal or Sensitive Data?

Engage survey results are collected and stored on the endpoint. Tanium sensors collect this survey results and metadata and store it in the Tanium Data Service (TDS) on the Tanium Cloud server.

Who Can See the Data Viewed in Engage?

Sensitive and/or personal data viewed in Engage's dashboard is visible to the authorized user's of the organization based on that organizations rule based access control (RBAC) configuration, and in limited instances to Tanium support personnel as described below.

Do Tanium Personnel Have Access To Personal and/or Sensitive Data Through Engage?

Under normal operations, only the Tanium user (i.e., the organization's user) has access to the Engage console. For Tanium Cloud, Tanium automates most management operations while intentionally limiting its own access to the organization's data. On rare occasions, a Tanium engineer may need limited and logged access to an organization's data for a brief duration, but only when necessary for normal service operations and troubleshooting, and only when approved by a senior member of the Engineering Team at Tanium.

Where Might I Learn More about Engage

Tanium Engage User Documentation is available here:
https://docs.tanium.com/engage/engage/index.html

About This Datasheet

Please note that the information provided concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable law. This document does not create, define, or represent any contractual relationship between you and Tanium. The terms of your agreement, if any, are set forth in your specific customer sales, user, and/or subscription agreements.