Tanium Enforce Privacy Datasheet

What Is Tanium Enforce?

Tanium Enforce provides endpoint management and security by providing centralized policy management and device configurations on endpoints. Enforce operates across operating systems regardless of device location: on-premises, remote, or cloud.

For example, organizations use Enforce to set policy on endpoints for native operating system functionality such as local policy, Bitlocker, Applocker, Windows Defender, and USB Device control.

What Data Privacy Issues Relate to Tanium Enforce?

Tanium Enforce allows an organization to configure and view policy settings on an endpoint. Configuring and viewing policy settings on an endpoint may include collection of IP addresses, computer names, and disk encryption recovery keys.

When Might Enforce Identify Personal Data?

Data collected by Tanium Enforce includes IP addresses and computer names. Organizations may configure and use Enforce to collect other types of personal data.

When Might Enforce Identify Sensitive Data?

Enforce scans include the identification of disk encryption recovery keys for macOS and Windows, which may be considered sensitive data. This data is also used by Enforce to apply related policies such as a Disk Encryption policy. Organizations may configure and use Enforce to identify other types of sensitive data.

Does Enforce Store Personal or Sensitive Data?

Enforce does collect and store personal and sensitive data. Disk encryption recovery keys may be stored on the Tanium Module Server or in the case of Tanium Cloud are stored in the customer's individual environment in Tanium Cloud.

Who Can See the Data Viewed in Enforce?

The organization's Enforce users with specific rights to view Disk encryption recovery keys can also view sensitive and/or personal data, and in limited instances Tanium support personnel may view the data as described below.

Do Tanium Personnel Have Access to Sensitive Data Through Enforce?

Under normal operations, only the organization's user has access to the Enforce 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 Enforce

Tanium Enforce User Documentation is available here: https://docs.tanium.com/enforce/enforce/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 sales, user, and/or subscription agreements.