Tanium Integrity Monitor Privacy Datasheet

What Is Tanium Integrity Monitor?

Tanium Integrity Monitor is used to manage IT compliance across networks. Integrity Monitor continuously monitors critical operating system (OS), applications, log files, and critical Windows registry paths for changes and other events. Integrity Monitor also provides a single console, agent, and infrastructure to help complete compliance, security, and IT operations tasks in combination with other modules and tools.

What Data Privacy Issues Relate to Tanium Integrity Monitor?

Tanium Integrity Monitor can be customized by organizations to monitor files and registries based on organization-created Monitors and Watch Lists. Integrity Monitor identifies and logs which organization's user changes a file or path. However Integrity Monitor does not read or store the changes themselves.

What Types of Personal Data Does Integrity Monitor Detect?

Based on the customization and use by organizations, Integrity Monitor may collect the identity of users who trigger monitored events. Integrity Monitor does not read or store the contents of files or registries.

What types of Sensitive Data Does Integrity Monitor Detect?

Tanium Integrity Monitor can be configured by an organization with watchlists for CREATE, WRITE, DELETE, RENAME, & PERMISSION file changes. These organization defined watchlists might include changes to sensitive files, folders, and registry keys. Data within the files is not exposed by Integrity Monitor.

Does Integrity Monitor Store Personal Data?

Integrity Monitor may store in logs the identity of users who triggered the monitored events discussed above.

Who Can See the Data Viewed in Integrity Monitor?

An organization's Tanium Administrator and other authorized Integrity Monitor users can see the data and events triggered by Tanium Integrity Monitor.

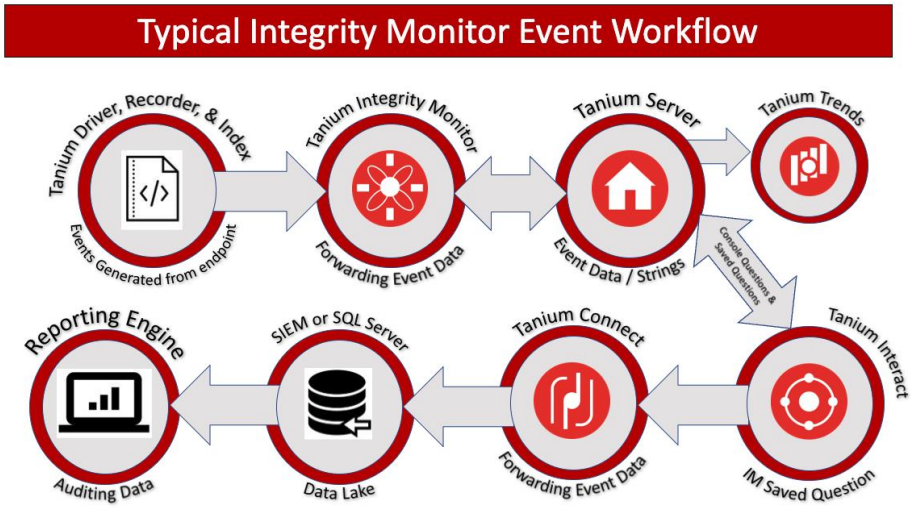
Do Tanium Personnel Have Access to Sensitive Data Through Integrity Monitor?

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

© 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. Further, Tanium Lockbox provides Tanium Cloud users visibility into these accesses, and optional approval authority when they occur.

A Data Map Detailing the Data Lifecycle in Integrity Monitor



Where Might I Learn More about Integrity Monitor

Tanium Integrity Monitor User Documentation is available here:
https://docs.tanium.com/integrity_monitor/integrity_monitor/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.

© Tanium