Tanium Investigate Privacy Datasheet

What Is Tanium Investigate?

Tanium Investigate is used by organizations to resolve incidents through collaboration and activity organization. Investigate helps to identify the root cause of issues that arise on Tanium-managed endpoints and arrive at resolutions to those issues. It does so by correlating performance events and activities that come from one or multiple hosts and allowing incident investigation teams to quickly notate and triage data points in one shared workspace. Finally, Investigate features an integration with ServiceNow to capture context from an initial ticket and save Tanium annotations on a given case.

What Data Privacy Issues Relate to Tanium Investigate?

Tanium Investigate presents performance metrics over a monitoring interval such as CPU, Memory, Disk, and Network usage based on type of events configured by the organization. Investigate also records endpoint-level information about system-impacting events occurring on endpoints. The data privacy issues relevant will depend on the events of interest, as Tanium Investigate integrates with other Tanium modules (listed below) for additional analysis. For example, Tanium Patch collects data that pertains to the state of operating system updates installed or required on an endpoint. A comprehensive list of event types can be found here.

What Types of Personal and Sensitive Data Does Investigate Detect?

Investigate will identify endpoint usage and performance data, which might include sensitive information (namely, user context) based on the organization's configuration; for example, user information like End User Name may be surfaced depending on event type (e.g., User Logon events, new assignment of special privileges) or similarly, local / remote IP addresses will be visible in some cases (e.g., for network connection events like an HTTP request to an Internet location). Other events contain file paths and file names, which could potentially contain personal data; similarly, the file browser feature allows downloading files from the endpoint, which may contain personal data. Lastly, Investigate integrates with other Tanium products (see next section), which may have access to personal data.

Does Investigate Store Sensitive and/or Personal Data?

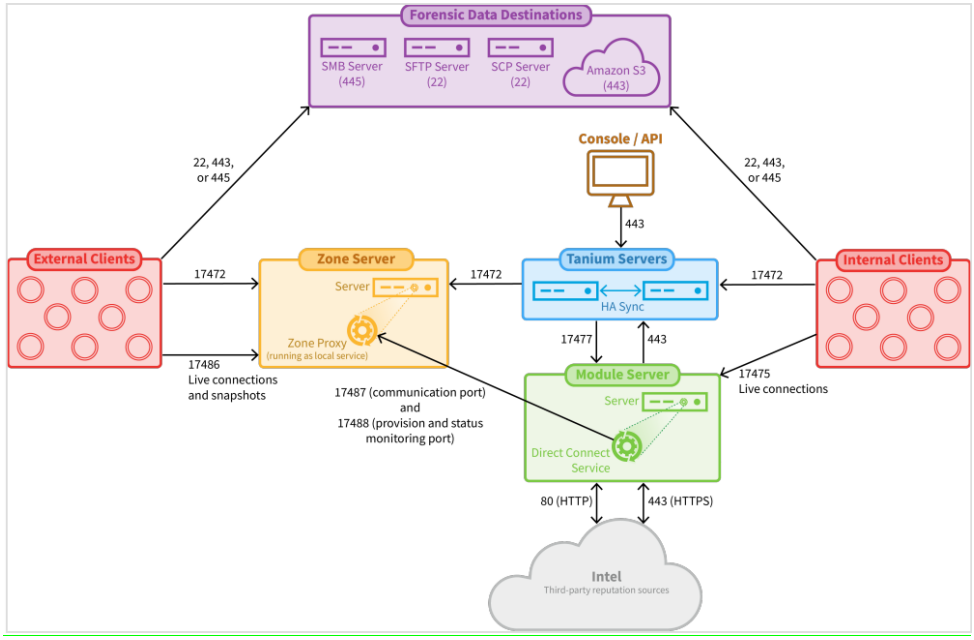
Data viewed by an organization's Investigate users stays on the endpoint on which it was discovered. If the users decide to capture artifacts of a given investigation to a saved case, this information is stored server-side to access historical information. If appropriate user permissions exist, the file system can be navigated through Investigate Direct Endpoint Connection (DEC), which allows for download of the files on the endpoint. Additionally, Tanium Investigate relies on data collected by other Tanium modules: Patch, Deploy, Enforce, Performance, Threat Response and Impact to date. For a more comprehensive understanding of data privacy implications, please read the Privacy Datasheets of those individual modules.

Who Can See the Data Viewed in Investigate?

Sensitive and/or personal data in Investigate is accessible based on an organization's privacy policies and data access privileges, such as role-based access control. By default, Investigate data is accessible to the Tanium Administrator, and may be accessible to the defined Tanium Investigate user.

Do Tanium Personnel Have Access to Sensitive Data Through Investigate?

Under normal operations, only the Tanium Administrator (i.e., the organization's user) has access to the Investigate 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. Further, Tanium Lockbox provides Tanium Cloud customers visibility into these accesses, and optional approval authority when they occur.



Where Might I Learn More about Investigate

Tanium Investigate User Documentation is available here: https://docs.tanium.com/investigate/investigate/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.