Tanium Threat Response Privacy Datasheet

What Is Tanium Threat Response?

Tanium Threat Response is used by organizations to detect, react, and recover quickly from attacks and the resulting business disruptions. Threat Response monitors activity in real time and generates alerts when potential malicious behavior is detected. Organizations can configure Threat Response intelligence to rely upon outside sources which are used to identify potential risks. Threat response continuously records key system activity across individual endpoints for historical analysis. Threat Response also includes sensors and packages which can be used to isolate incidents and limit data leakage. Finally, Threat Response can be integrated with other Tanium modules to collect and analyze additional endpoint information.

What Data Privacy Issues Relate to Tanium Threat Response?

Tanium Threat Response analyzes and records endpoint-level information about attacks and other unauthorized behavior on endpoints. The Threat Response Data Recorder captures historical telemetry events on the endpoint, such as process events, file events, and network events. In its default configuration, Threat Response identifies potentially malicious behavior based on the Tanium Signals Feed, and metadata related to those events is transmitted to the Tanium Cloud infrastructure. Organizations may customize and use Threat Response to identify specific events on endpoints, to capture Snapshots of an endpoint's historical database at a particular time, capture inspect and save specific event data on an endpoint using Live Connection, and save specified content from endpoints to selected servers using Live Response.

What Types of Personal and Sensitive Data Does Threat Response Detect?

As described above, Threat Response by default detects historical telemetry events on an endpoint, and communicates metadata related to those events to an organization's Tanium Cloud Server. The detected events may contain Personal Data and/or Sensitive Data depending on the Organization's configuration of its environment and user activity on the endpoint. Further, an organization's use of customized searches of recorded telemetry, Snapshots, Live Connection, and Live Response may capture Personal Data.

Does Threat Response Store Sensitive and/or Personal Data?

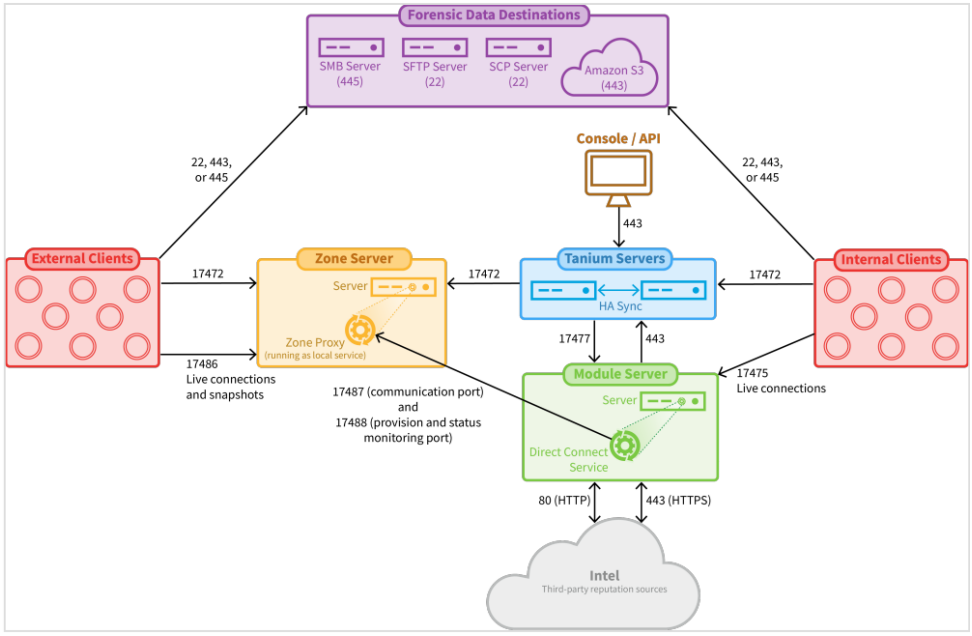
The Threat Response Recorder captures and stores historical telemetric events on the endpoint. By default, events identified by the Tanium data stream are communicated to and stored by the organization's Tanium Cloud server if they match criteria for suspected malicious activity. In addition, an organization may use Threat Response to capture snapshots of an endpoint's recorder database, or view and save individual events using Live Connect, on the Tanium Cloud server. An organization may also save specific information on other identified storage locations using Live Response. Depending on an organization's configuration of their environment, the events or snapshot may include Sensitive and/or Personal Data

Who Can See the Data Viewed in Threat Response?

Sensitive and/or personal data in Threat Response is accessible based on an organization's privacy policies and data access privileges, such as rule-based access control. By default, Threat Response data is accessible to the Tanium Administrator, and may be accessible to the defined Tanium Threat Response User. More detail regarding Threat Response's configurable permissions policy is available here.

Do Tanium Personnel Have Access to Sensitive Data Through Threat Response?

Under normal operations, only the Tanium Administrator (i.e., the organization's user) has access to the Threat Response 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 Threat Response

Tanium Threat Response User Documentation is available here: https://docs.tanium.com/threat_response/threat_response/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.