Tanium Comply Privacy Datasheet

What Is Tanium Comply?

Tanium Comply identifies vulnerabilities and compliance gaps across an organization's environment. Comply evaluates endpoints for security configuration exposure and software vulnerabilities using industry security standards, vulnerability definitions, and custom compliance checks. Comply's on-demand and enterprise-wide results can reduce overall risk, improve security hygiene, and simplify compliance audit preparation, with results in minutes.

Comply scans endpoints using the Tanium Scan Engine to evaluate Open Vulnerability Assessment Language (OVAL)-based checks. Comply utilizes Security Content Automation Protocol (SCAP) compliant content, such as standards published by the Defense Information Systems Administration (DISA) or the Center for Internet Security (CIS), to evaluate operating systems and applications for configuration of password policies, file permissions, and other components.

The Tanium Client gathers the results of these scans and sends them back to the Tanium Server for the organization's users to review or export. Comply also offers remote authenticated scans where the Tanium Scan Engine runs on a satellite and connects to remote devices to run the OVAL checks.

What Data Privacy Issues Relate to Tanium Comply?

Tanium Comply collects machine information such as hostname, IP address, and known vulnerabilities from endpoints within the organization's environment.

What Types of Personal Data Does Comply Detect?

Depending on an organization's configuration, Tanium Comply may collect IP addresses and hostnames. Organizations may also configure and use Comply to identify other types of personal data.

When Might Comply Identify Sensitive Data?

Comply gathers machine data any time an assessment is run on an endpoint. This information includes information about the machine, such as hostname and IP address, as well as more specific information about the configuration of an endpoint and whether it has any known vulnerabilities. Organizations may also customize and use Comply to identify other types of sensitive data.

Does Comply Store Personal Data?

Comply may collect and store personal data, as described above. This data is stored on endpoints and in the Tanium Data Service (TDS) on the server. The Comply workbench relies mainly on data from TDS.

Who Can See the Data Viewed in Comply?

Data in Comply is viewed through the Comply workbench, which is only visible to the organization's Comply user, and in limited instances to Tanium support personnel as described below.

Do Tanium Personnel Have Access to Sensitive Data Through Comply?

Under normal operations, only the organization's user has access to the Comply 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 users visibility into these accesses, and optional approval authority when they occur.

Where Might I Learn More about Comply

Tanium Comply User Documentation is available here:
https://docs.tanium.com/comply/comply/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.