

Tanium Benchmark Privacy Datasheet

What Is Tanium Benchmark?

Tanium Benchmark provides real-time data, automation and intelligence for assessments of endpoint Benchmark. Organizations use this data to prioritize actions with intelligent risk scoring based on operational and security metrics. Benchmark provides visualizations and reports to communicate key trends, improvements and comparisons against industry benchmarks. Benchmark also allows organizations to understand the risk impact by focusing on the entire enterprise, as well as by individual geographies and business units.

What Data Privacy Issues Relate to Tanium Benchmark?

Tanium Benchmark allows an organization's Tanium console user to identify endpoints that contain sensitive data, which may include identifying personal data such as passwords and social security numbers on the organization's network. Benchmark also relies on data collected by other modules and core content, which may include other types of personal data.

What Types of Personal Data Does Benchmark Detect?

Tanium Benchmark relies on data collected by other Tanium modules: Benchmark's Password Identification uses the "PCI 2 - System Passwords" rule in Tanium Reveal to assess cleartext passwords stored on endpoints. Further, Benchmark's Administrative Access uses data from Tanium Impact to assess lateral movement risk. Administrative Access displays the names of users as well as the number of endpoints they have direct and indirect access to.

What Types of Sensitive Data Does Benchmark Detect?

Tanium Benchmark relies on data collected by other Tanium modules, including Tanium Reveal, which may include cleartext passwords. Please see the Reveal privacy data sheet for more information about how this data is collected.

Does Benchmark Store Personal Data?

Benchmark does not collect or store personal data. All personal data used for risk scoring stays on the endpoint it was discovered on. Underlying data can be viewed in the Reveal console via a direct connection from the console to the endpoint.

Who Can See the Data Viewed in Benchmark?

Potentially sensitive and/or personal data viewed in Reveal's file snippets is only visible to the organization's Reveal user, and in limited instances to Tanium support personnel as described below.

Do Tanium Personnel Have Access to Sensitive Data Through Benchmark?

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

Tanium Benchmark User Documentation is available here:
<https://docs.tanium.com/Benchmark/Benchmark/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.