Tanium Reveal Privacy Datasheet

What Is Tanium Reveal?

With Tanium Reveal, organizations can detect sensitive, unstructured or structured data at rest on endpoints across an entire IT environment. Organizations use Reveal to continuously monitor for artifacts in data that match patterns. When sensitive content that matches a pattern is discovered, organizations can label the files where the content exists and further analyze or take action on them to address regulatory compliance, information security, or data privacy issues.

Sensitive data is a high-value target for cybercriminals, and this data is often scattered throughout complex IT environments. Despite these challenges, organizations must track and manage sensitive data for security, regulatory compliance, and data privacy purposes. But typically, IT, security, and compliance teams have limited capability to track sensitive data at scale on larger networks. Without real-time endpoint visibility, the risk of compliance breach and IP theft increases.

What Data Privacy Issues Relate to Tanium Reveal?

Tanium Reveal allows the organization's user of the Tanium console to identify and view sensitive data, which depending on the configuration, may include personal data such as passwords and social security numbers on the organization's network.

What Types of Personal Data Does Reveal Detect?

Reveal contains prebuilt, out-of-the-box rules that can be deployed to detect and view data across endpoints in the following categories:

- Cardholder Data
- System Passwords
- Credit Card Numbers
- Potential Personal Data Exposure
- US Social Security Numbers
- US Tax Information

Note that the organization's user must manually choose which rules to apply, and which endpoints will receive these rules. Organizations also have the ability to build additional rules using the "rule set deployment" feature described below, and to search for any arbitrary string using the "quick search" feature.

When Might Reveal Identify Sensitive Data?

Reveal users can identify and view sensitive data in the Reveal console by two primary methods — both under the organization's control. When Reveal is used to identify and view personal data, the viewed data may include the personal data on the organization's network.

Quick Search: The user inputs an ad-hoc search string into the Reveal console. This string can be any combination of letters or numbers. Endpoints that contain matches are listed, and the user can then select an endpoint in which to drill down to a list of filenames containing that contain the matched search string. From there, the user can view a text snippet of the document that contains the search string.

Rule Set Deployment: A user defines one or more search patterns for a given data category, for example, US social security number. That rule is deployed to the desired endpoints in the organization's IT environment. Once Reveal has completed processing its local index of data on the endpoint for files that match the rule criteria, those matches are presented in the Reveal console for review in the same way as a Quick Search.

Does Reveal Store Personal Data?

Reveal does not collect and store personal data. All data viewed by Reveal users stays on the endpoint it was discovered on. Data is viewed in the Reveal console via a direct connection from the console to the endpoint.

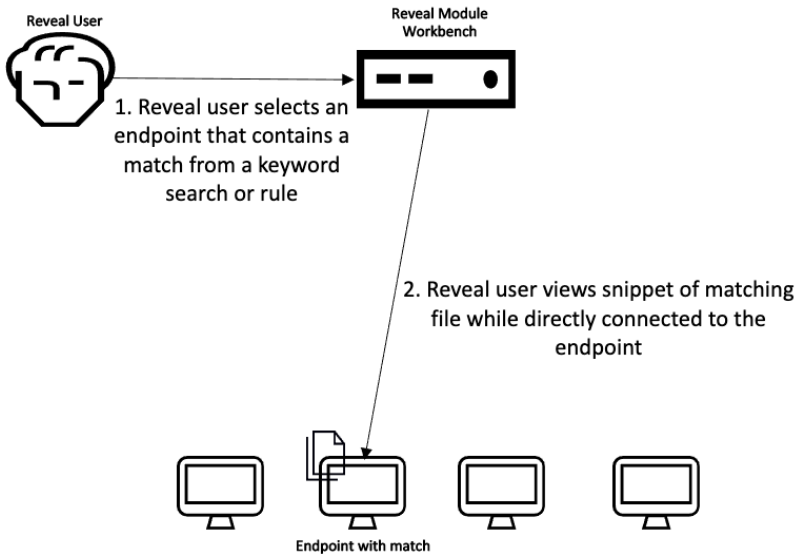
Who Can See the Data Viewed in Reveal?

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

Do Tanium Personnel Have Access To Personal or Sensitive Data Through the Reveal Console?

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

A Data Map Detailing the Data Lifecycle in Reveal



Where Might I Learn More about Reveal

Tanium Reveal User Documentation is available here:
https://docs.tanium.com/reveal/reveal/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.