SOLUTION BRIEF

TANIUM | Federal

Tanium for the Continuous Diagnostics and Mitigation (CDM) Program

A complete, accurate, and up-to-date view of your hardware, software, and virtual asset inventory with a configurable one-click integration into the CDM dashboard.

Do you trust the data in your CDM dashboard?

Federal organizations are facing a challenge of certainty concerning their IT risk posture: visibility and control. Countless frameworks, memos, and BODs have been issued on the topic of visibility, and yet, many federal agencies still don't have it.

With most configuration management databases (CMDB) pulling together huge amounts of data from many sources, accuracy gets lost in the shuffle. Your CMDB should have the exact data you need about your IT estate to make informed decisions to reduce IT risk – which is the goal of CISA's CDM program. But if you can't trust the data going into the dashboard, how can you trust the insights coming out?

With Tanium, federal organizations can gather real-time HWAM, SWAM, CSM, and VULN data directly from the endpoint, and utilize a configurable push-button integration straight into the CDM dashboard – without the need for custom scripts or manually reconciling data sets. With that insight, they can remediate issues as they arise.

Have real-time insights from your CDM dashboard

Federal agencies already use Tanium to funnel real-time data into CDM. With Tanium, federal agencies can reduce complexity, improve efficiency, and enhance security posture by delivering accurate and real-time data, automating workflows, remediating issues, and enforcing policies across organizations of any scale.

The platform gathers both IT operations and security data from endpoints in real time, so your organization can finally gain full visibility into your endpoint-based attack surface. Using our patented linear-chain architecture, data is transmitted at lightning speed and massive scale directly from any Windows, Mac, or Linux endpoint. Then, with these insights, administrators can pivot to action to remediate issues as they arise – helping contribute to an improved CDM AWARE score.

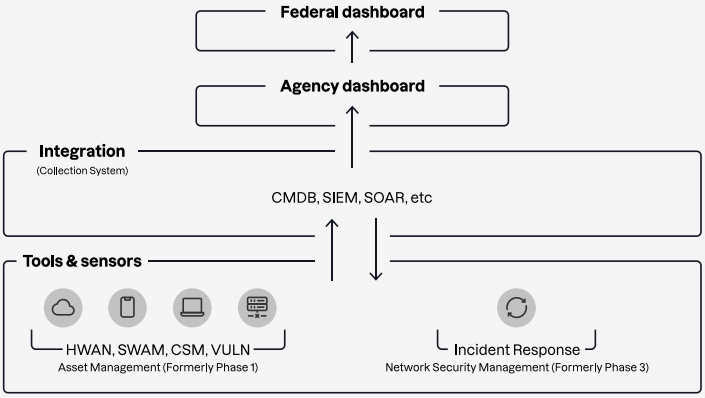
With Tanium, federal organizations can:

- Gain full certainty about the state of their endpoints right now – not based on information gathered days or weeks ago
- Funnel real-time, accurate HAWM, SWAM, CSM, and VULN data directly from the endpoint and into the CDM dashboard
- Pivot from analysis to remediation in the Tanium platform, once issues have been identified, to close security gaps with patching and deploying third-party updates to harden the attack surface
- Seamlessly report to decision-makers on the status of asset inventory, compliance, and more from the CDM dashboard, or directly in Tanium, with easy-to-digest
- Reduce complexity and cost by replacing multiple point solutions with a single platform that covers multiple CDM capability domains
- Enhance security and compliance by enforcing policies, remediating issues, and reporting on endpoint status in real time

Tanium and CDM customer proof points

One federal civilian agency utilized the Tanium-to-CDM-integration to:

- Meet 92% of all CDM, HWAM, SWAM, CSM, and VULN requirements
- Eliminate custom scripting to get data from their tools into CDM dashboards, saving significant time and reducing the chance of errors
- Save millions of dollars through tool consolidation and reduce infrastructure with a FedRAMP Authorized Tanium Cloud instance



FedRAMP™

Tanium is FedRAMP Authorized at the Moderate impact level

www.tanium.com/federal

Improve your CDM insights today

Your organization needs a solution that can infuse real-time, accurate endpoint data into your CDM dashboard and pivot to remediation right away. With Tanium, federal organizations will have a single source of truth for endpoint data, with a single agent that can improve their CDM insights and improve their CDM AWARE score.

Lastly, when it comes to future-proofing organization, Tanium's FedRAMP Authorized cloud platform gives you real-time endpoint data such as certification encryption status, security vulnerabilities, supply-chain risk management (with SBOM), identification of sensitive data, Digital Employee Experience (DEX), patching and OSs update deployment across Windows, Mac and Linux devices, and more.

Tanium, the industry's only provider of Converge Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.