SOLUTION BRIEF

TANIUM | Public Sector

Tanium for Federal Government

A modern, scalable, efficient, and proven solution that reduces IT risk for the United States Federal Government

Reduce IT risk by managing and securing distributed endpoints

Managing and securing endpoints is more challenging than ever before. The federal government's operations are complex, often siloed, and reliant on an increasing volume of diverse, dynamic, and distributed assets.

Many CIOs, CISOs, and CTOs struggle to maintain visibility and control over their networks. They are often using outdated hardware and software that give a stale and incomplete view of their environment and its risks. Their IT operations and security teams are often siloed and prioritize different outcomes. Add in a growing suite of regulatory requirements that consume a tremendous amount of staff time, and it can be tough to keep up.

The result: many technology leaders and teams are stuck in a reactive approach to managing and securing their environment, and are never fully protected against attacks, performance drops or data loss. Common challenges across the Federal government include:

- CIOs, CISOs, and CTOs must manage and secure their networks with little visibility or control.
- IT operations and security teams struggle with tasks like maintaining patch compliance.
- Despite heavy investment, federal organizations carry high levels of risk due to the difficulties in managing legacy software and point solutions.

A converged approach to endpoint management and security

The Tanium platform can help you reduce your attack surface with a wide range of features that make it easy to see a real-time view of every endpoint connected to your environment, apply fundamental controls and remediate issues as they come up – all from one platform and with one agent.

With Tanium, you can:

- Have a single source of truth for real-time endpoint data — no matter how many endpoints you have or where they are located.
- Automate time-consuming processes like patching and policy management so teams can re-focus on higher-value projects like threat hunting.

Protect your mission-critical assets, public services and sensitive data by reducing your attack surface and giving you full, accurate visibility.

With Tanium, you'll have unparalleled real-time visibility and control over your endpoints, allowing you to manage and secure your entire environment with just one agent and on a single platform.

FedRAMP™

Tanium is FedRAMP Authorized at the Moderate impact level

Visibility

Create an accurate, real-time picture of the endpoints in your environment, if they are healthy and within policy.

If you can't see your endpoints, you can't manage or secure them. Yet most organizations can't see all their endpoints, software or where their sensitive data is stored — and the move to remote work has created even more blind spots with hidden risks. But with Tanium, you can:

- Rapidly discover and create an inventory of all assets in your environment — including endpoints and software that you didn't know you had.
- Find where all your sensitive data is stored, look inside files for a more granular view, and check user privileges — all in real time.
- Maintain compliance against relevant cybersecurity frameworks by continuously scanning for, identifying and remediating misconfigurations.

Control

Remediate your risks and inefficiencies across your entire environment as soon as you find them.

Seeing your endpoints is just the start. Yet modern environments can carry hundreds of thousands of vulnerabilities and compliance gaps, and operations and security teams struggle to mitigate these risks. But with Tanium, you can:

- Streamline and automate key tasks like patching and OS updates, so operations can fix issues at scale and spend more time on higher- value actions.
- Take a proactive approach to security, and let teams hunt for, identify, defend against, and remediate threats — all from one platform.
- Optimize costs and reduce complexity by consolidating point tools, and accurately reclaiming unused software licenses.

Remediation

Investigate and respond to incidents in real time.

Closing endpoint risk is a cross-functional effort. Yet legacy tools silo operations and security teams from one another, forcing them to work from their own data sets and prioritization of what risks to close first. But with Tanium, you can:

- Rapidly detect, contain and remediate a wide range of incidents and vulnerabilities across all endpoints from one tool.
- Reduce friction, align priorities, and make shared risk-based decisions using real-time data, so teams and leaders agree on the right next steps to take.
- Remediate issues in a fraction of the time it takes other tools due to rapid, and real-time access to data, and the ability to switch to remediation in just a few clicks.

To learn more about how Tanium supports U.S. federal organizations, whether on premises or FedRAMP® Authorized, in the cloud, visit: www.tanium.com/federal

FedRAMP™

Tanium is the platform that security-conscious public sector organizations trust to protect people; defend data; secure systems; and realize the full potential of their IT investments. For more on The Power of Certainty™, visit www.tanium.com and follow us on LinkedIn.