Reducing IT risk for the U.S. Federal Government

How Tanium provides support for emerging threats, new guidance and industry topics

Operations in the U.S. federal government are complex and rely on an increasing volume of diverse, dynamic, and distributed hardware and software. This, along with the constantly changing cyber threat landscape has resulted in numerous mandates, executive orders, programs and Binding Operational Directives (BODs) – all with the goal that federal systems are protected and the risk to national security is reduced.

Tanium has partnered with the U.S. federal government to improve its ability to respond to emerging challenges, and address federal guidance, enabling it to continue delivering services, and maintaining mission-critical operations through times of uncertainty.

We know that IT operations and security leaders in the U.S. federal government are faced with:

- Reducing costs, improving services, and securing their organization so they can achieve their mission.
- Securing networks when they have very little visibility or control over their environment.
- Modernizing systems that rely on legacy point tools, and siloed and outdated data.
- Reducing staff time spent on manually maintaining patch compliance and responding to FISMA audits.
- Offloading risk, despite heavy investment in Cloud and SaaS.

With Tanium's Converged Endpoint Management Platform (XEM), federal government organizations can have full visibility of any endpoint (anything with an IP address) that is connected to their environment, the comprehensive control to manage Windows, Mac and Linux endpoints and a single source of truth for all endpoint and IT Operations data – all in one platform, available in the cloud or on premises.

This document explores how organizations across the federal government have used Tanium to address emerging issues, BODs and beyond.

Executive Order 14028: Improving the nation's cybersecurity

What it is:

The Executive Order calls for bold change versus incremental change to vastly improve the government's cybersecurity practices.

How Tanium helps

The Tanium Platform was engineered to overcome legacy limitations and modern challenges. Its unique, patented, and proven communications architecture empowers enterprise and risk managers with the comprehensive real-time visibility and control needed to make critical decisions, allowing them to take the right action, right now.

The Tanium Platform provides a reliable endpoint management and security solution that is robust enough to run in a variety of diverse environments, yet flexible enough to handle management and security needs that change second by second. It truly represents the bold change this EO calls for.

Learn more

tanium.com/solutions/federal-government

Zero Trust: OMB memorandum on moving the U.S. government toward Zero Trust cybersecurity principles

What it is:

The OMB Memo on Zero Trust encourages the federal government to meet five Zero Trust security goals. It calls for improvements and investments in validating network, identity, data, device security posture and policies before granting access to critical systems.

How Tanium helps

The endpoint is the point of convergence for users, data and applications; it is a primary battleground in modern cyberspace. Organizations now operate borderless environments and must directly manage and secure these endpoints wherever they are located on a 24/7 basis.

Tanium is ideally suited to support Zero Trust principles by providing the highest fidelity, real-time data on endpoint posture for risk assessment, policy enforcement and even remediation – all alongside existing Zero Trust frameworks of identity and network access management. Is the device manageable, under management, and compliant?

Tanium more specifically helps address pillar five of the OMB Memo.

Learn more

explore.tanium.com/zero-trust

Binding Operational Directive 22-01: Reducing the significant risk of known exploited vulnerabilities

What it is:

The US Cybersecurity and Infrastructure Security Agency (CISA) issued a directive that requires federal agencies to patch known exploited vulnerabilities and introduced a catalog of known vulnerabilities that will be regularly updated.

How Tanium helps

Tanium was built to give organizations of any size full visibility into the security posture of their endpoints. With many federal agencies already using Tanium for this exact use-case, it is the best tool available to meet CISA's quickest timelines of closing certain vulnerabilities.

With Tanium, organizations can first discover the previously unseen or unmanaged endpoints connected to their environment, and then search for the specific vulnerabilities listed in the Directive. Then organizations can close those vulnerabilities at unprecedented speeds, at scale and have the confidence the patches were applied correctly and that endpoints are secured. This whole process commonly takes less than one day for existing Tanium customers.

There are numerous examples to draw from where Tanium customers were able to remediate vulnerabilities such as the Log4j, PrintNightmare, SolarWinds exploits, and the WannaCry vulnerability within minutes. The process for finding and fixing the specific vulnerabilities outlined in the Directive is no different.

Learn more

community.tanium.com/s/article/CISA-Binding-Operational-Directive-22-01-How-Tanium-Can-Help

Log4j (ED 22-02)

What it is:

First reported on December 9, 2021, the Apache Log4j vulnerability is one of the most serious vulnerabilities on the internet in recent years, putting millions of devices at risk.

How Tanium helps

Tanium enables federal IT teams to quickly identify vulnerable instances of the Apache Log4j utility, search file paths for JAR, EAR, and WAR files for references to the impacted library in common file formats and detect instances of exploitation. Upon detection, teams can triage and promptly remediate exposure to the Log4j vulnerability by notifying application owners, applying recommended patches or conducting deeper investigation.

Once Log4j is remediated, Tanium helps continuously enforce compliance through automating patch management, software updates and configurations at scale.

Learn more

tanium.com/log4j

Endpoint Detection and Response (EDR)

What it is:

EDR (Endpoint Detection and Response) capabilities have come into sharp focus for many federal agencies, with the cybersecurity Executive Order, and OMB Memo on Improving Detection of Cybersecurity Vulnerabilities and Incidents, which introduced new requirements for endpoint management and security.

EDR is a broad term that is defined differently across security vendors, analysts and practitioners; but it comes down to the goal of securing endpoints by detecting known threats. Unlike many EDR-only tools on the market, Tanium stands alone in its ability to secure endpoints by investigating and remediating known and unknown threats, at scale with unrivaled speed.

How Tanium helps

- *Complete visibility:* Only Tanium can help you find all of your devices, unmanaged or managed, across the globe and provide real-time data on their status. One Tanium customer gained full visibility into 300,000 devices in seconds.
- *Total control:* Easily push and validate, including other endpoint agents. If you don't have visibility, triage, remediation, and control of what's on your endpoints, your security tooling doesn't matter.
- One Tanium customer identified and fixed 20% of another vendor's EPP/EDR agents that were in a broken status.
- *Rapid remediation:* The ability to investigate, contain, and remediate all from one platform. Tanium is the only solution that can accurately investigate threats, contain a device, then confirm it and bring it back to a good state. You need a tool that not only remediates your vulnerabilities but can also disprove an alert so you can be sure the threat is gone for good. One Tanium customer found and remediated the Kaseya vulnerability across more than 100 critical endpoints.

Learn more

tanium.com/blog/endpoint-detection-and-response-what-edr-is

Continuous Diagnostics and Mitigation (CDM)

What it is:

The CDM program is designed to provide an added layer of protection in a hybrid environment. As the distributed workforce grows, federal agencies face a broader threat landscape. Bad actors are gaining access to more user credentials than ever before, with their algorithms outperforming humans 1,000 to one. In this new environment, federal agencies must approach security infrastructure comprehensively — considering device, network and data security.

How Tanium helps

Agencies need to reduce complexity with a converged endpoint management and security platform, so they can reduce risk and act quickly to efficiently manage and secure their environment anywhere endpoints exist.

Several U.S. Federal agencies leverage use Tanium to send data to the CDM dashboard. Both asset discovery and vulnerability reports can be sent using this method. Custom tags can be applied by targeting a group of endpoints through a Tanium question and deploying an action to add the custom tags. Additionally, assets can be targeted using multiple attributes and the asset will add the correct custom tag(s).

Learn more

tanium.com/resources/take-control-of-your-it-assets-management

National Institute of Standards and Technology (NIST)

What it is:

NIST adoption is growing. According to Network World*, 39% of cybersecurity professionals said their organization adopted some portion of the NIST Cybersecurity Framework over the past two years. Insurance companies are considering making the NIST Cybersecurity Framework a risk management standard for premiums and customer service programs. Adopting the NIST Cybersecurity Framework can help organizations gain a better understanding of their environment and improve their security posture.

How Tanium helps

Tanium can help organizations achieve much of the framework, by providing key capabilities, facilitating continuous monitoring, and supporting the transition through defined Implementation Tiers.

Learn more

tanium.com/resources/aligning-to-the-nist-framework

Cloud/FISMA/FITARA

What it is:

The more physical infrastructure the government supports, the more difficult it is to inventory and secure. FISMA and FITARA are both acts that support modernization of the federal government with the reduction of legacy infrastructure and adoption of cloud services.

A large number of all federal endpoints are more off-campus now than ever before – creating the need for a greater focus on threat hunting, and security data analysis, using real-time data. But with a workforce still largely tasked with managing legacy, on-premises tools, federal IT teams are too busy pushing software updates manually, replacing and maintaining old servers, and supporting on-premises tools, to respond to modern threats as proactively as they'd like. With more and more infrastructure to manage, each legacy asset represents a threat vector, which leaves federal organizations vulnerable.

How Tanium helps

Tanium Cloud for US Government (TC-USG) is a Converged Endpoint Management Platform that is pre-configured out of the box, fully managed by Tanium, and FedRAMP Ready at the Moderate-Impact level.

With TC-USG, organizations can combine their security and operations functions into one console which allows siloed teams to work from the same endpoint data set – making it easier to find vulnerabilities across the organization and take action quickly. And, because Tanium manages the software as a service, federal IT teams don't have to allocate additional resources to manage the solution. Software releases, patches and general maintenance are all handled by Tanium, which means teams can focus precious time on higher-value activities like threat hunting or security data analytics.

Learn more

tanium.com/blog/ready-status-fedramp-marketplace

Center for Internet Security (CIS) controls

What it is:

The Center for Internet Security (CIS) is a nonprofit organization dedicated to making the connected world a safer place by developing, validating, and promoting best practices that help protect organizations against cyber threats. CIS's 18 controls are recommended actions and specific steps that organizations can follow to aid in preventing today's most pervasive and dangerous cyberattacks.

How Tanium helps

Tanium addresses all CIS controls. With Tanium, you can:

- Discover and inventory all assets across the estate in near real-time, quickly and easily.
- Collect multiple data points from the endpoint estate, and get evidence that essential controls are in place. Gaps in controls can be closed with policies.
- Implement near real-time vulnerability and patch scans, and rapidly highlight where missing critical patches and vulnerabilities exist.
- Create reporting dashboards to more easily measure complaince on a daily basis.

Learn more

cisecurity.org/services/cis-cybermarket/software/tanium

Mitre Att&ck Framework

What it is:

In 2013, MITRE started ATT&CK – a reference detailing tactics and techniques commonly used by attackers during network intrusions. The MITRE ATT&CK Framework created a common way for organizations to view cyberattack risks and more easily prioritize their defenses to have the maximum impact on reducing those risks.

Since inception, the ATT&CK framework has evolved into a massive public knowledge base leveraged by both government and industry to classify attacks in a consistent manner, compare and contrast one attack to another, determine how an organization's network was compromised, and ultimately better defend against future attacks.

How Tanium helps:

Tanium has helped federal agencies and other organizations take a proactive and efficient approach to risk and compliance. Through the combination of its extensible data model, distributed communications protocol, and lightweight agent, the Tanium platform enables customers to save time and reduce costs associated with managing risk.

Learn more

tanium.com/blog/how-tanium-and-the-mitre-attck-framework-empower-federal-decision-makers-to-manage-and-prioritize-risk-in-todays-complex-environments

Risk Management Framework

What it is:

Since 2010, the U.S. government has required all federal information systems to comply with the government's Risk Management Framework (RMF), a set of security standards for architecting, securing, and monitoring IT systems.

Now managed by the National Institute of Standards and Technology (NIST), the RMF standards offer detailed best practices for improving IT security in the face of threats such as data breaches and ransomware attacks.

How Tanium helps:

The Tanium platform provides security and IT operations teams with a single, comprehensive, real-time view of critical endpoint data so that organizations can make informed decisions and act quickly to minimize disruptions and reduce risk. Tanium modules — components of the Tanium platform — address key requirements of the RMF.

Learn more

tanium.com/blog/comply-with-risk-management-framework-requirements

Visit tanium.com/federal to learn more about how your organization can reduce its IT risk with having visibility of all endpoints connected to your network, and the control to manage your devices from one platform.

Tanium, the industry's only provider of Converged 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.