SOLUTION BRIEF

TANIUM | Federal

Tanium for the U.S. Department of Defense

A comprehensive, converged platform for enterprise-wide IT operations and security management

Working through uncertainty to ensure command and control

The United States Department of Defense (DoD) faces several challenges when it comes to endpoint management and security. The highly distributed and complex nature of DoD operations can create a real lack of visibility into the health and status of the network, which can adversely affect mission critical systems, leaving networks at risk.

When it comes to IT operations and security, all branches of the DoD share these challenges:

- Legacy applications and hardware do not support modern security measures or current operational and security requirements.
- Disparate tools return disparate data sets that require tedious, manual work to reconcile.
- Homegrown systems require additional resources (time, people, and money) to maintain, operate, and integrate with modern IT processes and infrastructure.
- Security teams spend precious time using many point tools to answer simple questions: what is connected to our network, and can we take action if something doesn't look right?

Command and control of DoD networks is constantly under attack from willing, motivated, and sophisticated adversaries. To maintain a high level of C2, the DoD must respond swiftly and accurately.

> **With Tanium's Converged Endpoint Management (XEM) platform, DoD IT operations and security teams can modernize their operational efficiency and reduce the time and resources required for endpoint management across the enterprise.**

An enterprise solution for the DoD

Tanium's Converged Endpoint Management (XEM) platform provides a lightweight agent that can be deployed on all endpoints, regardless of the hardware or operating system. This enables the DoD to gain real-time visibility into all endpoints in the environment, allowing security teams to quickly identify and remediate threats all from one platform.

With Tanium's robust flexibility, IT administrators can configure the tool to address many use-cases within one platform, including:

- IT operations management
- Unauthorized software management
- Software asset utilization and inventory
- Threat hunting and remediation
- Software bill of materials investigation
- Third-party patching and operating system upgrades
- Bare-metal provisioning
- Integration with tools already in use by the DoD, including Microsoft, ServiceNow, and more

With Tanium's XEM platform, the DoD can enhance its security posture by achieving real-time visibility into all endpoints, identifying and mitigating threats before they cause damage — enabling the warfighter to focus on the mission at hand.

Visibility

Create an accurate, real-time picture of the endpoints in your environment. Know if they're 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 — especially across large, complex, distributed environments. But with Tanium, you can:

- Rapidly discover and create a real-time 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 risks and inefficiencies across your entire environment as soon as you find them.

Seeing your endpoints is just the start. 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 teams can fix issues at scale and spend more time on higher- value actions.
- Take a proactive approach to security, and empower teams to 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. Legacy tools can silo IT 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 platform.
- 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.

Tanium is trusted by five branches of the U.S. Armed Forces to secure and defend the nation's networks. Learn more: www.tanium.com/federal

Tanium, the industry's only provider of converged endpoint management (XEM), 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. State and local governments, educational institutions, federal civilian agencies 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. Visit us at www.tanium.com.