carahsoft

TANIUM | Public Sector

# Tanium Cloud for U.S. Government

## A FedRAMP® Authorized solution for autonomous endpoint management (AEM), offering digital employee experience, threat response, SBOM and more in the cloud.

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, CMAS and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Tanium, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

**Explore More Resources:**
carah.io/taniumresources

**Join Events & Webinars:**
carah.io/taniumevents

**Discover Technology Solutions:**
carah.io/tanium

**Learn About Procurement:**
carah.io/taniumcontracts

**Connect With Our Team:**
Tanium@carahsoft.com
(703)673-3560

# Tanium Cloud for U.S. Government

**A FedRAMP® Authorized solution for autonomous endpoint management (AEM), offering digital employee experience, threat response, SBOM and more in the cloud.**

## Benefits of Autonomous Endpoint Management (AEM) in the Cloud

**VISIBILITY**

See into every endpoint, managed or unmanaged, with complete, accurate and real-time visibility.

**CONTROL**

Take control of your entire IT estate in seconds with minimal network impact.

**REMEDIATION**

Investigate and respond to incidents in real time.

Tanium's Converged Endpoint Management (XEM) platform is a FedRAMP® Authorized solution that gives federal organizations an integrated view of all endpoint data and a common taxonomy, to reduce risk, and secure federal endpoints – all from the cloud.

FedRAMP™

**Tanium is FedRAMP Authorized at the Moderate impact level.**

www.tanium.com/federal

## Reducing risk across a distributed workforce

Security threats across the public sector are increasing, and regulations like FISMA and FITARA started the shift across the federal government to put more emphasis on retiring outdated hardware and software in an effort to reduce costs and risk - with a move to the cloud.

Whether there is a need to adapt to a more distributed workforce, or to increase the use of cloud infrastructure, IT groups are grappling with how to secure their environments. With a more distributed environment, the endpoint is acting as the new perimeter, which means that all unmanaged devices are particularly vulnerable to malware, phishing, and other modern threats. And still, many federal government organizations are still relying on legacy, outdated technology to manage and secure their endpoints - whether those endpoints are on premises or remote.

## Legacy infrastructure increases risk

The more physical infrastructure the government supports, the more difficult it is to inventory and secure. A large portion of all federal endpoints are more off-campus now than ever - 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.

What federal government entities need is the ability to manage all their endpoints, on, or off-network from a single cloud-based platform that can reduce risk by retiring servers and outdated hardware, shift staff focus to higher value activities and get certainty with real-time visibility into their IT environment - at scale.

## Tanium Cloud for U.S. Government: a FedRamp ® Authorized solution

Tanium Cloud for U.S. Government (TC-USG) is an autonomous endpoint management platform that is pre-configured out-of-the-box, fully managed by Tanium, and FedRAMP® Authorized at the Moderate-impact level.

The solution gives federal organizations full visibility into their IT environment, the control to take comprehensive action and a single source of truth for all endpoint data, at scale.

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 allows teams to focus on higher value activities like threat hunting or security data analytics.

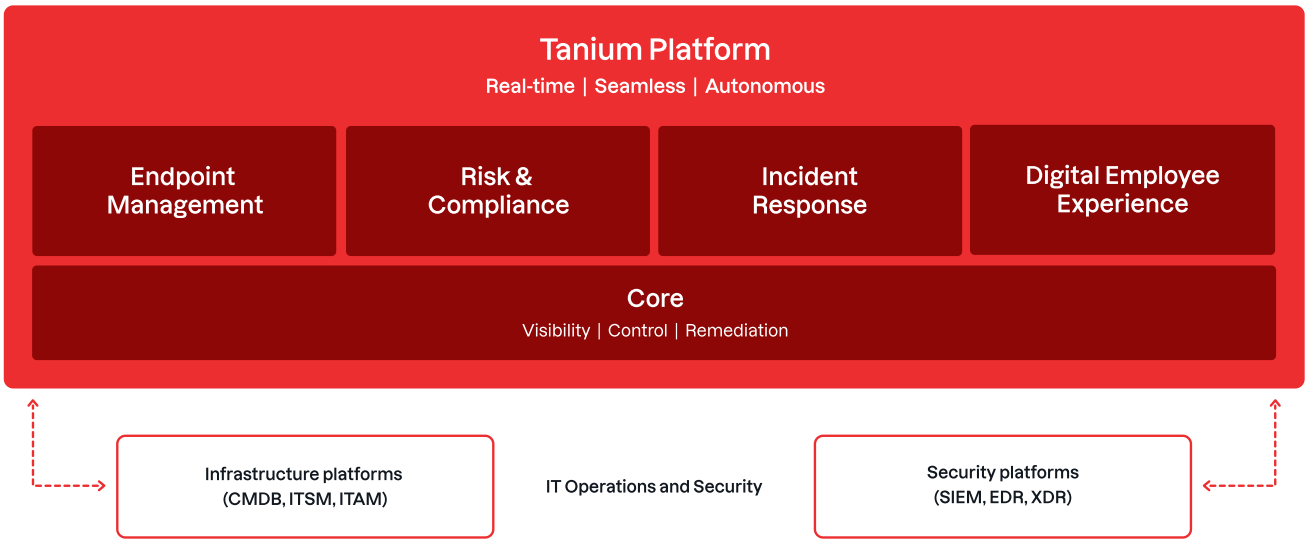
## Benefits of Tanium Cloud for U.S. Government

- **Get visibility into all your endpoints in real time**, and know what's connected to your environment at all times.
- **Have a single source of truth** for endpoint data at scale in minutes.
- **Reduce your attack surface** by closing entry points into systems that store valuable data.
- **Practice continuous compliance** with confidence that policies are being enforced, and have control to diagnose and fix issues as they arise.
- **Have the control to take action** and respond quickly if something doesn't look right.
- **Manage and secure federal environments** large or small, and fold in new endpoints as they are connected to the network.
- **Reduce your risk profile** by retiring servers used for legacy tools, and reprioritize staff time on more impactful activities like threat hunting - not managing hardware and software.
- **Eliminate legacy, disparate point solutions** and pull the operations, security, and compliance capabilities you need into a single console with minimal management overhead.
- **Comply with Federal requirements** for Cloud Service Offerings, and FISMA/FITARA with a FedRAMP Authorized solution.
- **Focus staff time on higher value activities** when the management, maintenance, and updates are done by Tanium.

## Faster time to value

With TC-USG, organizations of any size can spin up an instance very quickly, with critical IT operations, risk, and security solutions ready-to-go. Crucially, the service requires zero infrastructure. While other solutions make this claim, on-premises infrastructure is often still required to deliver critical services, such as OS patches or software updates. TC-USG gives organizations the ability to deploy new operations and security capabilities fast - significantly reducing internally committed hours needed at the beginning of implementation. Tanium Cloud for U.S. Government cascades benefits throughout your entire organization. With a converged platform, IT operations and security teams can work from the same data set, which reduces risk and ensures federal organizations can focus on their objectives, strategic initiatives, and reducing their attack surface. All using one platform, one agent, and zero infrastructure.

## Autonomous Endpoint Management




**To learn how Tanium's FedRAMP Authorized solution can reduce your attack surface and comply with federal programs, visit www.tanium.com/federal.**