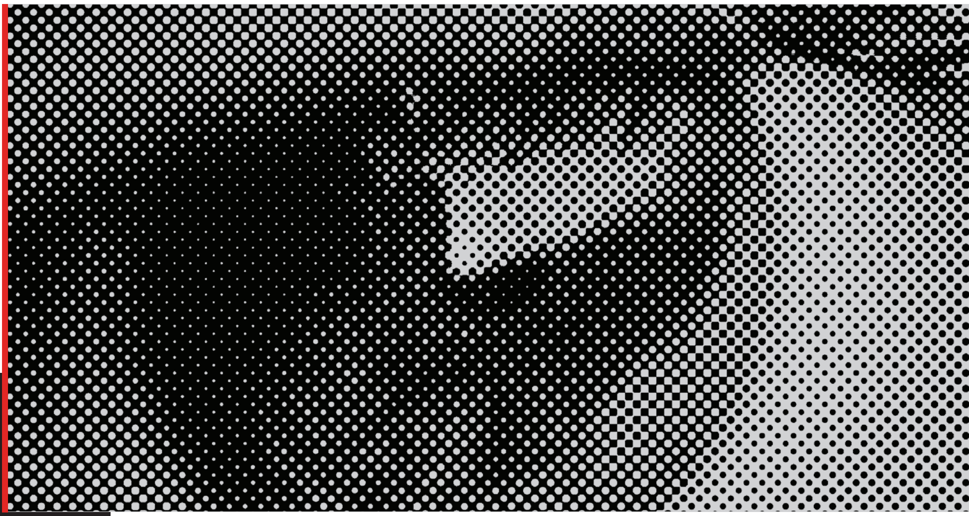
INDUSTRY BRIEF

DEFEND at the Speed of Cyber

Using Tanium to Meet CDM DEFEND Requirements

The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program is moving rapidly into Phase 3 – DEFEND. Building on the basic endpoint and user access protections offered by CDM Phases 1 and 2, DEFEND brings surveillance, analysis, forensics, and security posture improvement tools and methods into CDM's suite of functionalities offered to civilian agencies.



CDM DEFEND Scope Synopsis

DEFEND provides support for all phases of the CDM Program to develop, implement, and maintain a common set of CDM capabilities across agencies, including:

- Provision agencies with CDM-approved products and associated services.
- Fill existing gaps in agency CDM solutions to achieve a common set of capabilities.
- Provide O&M for existing CDM solutions, while continuing to enhance and refresh approved products.
- Enable, through CDM tools and sensors, agency dashboard data feeds and CDM governance principles.
- Provide agency-specific training for the CDM Solution, the agency CDM Dashboard, and CDM governance support.

CDM DEFEND overview

CDM DEFEND focuses on two primary factors: **"What's happening on the network?"** (including Boundary Protection, Manage Events, Operate, Monitor & Improve, and Design & Build in Security); and **"How is the network protected?"** In addition, the scope for DEFEND includes tech refresh/upgrades provided originally by foundational Phase One (**"What is on the network?"**) and Phase Two (**"Who is on the network?"**).

Tools must be evaluated and approved by the Department of Homeland Security prior to being placed on the CDM Approved Products List (APL) and may be procured from GSA's Schedule 70 CDM SIN (132-44).

Know **what is on the network** in seconds

Tanium's business resilience management platform provides enterprise-wide visibility into what is on an organization's network—including configuration settings, vulnerabilities, unauthorized hosts, objects, and processes—all within seconds. The more complex and diverse a network is, the more value can be found in using Tanium.

Know **what is happening on the network** in seconds

Tanium's extremely light footprint and agile collection methods means agencies can find out what's happening on the network in near real time. Why risk waiting 72 hours when you can know definitively—from the endpoints themselves—in seconds?

What **DEFEND at the speed of cyber** means

DEFEND at the speed of cyber means integrators and agencies can now implement a secure Cyber Defense platform capable of delivering near real-time visibility into enterprise networks around the globe. Tanium's current products—all of which are

All of Tanium's current products are approved by the Department of Homeland Security for inclusion in the Continuous Diagnostics and Mitigation (CDM) Approved Products List for Phase 3 - DEFEND.

approved by the Department of Homeland Security for inclusion in the Continuous Diagnostics and Mitigation (CDM) Approved Products List for Phase 3 - DEFEND—are also compatible with all popular adjunct technology tools, such as Splunk and Palo Alto Networks. Tanium offers open architecture integration tools and methods to make the largest enterprise integrations achievable.

How Tanium supports CDM

Tanium's product suite comprises our Core Platform and Tanium Functional Modules, which add incremental capabilities. All of these tools have been approved by DHS for inclusion in the CDM DEFEND Approved Products List (APL) and are available for implementation today. Tanium can be implemented as a comprehensive enterprise-wide, cloud-enabled agency solution or used as functional blades of gap-filling or extensions for augmenting existing cyber services.

Why DEFEND at the Speed of Cyber?

Threat actors don't wait, and neither can you. According to Verizon's 2017 Data Breach Investigations Report: "… compromises are measured in minutes or less 98% of the time." Yet, the time to discover a breach continues to increase. Agencies need comprehensive solutions to address these real-time threats.

Tanium is architecturally advantaged

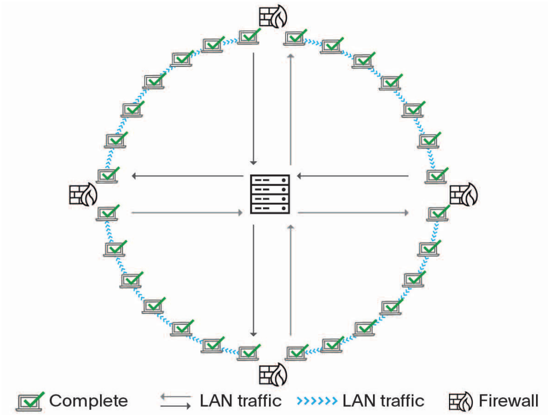
Tanium's major differentiator is its unique architecture, which provides the ability to query every endpoint with incredible speed and efficiency across the largest enterprises with 99.9%+ accuracy. Its current installed base includes millions of endpoints in DoD, FEDCIV, and commercial enterprises.

Using this architecture, agencies can expect to see 15-second visibility and control across all endpoints. For the first time, analysts are seeing exactly what's happening, as it's happening, so they can make better decisions and quickly take corrective actions. The speed, comprehensiveness, and accuracy of the data will provide decision makers with the near-real time visibility needed for effective security to better defend against attackers and prove compliance with Federal mandates.

By decentralizing data collection, aggregation, and distribution down to the endpoint, Tanium's Linear Chaining Architecture harnesses the intrinsic speed of low-latency LAN traffic and dramatically reduces direct client-to-server communications, effectively eliminating the crippling inefficiencies caused by bloated databases, overloaded connections, and heavy traffic across WAN segments (see Figure 1). With Tanium, security incident response teams can confidently hunt and remediate advanced threats across millions of endpoints, and IT operations teams can accurately manage and inventory every single global asset within seconds.

Unlike traditional tools, which require dozens to thousands of secondary servers to scale their infrastructure, the Tanium Architecture's streamlined communications allows it to effortlessly support millions of endpoints and maintain optimal performance. There's no need for ongoing investments in costly hardware even as the network grows over time. With this breakthrough architecture, secondary relay, database, or distribution servers are no longer necessary at different departments, bureaus, or geographically dispersed agency offices.

Figure 1 Tanium Architecture



Tanium Functional Modules

Tanium's Functional Modules are purpose-built extensions geared for specific security and management use cases and problems, such as threat response, patching, checking for file integrity, or ensuring compliance.

Tanium allows organizations to lower cost by consolidating point tools and increasing service levels with the benefits of the speed, scale, and completeness that Tanium delivers. Figure 2 illustrates how Tanium complies with DEFEND functional requirements.

Tanium Enterprise

Tanium Enterprise is the most comprehensive cyber security tool bundle we offer. With one stratified product any agency can procure and implement the entire suite of Tanium's cost-effective and proven tools.

Tanium Core Platform

The foundation of the Tanium solution is Tanium Core Platform. With the Tanium Core Platform, security and IT operations teams can ask any question about their environment in plain English, retrieve accurate and complete data, and immediately take any corrective action needed directly on the endpoint. The core platform also allows organizations to visualize trends and feed endpoint data into systems such as SIEMs, log analytics tools, help desk ticketing systems, CMDBs, and big data clusters.

Tanium Threat Response

Incident Response teams can hunt, detect, investigate, contain, and remediate threats and vulnerabilities using Tanium Threat Response. They can take an initial lead, quickly search, filter, and visualize forensic data, and piece together the story of what happened on a single endpoint. They can then pivot to fully scope any incident across the enterprise.

Tanium Asset

Tanium Asset gives operations and IT asset management teams a thorough and up-to-date picture of their endpoint hardware, software, and configuration inventory. This helps organizations make the right decisions about how to deploy their assets most efficiently.

Tanium Comply

Check system configurations for millions of endpoints against standard security benchmark using Tanium Comply. With on-demand, enterprise-wide results, organizations can improve overall security hygiene and simplify preparation for industry compliance audits.

Tanium Discover

Bring unmanaged endpoints under control with Tanium Discover. Discover finds unmanaged assets within the enterprise environment—even across the largest global networks—in seconds.

Tanium Integrity Monitor

Tanium Integrity Monitor simplifies regulatory compliance by making file integrity monitoring more effective enterprise wide. Integrity Monitor offers the ability to link file integrity monitoring with active alert investigation, configuration compliance, and vulnerability scanning.

Tanium Patch

Tanium Patch enables organizations to customize patch workflows with up-to-the-second endpoint visibility and control with just a single server, regardless of network scale. It generates patch reports and returns current results from every endpoint of interest across the enterprise environment.

Tanium Protect

Tanium Protect manages native operating system controls at enterprise scale. Anti-malware, application control, and exploit mitigation are simplified, and organizations can move from investigating their environment to taking proactive action to protect against threats instantly.

Figure 2

How Tanium Modules Meet CDM Functional Requirements

	Tanium Functional Modules								
CDM Functional Requirements Rollup	Enterprise	Core Platform	Threat Response	Asset	Comply	Discover	Integrity Monitor	Patch	Protect
CDM Phase 1									
II - 2.1.3 HWAM Tool Functionalities	X	X	X	X	X	X	X	X	X
II - 2.2.3 SWAM Tool Functionalities	X	X	X	X	X	X	X	X	X
II - 2.3.3 CSM Tool Functionalities	X				X				
II - 2.4.3 VUL Tool Functionalities	X				X			X	
CDM DEFEND (Phase 3)									
II - 4.2.2.6 MNGEVT Tool Functionalities	X	X	X		X	X	X	X	X
II - 4.3.2.5 OMI Tool Functionalities	X	X	X		X	X	X	X	X
II - 4.4.2.4 DBS Tool Functionalities	X	X	X		X	X	X	X	X

Implementation matters

Tanium prides itself in its professional support to implementation:

- Tanium SMEs are assigned to every implementation engagement – at no additional cost.
- Integrators, agency users, and stakeholders are provided copious installation materials, training, Ops Concept documents, etc.
- Every implementation includes plug-ins to popular third-party cyber tools, including Splunk, Palo Alto Networks, and many others. Each license includes a robust customization toolkit with examples of policy-driven scenarios and sample code. Tanium supports common data exchange formats, including CEF, syslog, json, and delimiter-separated values, among others. Tanium also provides a fully-functional SOAP API and every Functional Module has a REST API.
- For integrators and agency decision makers, Tanium provides Proof of Concept and Cyber Lab installation support, when requested or required. Integrators have found this particularly useful when making "competitive advantage" decisions about which tools to recommend and field.
- Tanium offers CDM Dashboard support out-of-the-box.

These features and benefits have proven results. Implementation times are faster, numerous heterogenous host/client agents can be replaced by the Tanium lightweight agent and, once piloted, the pilot instance can easily go live into the operational environment. Additionally, because of Tanium's Linear Chaining Architecture, dozens, if not thousands of servers can be eliminated from obsolete hub-and-spoke product implementations.

The value of Tanium

Tanium's integrated platform of cyber defense tools are generational improvements over current mainstream technology, offering complete enterprise-wide scans in seconds instead of days. This industry-leading performance is made possible by Tanium's unique and advanced linear chaining architecture, which scales exceptionally well and eliminates vast numbers of costly and slow servers and network traffic. Here are a few examples of the difference Tanium can make in an agency's enterprise network:

- Pushed >2 million patches in under 4 hours while server throughput was capped at 250 Mbps for the app.
- Found >200 instances of a leaked document in seconds.
- Identified that only 2% of endpoints were actually patch-compliant while existing tools indicated 95-97% patch-compliance.
- A client's SOC was able to reduce the number of endpoints on which they used Encase imaging by about 80% by using Tanium Trace for preliminary investigations.
- During the WannaCry outbreak, a client used Tanium to patch 3,000+ endpoints that existing tool was not able to patch successfully. This increased compliance from 95% to 99.9%.
- During a training class, a real-world event kicked off. After only one day's worth of training, client users were given permission to use Tanium for their investigation. They were able to complete their mission at a site halfway around the world in a matter of hours. Once complete, they were amazed at the speed and capabilities of Tanium and said their existing toolset would have taken weeks to get the same results.
- Tanium found >5,000 endpoints with McAfee Antivirus and Symantec installed and running, even though they had switched to Symantec 18 months earlier.

For a demo, cyber lab installation opportunities and Federal Agency Use Case discussions, please contact sales-federal-team@tanium.com.

TANIUM

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control, and manage millions of endpoints across the enterprise within seconds. With the unprecedented speed, scale, and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations.

tanium.com @Tanium info@tanium.com