Whitepaper

Tanium and CDM

Federal Agencies Need a Transfomational Platform to Combat Modern Cyber Threats

Table of Contents

Executive Summary

The purpose of this white paper is to provide a fact-based and data-driven perspective of why the Tanium platform is a superior alternative to HCL's BigFix, specifically with respect to the Capabilities Group 1 Requirements of CDM Defend and the complex challenges facing federal agencies.

This paper discusses the following in detail:

- Security concerns regarding the foreign ownership of BigFix's intellectual property
- Technical and performance deficiencies of the BigFix architecture
- Tanium Mapping to CDM Capabilities Group-1 Requirements
- Agency benefits of the Tanium Platform, including:
  - Reduced cost
  - Timely and reliable IT and security data for critical risk management decisions
  - Reduced complexity to manage and prioritize security risks
  - Scalability for unified endpoint management (UEM) and unified endpoint security (UES)

HCL BigFix Concerns

US Government agencies are targets for malicious cyberattacks from increasingly more sophisticated and capable adversaries. Enterprise networks are also more complex than ever before—endpoint (EP) growth, the explosion of IoT and the multitude of point tools have further complicated cyber defense problems that require modern, scalable and reliable risk management solutions. Agencies find that they are often left open to vulnerabilities, disruption, EP agent bloat and they lack trust in BigFix's results.

Asset management is a critical component of managing risks and meeting compliance requirements, so having accurate, timely data is critical for risk management decisions. As many Federal agencies have come to recognize, BigFix's EP management solution is costly, slow and unreliable as demonstrated by the need to run parallel instances of functionally redundant point products from vendors such as Microsoft, Forescout and Tenable, to name a few.

Security concerns regarding the ownership of BigFix's intellectual property by HCL Technologies, Ltd. (HCL), a foreign-owned and controlled company headquartered in a country with whom the US has no foreign Trade Agreement (i.e., HCL/BigFix is not Trade Agreements Act and Buy American Act compliant) have become central to risk management concerns of agencies trying to protect sensitive mission and citizen data and not share vulnerabilities with offshore concerns. The pedigree of the code and India's unfettered access to HCL's and its clients' data due to that country's unusual data transparency laws have become serious concerns among agency risk and accountability managers. Thus, BigFix puts agencies in a very precarious risk management position.

But, it's not just about foreign nationals developing cybersecurity software and Federal agency data protections. Performance matters. Due to the inherently inefficient nature of the BigFix architecture, scaling is problematic and extremely expensive, especially for clients with high availability (HA) requirements.

Due to the recent and relatively abrupt change in BigFix's ownership, product stability, roadmap and functionality have also become major concerns. Many BigFix customers have complained that IBM let BigFix innovation atrophy over the last four years. What's important to note is that HCL is primarily an international IT services company, not a commercial software product developer. They rely now heavily on their current partner, IBM, for code development, enhancement and maintenance. Agencies are concerned about what happens when that relationship eventually goes away.

The costs associated with operating and maintaining BigFix are especially troubling for large Federal enterprises. Scores measured by the Federal Information Technology Acquisition Reform Act (FITARA) could be significantly improved with the removal of hundreds, if not thousands of root, application, data base and relay servers and the software that runs on them. Leaving this obsolete solution in place handcuffs agencies, preventing vital investments in more modern and cost-saving solutions.

These fundamental problems require an innovative solution and this paper hopes to address them.

Tanium CDM DEFEND Capability Group-1 Mapping

Tanium at its very core is a modern and comprehensive endpoint management platform with core capabilities and optional functional modules that provide comprehensive security controls and risk management tools through unparalleled visibility into enterprises having tens of thousands to millions of EPs. The following section maps CDM DEFEND Capabilities Group 1 (CG-1; a.k.a. legacy CDM Phase 1) requirements to Tanium capabilities. The matrix below summarizes Tanium's ability to cover the requirements set forth in CG-1.

A minimal Tanium deployment which fully satisfies CG-1 requirements for an up-to one million EPs enterprise would include three Tanium appliances (six for HA applications), the Tanium Core Platform and Asset, Discover and Comply modules. Tanium is H/W platform agnostic. Its software can run on optimized Tanium appliances, in the cloud (public/private/FedRAMP or hybrid) or on customer-premise equipment.

Tanium's Core Platform provides foundational capabilities such as the Tanium Console, Tanium's Connect and Trends features as well as administrative functionality such as data retention, system deployment tools and host agents. The Core Platform is mandatory in all Tanium deployments. It's important to consider that, unlike BigFix, the addition of functional modules requires no changes or additions to the agent, nor additional servers.

Table 1 below summarizes Tanium's ability to cover CG-1 requirements:

Capabilities Group 1 Req's	General Description	Tanium Core	Tanium Asset	Tanium Comply	Tanium Discover	BigFix Lifecycle	BigFix Inventory	BigFix Compliance	BigFix IBM's QRadar® *
HWAM	Multi-factor inventory & baseline of IP-addressable HW. Ability to identify and locate unauthorized HW on network.	√	√		√	√			
SWAM	Multi-factor inventory & baseline of SW installed on managed HW devices. Ability to identify and locate unauthorized SW.	√	√				√		
CSM	Manages configuration baseline benchmarks and actual settings of HW and SW assets. Assigns risk scores based on incorrect settings.			√				√	
VUL	Discovers, identifies and locates known security vulnerabilities defined by CVEs and other sources in network assets.	√		√	√				√
Max Endpoints	N/A	Up to 1,000,000 with three (min recommended) servers				Up to 250,000 with 250 to 500+ servers			

** Note: To meet Vulnerability Management requirements, BigFix offers a separate integration with IBM's QRadar® which adds an additional external point solution product*

BigFix and Tanium operate in fundamentally different ways to satisfy CDM requirements. The following sections will detail these differences to allow DHS to better distinguish advantages and disadvantages between the two platforms and clearly understand the immense value of a unified EP management and security platform.

HWAM

Tanium fully meets all of the operational and functional requirements for HWAM as detailed in DHS's CDM requirements using its Core Platform, Asset and Discover functional modules. With Tanium, assets are managed with a single agent irrespective of the modules being used. For unmanageable devices such as routers, switches, printers, IoT devices, etc., Tanium's Discover module can find and report back basic information about them as well as track their presence over time and determine their interaction with Tanium managed devices.

BigFix also relies on an agent installed on all managed EPs. Like Tanium, HWAM attributes are provided out-of-the-box; however, with BigFix there are instances where attributes require customization within a BigFix Analysis, requiring agencies to have access to a BigFix SME that is familiar with the arcane proprietary Relevance language. This skill is becoming increasingly scarce and many agencies struggle to customize and configure attributes accurately.

The Achilles heel of BigFix's performance is in the manner in which content is executed on the EP and the massive EP burden and network traffic load that creates. Each individual piece of content to which an EP is subscribed (typically thousands) is evaluated continuously during what's called an Evaluation Cycle. This means that the more content subscribed, the longer the Evaluation Cycle. In instances where there is either too much content added or there are inefficient Relevance clauses created (e.g., iterating through entire filesystems or making Active Directory queries), clients become "stuck" in a never-ending loop and never get through their entire Evaluation Cycle before starting it over again. This state is difficult to detect, but when this happens, any new content added (e.g., a new vulnerability or patch) will never be evaluated until manual intervention is taken either on the affected EP(s) or the content created.

For unmanaged devices, BigFix has an NMAP-integrated solution. In order to function correctly, agencies must use highly trained network SMEs to properly deploy dedicated NMAP scanners across all their various subnets. This is a manual process that can lead to many missed devices as subnets may be created without a scanner. In such a case, the entire subnet and its assets simply won't be scanned, and what cannot be seen cannot be managed. Once devices are discovered and visible in the console, analysts must employ a manual method to categorize them leaving many device tags with a very low degree of accuracy barring individual investigation and intervention.

By contrast, Tanium's patented linear chain architecture virtually eliminates network traffic and EP burden compared to BigFix. Additionally, since this is executed using each of the Tanium-managed EPs themselves, visibility into the entire network is automatic and assured. With the Tanium Asset module, most HWAM attributes are provided out-of-the-box. Unusual or unique devices requiring a custom sensor can be scripted using any of several popular scripting languages (e.g., PowerShell, VBScript, Shell, Python), simplifying deployment efforts. For unmanaged devices, Tanium Discover provides numerous easily configurable methods (NMAP, ARP, ICMP), which can be combined to provide the highest degree of confidence. Within Discover, auto-labels can be created to identify common devices using attributes unique to each with a very high degree of accuracy and these devices can be tracked over time.

While both tools meet HWAM requirements, Tanium delivers far superior speed and accuracy with an infrastructure that is a fraction of that required by BigFix.

SWAM

Tanium fully meets all of the operational and functional requirements for SWAM using its Core Platform and Asset functional module.

With a separate BigFix Inventory license, a new server is required to host a GUI front-end for the SWAM-related data. The data relies on regular software scans being run on each EP. The EPs cache their results each scan and a separate action is run later to upload the results to the BigFix server. From there, a separate job regularly (by default every 24 hours) imports the data from the BigFix server to the BigFix Inventory server. For larger deployments, these time gaps between each of the separate jobs make it difficult or even impossible to get SWAM data from the entire enterprise within the CDM-required timeframe (72 hours). The data is accessible from the BigFix Inventory server via an exposed REST API.

With Tanium Asset, scans are run regularly on EPs and their data is sent immediately to the Tanium server. Because these sorts of scans are changes-based, network traffic is kept to an absolute minimum while administrators can be alerted of new software installs within seconds. These very lightweight and quick scans enable

agencies to monitor their assets instantaneously. For example, one large DoD client scans their 600,000-EP enterprise every 15 minutes, whereas BigFix struggles to scan networks having only 250,000 EPs in 72 hours. Software rationalization is another key concern of Federal agencies and it has two components: a) license reclamation for unused or underused applications, and b) an agency's ability to complete their cybersecurity mission with fewer and often overlapping point solutions. Tanium inherently does both without the need for supplemental and expensive products. The latter component is a key Tanium feature in that its agent serves all Tanium functional modules which permits agencies to eliminate redundant point solutions, EP agent bloat and the associated costs necessary to field and maintain redundant software and hardware.

CSM

Tanium fully meets all of the operational and functional requirements for CSM using its Core Platform and Comply functional module.

With a separate BigFix Compliance license, another new server is needed to host a GUI front-end for the CSM-related data. This is a complex solution that uses HCL-provided Fixlets and BigFix Analyses that are customized for agency-specific values, with supported by benchmarks from CIS and DISA STIGs on most platforms. Any benchmarks that are not provided by HCL must be created and maintained by each individual agency, which are not generally shared, creating redundant development and effort. The Fixlets and BigFix Analysis properties are each added to the clients' Evaluation Cycle, adding additional burdens to the scans. The Fixlets indicate compliance with the check and the Analysis properties return the actual values set on the devices for each of the checks. This data is regularly (by default every 24 hours) imported from the BigFix server to the BigFix Compliance server, where it is then normalized for consumption. The data is accessible from the BigFix Compliance server via an exposed REST API.

With Tanium Comply, any standards-based benchmark that is provided by the managing organization (CIS, DISA STIG, etc.) in XML format can be easily imported and customized for agency-specific values. Multiple industry-standard scan engines are supported (Java, CIS-CAT, SCC, etc.) and deployed to managed EPs, which run regular scans against the deployed benchmarks.

VUL

Tanium fully meets all of the operational and functional requirements for VUL using its Core Platform and the Comply and Discover functional modules.

For Vulnerability Management, BigFix offers an integration with another separate license for IBM's QRadar®, which is rarely used by BigFix customers, necessitating an investment in yet another external point solution product. When implemented, this solution relies on deploying scan profiles to EPs, which are run regularly. The data is then imported into BigFix and can be viewed in Web Reports.

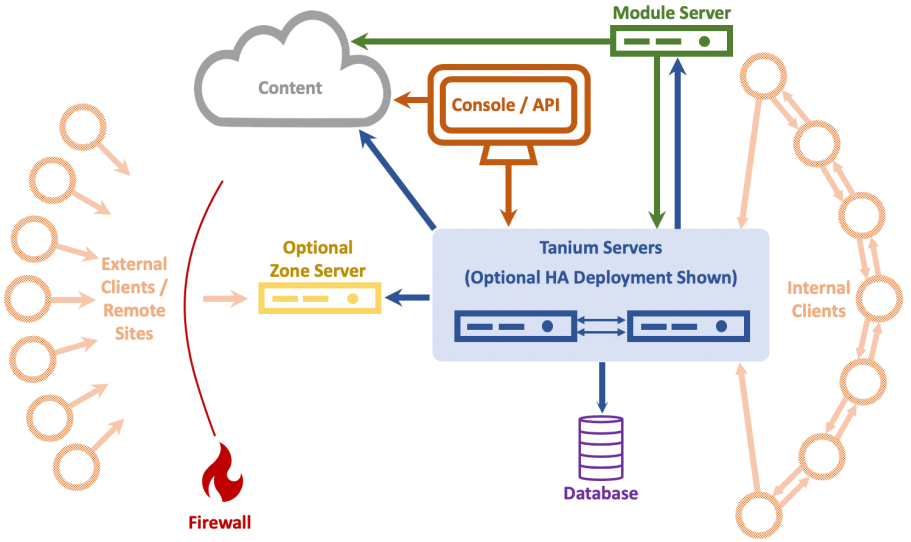
With Tanium Comply, there is a Tanium-managed vulnerability library that is shipped out-of-the-box that contains all published CVEs. Agencies can also import their own OVAL definition files to supplement the Tanium library. Again, because of Tanium's inherently efficient and fast scanning capabilities, vulnerability scans can be scheduled to run almost continuously, providing the best possible visibility into asset exposure and risk.

Representative Use Cases

Big Fix Replacement

Tanium has revolutionized the endpoint management industry through

its patented, yet open, platform and communications architecture. Legacy architectures typified by products like BigFix rely on massive hardware deployments in order to scale. To illustrate, BigFix has a rigid vendor-recommended limit of 250,000 EPs per root server. That means that for enterprises having more than 250,000 EPs, BigFix must be designed with less than or equal to 250,000-EP enclaves. At scale, the architecture can consist of a BigFix server, separate servers for software applications, configuration management and patching, etc., in addition to relay servers which manage content and distribution. In a BigFix instance of 250,000 EPs, relay servers alone could range in number from 250 to well over 500 servers, and of critical importance, clients must remain associated with their assigned relay server. Tanium, on the other hand, can manage up to a million EPs with only three Tanium appliances (optimized servers) and is platform-agnostic (private/public/FedRAMP or hybrid cloud, Tanium appliances or customer-premise equipment). BigFix is further limited by the number of concurrent users that its Console and/or WebUI can support - currently the WebUI (which has no API) only supports up to 30 concurrent users and 120,000 managed EPs. As discussed in Section 2.0 above, BigFix scales poorly, continually produces questionable results, especially in enterprises having a large amount of content and often requires manual intervention to manage and maintain.



Tanium's architecture leverages its linear chain topology (please see Figure 2 below) to minimize traffic on the network and to achieve enterprise-wide scans in seconds or minutes rather than days or weeks, compared to BigFix. Endpoints in the linear chain are aware of their neighbors and will report a device that joins adjacent to its address space. Thus, analysts are alerted if an asset joins the network and whether or not it has the Tanium agent, allowing the analyst to take swift action to assess and remediate its level of compliance and risk. Endpoints with the agent who join but are missing content will receive the missing content automatically.

Tanium's ability to out-perform BigFix in finding issues, vulnerabilities and even unmanaged assets attached to the network has become legendary among Tanium customers and users. The data for each example in the list below was volunteered by different Federal customers regarding their experiences with Tanium's results and performance:

- One of the most regulated government agencies with 60,000 EPs was spending ~$4.8M annually to support their BigFix environment and was contemplating adding Life Cycle Management for additional functionality. As part of the Analysis of Alternatives, the customer conducted a Proof of Concept (POC) pilot with Tanium's Operations Suite against BigFix resulting in the following:
  - Reduced infrastructure by eliminating 1,555 servers and realizing 98% savings
  - Reduced patching cycle time by 98.9% from 4 weeks to 8 hours
  - Reduced related costs from $4.3M resulting in savings of 49.8%
  - Recognized a Cost Avoidance of an additional $7.92M by not adding the Lifecycle Management software and the required additional infrastructure

- Reduced overall project spend by ~$10M (82%) by standardizing on Tanium's security Operations Suite

- BigFix was being used for various purposes: patching, software deployments and all-purpose Fixlets for updating regkeys, files and settings. However, it was exceptionally chatty on the network and had scaled such that it required more than 1,700 relay servers. Tanium POC pilots using a broad base of use-cases demonstrated that its solution was much faster, more efficient and provided centralized visibility into the client's large enterprise. As a direct result, BigFix was replaced with Tanium globally.

- Once installed, Tanium identified that only 2% of EPs were actually patch-compliant while BigFix and its backup SCCM, indicated 95-97% patch-compliance.

- During the WannaCry outbreak, a US Department of Defense client contacted Tanium to ask for its assistance to patch vulnerable and unknown assets:

  - Friday afternoon – Initial call
  - Saturday morning – Tanium had identified vulnerabilities and remediated over 485K of the >600K devices
  - Within 24 Hours – 80% of their systems were patched. This included >3,000 EPs that their existing tool was unable to patch successfully, increasing compliance from 95% to 99.9%
  - Within 48 Hours – All of their systems were remediated
  - Monday morning – Work as usual

- A federal government client was able to push >2 million patches in under 4 hours while server throughput was restricted to 250 Mbps by the system administrator.

- During a training class, a real-world incident occurred. After only one day 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 reported that they were amazed at the speed and capabilities of Tanium and said their existing toolset would have taken weeks to get the same results.

- One of Tanium's clients found >200 instances of a leaked document in seconds across their enterprise.

- When initially deployed, Tanium discovered >5,000 EPs with conflicting McAfee and Symantec antivirus products installed and running, even though the customer had switched to Symantec's products throughout its enterprise 18 months earlier.

- A large federal health-related service recently implemented Tanium. They had 6 different tools, all overlapping. With this roll-out they reported that they will save over $6M a year by the tool rationalization approach.

- The Armed Services of the United States and the Intelligence Community currently entrust over 2.5M EPs to Tanium's endpoint control and management.

When contemplating replacing BigFix, whether because of performance,, risk-trust issues, cost or concerns about foreign ownership and data integrity, Tanium's lean architecture and building-block platform represents a transformational leap forward which will pay for itself over the course of months instead of years. Because of Tanium's high performance and because so much hardware and server software/ contractor admin resources can be retired or repurposed, agencies also will get windfall benefits such as higher FISMA, FITARA and AWARE scores. In enterprises with up to one million EPs, additional physical servers and additional host agents will not be required to deploy the new functionality (Note: In the case where large numbers of EPs are being added – not just additional software functionality delivered – additional CPUs, memory and drive storage may be recommended to improve existing server performance). Also, for agencies or components requiring

HA, simply doubling the minimum number of appliances or servers from three to six will suffice.

What about all those Fixlets? Tanium provides expert technical support during switch-over to convert custom functionality incorporated in Fixlets which may be unique to an agency and not be part of Tanium's commercial offering. Thus, agency investments in BigFix customizations can be preserved.

Top Reasons Customers Choose the Tanium Platform over BigFix:

- Scalability – Tanium scales to one million endpoints and beyond while needing only three appliances. Big Fix has inherent scalability issues and is vastly more expensive to maintain and deploy. Deployment of new Tanium modules will not require additional servers/appliances or multiple agents on the managed hosts.

- Ease of Use – Tanium's primary query method is through its patented natural language parser. Natural language "questions" generate queries that can be run ad-hoc, stored and/or scheduled to be run automatically, averting the need for scripters and programmers. Vivid data visualization capabilities make it easier to measure and communicate insights across the enterprise. Extensible and open, the Core Platform contains a variety of ready-to-use connectors, and its open APIs allow seamless integration of endpoint data with other IT systems.

- Speed – Tanium can scan and produce results in enterprises having hundreds of thousands of EPs in around 15 seconds. This can allow agency risk managers to do on-demand or automated scans in as little as every 15 minutes without burdening the EPs or the networks. This ensures that the data being fed to the CDM Dashboard is timely and accurate. It also gives the risk managers the ability to take actions instantly – something that will most assuredly improve AWARE scores.

- Reliability – Whether brought in to validate BigFix's performance in an incident/event, or in head-to-head comparisons, Tanium consistently finds undiscovered and unmanaged assets which should have been under BigFix control, uncovers out-of-compliance assets and assets that have missed important patch cycles which should not have gone undetected.

- Service – Tanium's service delivery model is also differentiated from HCL. Technical Account Managers (TAMs; Tanium product SMEs) and Customer Success Managers (CSMs) are assigned to support the mission of every Tanium instance at no additional direct cost to the Government. These experts provide support at project inception and continuously support throughout the lifecycle of the deployment. All Tanium training, whether in-person or self-paced, is also provided at no additional direct cost to the Government. In the rare event that dedicated on-site support is required, Tanium can provide, as an option, fully trained, cleared (when required) operators.

- Trust – Tanium is a mature US company that does not use foreign nationals to develop or access the software for support purposes or have access to Federal agency data. Cleared technical staff are also available.

To summarize, Tanium provides Federal agencies with a true enterprise-scale cybersecurity solution which can completely and confidently replace BigFix and grow to support mission needs. In addition to the basic CG-1 capabilities BigFix provides, the Tanium platform can be extended efficiently and cost-effectively to cover CDM DEFEND's more advanced security protections and reporting capabilities required under DEFEND's Capabilities Groups 3 and 4 requirements.

Network Access Control for Advanced Compliance-based Control

ATanium monitors managed assets for continuous compliance and can identify unmanageable assets such as switches and routers, IoT

devices, IP and mobile phones, etc. For greater visibility and control of assets that cannot be configured with a Tanium agent Tanium has integrated Cisco's Identity Services Engine (ISE) with its own Network Quarantine Service (NQS) to control agentless assets on the network. When an asset is deemed non-compliant, meaning it has open high-risk vulnerabilities, missing critical patches, missing essential software or other configuration/policy violation issues, Cisco ISE works in conjunction with Tanium to adaptively isolate and analyze those higher risk assets. Being able to adaptively isolate an asset allows agencies to maintain mission operations while still controlling network access or adding additional agents.

As an example, if a user attached an out of date, non-compliant device, such as a BYOD tablet or laptop, to the network, Tanium and ISE would restrict that device's access to an isolated VLAN, limiting access to critical resources until the device is brought into compliance or removed, per policy. This could involve making configuration changes, installing or uninstalling software, patching the device or other remedies, including extended quarantine, if necessary. Once the device is compliant, Tanium can instruct ISE to release restrictions.

Additionally, Cisco ISE and its related software and hardware capabilities are CDM DEFEND BOUND-requirements compliant, meaning that a Tanium instance integrated with Cisco ISE can comply with all Capabilities Group 3/Phase 3 requirements.

Tanium also has instances with clients where its software interfaces with products from companies such as Forescout to leverage other vendor solutions which address unmanageable devices as a point solution. By leveraging a client's installed base of legacy software/solutions, Tanium can deliver cost-savings integrations by leveraging the investments clients have already made in such tools.

Threat Hunt

The purpose of active threat hunting is to reorient and retool an agency from passive and reactive defense of its assets to an active search for, and containment of, sophisticated threats that can evade normal security controls and measures. The most alarming trend in information security today is the pace of advancement in skill, precision and tactics at an attacker's disposal. Incident response teams are constantly under siege and almost all are powerless when combating sophisticated and determined attackers. This is because many defenders rely on a toolbox of point solutions whose tools can only provide views of their enterprise that are hours, days, or even weeks old. Sound security relies on reliable, real-time data and the ability to move at the same pace or more quickly than the adversary. Providing this capability involves skilled threat hunters and a set of sophisticated and integrated tools that provide enterprise visibility in real-time.

Tanium's Threat Response is a comprehensive set of tools that enable threat hunters to hunt, detect, investigate, contain and remediate threats and vulnerabilities with unparalleled speed and scalability. This provides hunters the ability to:

- Compile evidence, a timeline and reconstruct the story about what happened on an EP with in-console data enrichment from internal or third-party intelligence sources
- Automate threat detection with continuous, proactive and real-time scanning for Indicators of Compromise (IOCs) and resultant alerting
- Search for suspect files, explore registry settings, collect information, or hunt for anomalies across the enterprise and eliminate threats in seconds

Threat Response provides the capability to investigate suspicious anomalies found locally or via imported intel such as IOCs and then do immediate scans to get alerts within seconds and/or continuously scan for that intel on

EPs. Suspicious anomalies can trigger warnings from Tanium Signals, which provides real-time alerting as malicious or suspicious activity occurs on EPs. As alerts are received in Threat Response, analysts are able to review the alert, which includes context around what triggered it, and then pivot to investigate forensic details on the specific EP in question. This includes the ability to make a live connection to the EP in order to view forensic events as they are being recorded, as well as the ability to navigate the file system and collect artifacts from that EP. In addition to a live connection, hunters may also use Tanium Live Response to pull back forensic artifacts to a central location from the EP in question.

The Tanium Core platform was designed from the ground up to provide real-time, context-rich information. The ability to get information from the entire network and take actions on the entire network in seconds gives customers unparalleled visibility and control. Having this immediate visibility and control, at scale, reduces the amount of time it takes to make business decisions, investigate events and effect change. Integral to the Core platform is Tanium's Connect module which provides the ability to gather information and alerts from the entire network in seconds using the Tanium Platform, and send that information to external resources such as SIEM tools, CMDBs, SQL Databases, simple email alerts, or even files.

When it comes to threat containment, it's all about a bad actor's dwell time, ability to move laterally and the resulting compromise of high-value data assets. Tanium's Reveal detects sensitive unstructured data at rest on EPs across an entire enterprise and can continuously monitor for artifacts that match patterns. When sensitive content that matches a pattern is discovered, files can be tagged for further analysis or immediate action can be taken to address regulatory compliance, information security or data privacy issues.

The ability to have real-time visibility and control over what is happening on the network is critical for incident/event recovery. Not only can Tanium be used to interrogate and investigate EPs, but it can also be used to secure the network by scanning EPs for vulnerabilities and compliance with Tanium's Comply module. Comply provides a vulnerability library for scanning impacted systems in minutes. Comply scans surface vulnerabilities in the enterprise, provides CVSS scoring and allows for rapid identification of impacted EPs. Tanium's Threat Response is a unified workbench which provides the ability to identify, scope and investigate and alert cyber analysts in a matter of minutes using real-time data.

Next Steps

Agency Pilot Support

Tanium offers all potential clients a rapid cost-free, tech-expert supported and comprehensive Proof of Concept (POC) pilot to demonstrate the functional capabilities of the Tanium platform. Within minutes of deploying Tanium to the enterprise, agencies are able to perform comprehensive software and hardware inventory scans on "live" assets, complete configuration settings compliance and vulnerability scans and rapidly search for IOCs. This POC process allows agencies to perform hands-on, focused, use case-driven assessments of the Tanium platform in their own environments. Because Tanium only requires a single application server and module server, there are minimal infrastructure requirements. In most cases, an all-in-one virtual appliance can be used for temporary POCs.

Appendix

API: Application Programming Interface

ARP: Address Resolution Protocol

AWARE: Agency-Wide Adaptive Risk Enumeration

BOUND: CDM Boundary Protection

BYOD: Bring Your Own Device

CDM: Continuous Diagnostics and Mitigation

CG-1: CDM Capabilities Group-1

CIS: Center for Internet Security

CIS-CAT: Center for Internet Security - Configuration Assessment Tool

CMDB: Configuration Management Data Base

CPU: Central Processing Unit

CSM: CDM Configuration Settings Management

CSM: Customer Success Manager

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System

DEFEND: Dynamic and Evolving Federal Enterprise Network Defense

DISA STIG: Defense Information Systems Agency Security Technical Implementation Guides

EP: Endpoint

FedRAMP: Federal Risk and Authorization Management Program

FISMA: Federal Information Security Management Act

FITARA: Federal Information Technology Acquisition Reform Act

GUI: Graphical User Interface

HA: High Availability

HCL: HCL Technologies Ltd., Noida, India

HWAM: CDM Hardware Asset Management

IBM: International Business Machines Corporation, Armonk, NY

ICMP: Internet Control Message Protocol

IOC: Indicators of Compromise

ISE: Identity Services Engine

NMAP: Network Mapping (tool)

NQS: Network Quarantine Service

OVAL: Open Vulnerability and Assessment Language

POC: Proof of Concept

REST API: Representational State Transfer Application Programming Interface

SCC: Strongly Connected Components

SCCM: System Center Configuration Manager

SIEM: Security Information and Event Management

SME: Subject Matter Expert

SQL: Structured Query Language

SWAM: CDM Software Asset Management

TAM: Technical Account Manager

VUL: CDM Vulnerability Management

WebUI: Web User Interface

XML: Extensible Markup Language

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