

# **Top Tanium Use Cases**



Endpoint Detection and Response

Security Hygiene

IT Operations Management

IT Asset Visibility

# **Tanium Product Modules**

# **Stop Breaking Your Endpoints**

#### See everything, do anything with Tanium

Relying on a patchwork of point solutions and legacy platforms is a recipe for failure. It's time to re-platform. Take back control with Tanium.

#### **Tanium Core Platform**

Regain control by asking questions about endpoints in plain English and getting accurate answers in seconds so corrective action can be taken quickly. Visualize results and feed endpoint data into SIEMs, help desk ticketing systems, CMDBs, and other third-party systems for additional analysis.

	Ask a Question	Question Builde
	get ip address and domain name	Q Search
	Please select one of the following queries:	
	Get IP Address and Domain Name from all machines	
	Get Tanium Client IP Address and Domain Name from all machines	
	Get IP Address and Domain Member from all machines	
	Get IPv4 Address and Domain Name from all machines	
	Get IPv6 Address and Domain Name from all machines	
, Ir	ateract Summary	
F	undamental Interactions with Endpoints	
	teract gives you instantaneous endpoint visibility and control to make better decisions and take faster actions.	

#### **Tanium Discover**

Find unmanaged assets within the enterprise environment and bring them under control in seconds. Take immediate action on rogue assets and get a rich set of information for all located assets.

0	Discover			Manage Home Page	0
	event types as a source: • Rules notifications • New Unmanaged Interfaces • New Managed Endpoints • Lost Interface				
0	Metrics				
	Total Managed Interfaces 260	Managed Interfaces	Total Unmanaged Interfaces 46	Unmanaged Interfaces	
		85 %		15 %	
	200	60 76	40	15 %	
•	Reports	03 %		15 %	
-		00 76		15 %	
-	Reports naged Interfaces	OO 76 Managed Interfaces		13 76	

#### **Tanium Asset**

Get a thorough and up-to-date picture of hardware and software inventory to make the right decisions deploying assets efficiently, and enrich Configuration Management Databases with accurate information.

<b>F</b> TANIUM				
All Software All Software Report				Create Copy
Filters: No filters applied				
items: 1,029			Search Report	
				Text Wrap:
Name	Version	Wendor	= count	=
bgssglue	0.1	CentOS	906	
	0.1	CantOS CantOS	906	
which				
which yum-metadata-parser	2.19	CentOS	906	
which yum-metadata-parser yum	2.19 1.1.2	CentOS CentOS	906 906	
which yum-metadata-parsee yum xx-tama-compat	2.19 1.1.2 3.2.29	CentOS CentOS CentOS	906 906 906	
Itopseglue which yum-metadate-paneer yum xxo-zema-compat gdom gruppg2	2.19 1.1.2 3.2.29 4.990.9	CentOS CentOS CentOS CentOS CentOS	906 906 906 906	

#### **Tanium Patch**

Customize patch workflows with up-to-the-second endpoint visibility and control. Define custom workflows and generate patch reports from every endpoint across the environment.

	DEMO.TAN	NUN	.com						ged In: chanel.cha d: 7.2.314.3019   UI: 1	
Patch			> Pato Patch							
Home										
Patches							Patches: All	Applicable   Not Applicable	Filter: All	lelected
All		138							Filter by text	Q
- Contraction -										C
Patch Lists			* =	Title	Severity	Release Date	Vendor KBs	CVEs	Applicable	
Blacklists			٠	November, 2016 Security Monthly Quality Rollup for W	Critical	12/13/2016	KB3197868	CVE-2016-7241 CVE-2016-723	9 CV 170	1
Deployments			•	2017-05 Security Monthly Quality Rollup for Windows	Critical	5/9/2017	KB4019264	CVE-2017-0064 CVE-2017-007	7 CV 170	
Pepioymenia			•	Security Update for Windows 7 (KB2803821)	Critical	8/13/2013	KB2803821	CVE-2013-3127	170	
Deployment Templates			•	Security Update for Windows 7 (KB2884256)	Important	10/8/2013	KB2884256	CVE-2013-3894 CVE-2013-388	B C\ 170	
Scan Management			•	Security Update for Windows 7 (KB2868038)	Important	10/8/2013	KB2868038	CVE-2013-3894 CVE-2013-388	B CV 170	
scan wanagement			•	Security Update for Windows 7 (KB2862335)	Important	10/8/2013	KB2862335	CVE-2013-3894 CVE-2013-388	8 C\ 170	
faintenance Windows			٠	Security Update for Windows 7 (KB2887069)	Important	12/10/2013	KB2887069	CVE-2013-5058 CVE-2013-390	7 CV 170	
			•	2017-12 Security Only Quality Update for Windows 7 f	Important	12/12/2017	KB4054521	CVE-2017-11885 CVE-2017-11	127 170	
			٠	Internet Explorer 11 for Windows 7	None	5/13/2014	KB2841134	None	170	
			•	Security Update for Windows 7 (KB3149090)	Important	4/12/2016	KB3149090	CVE-2016-0128	170	
			•	Security Update for Windows 7 (KB2973201)	Important	7/8/2014	KB2973201	CVE-2014-2781	170	

## **Tanium Deploy**

Simplify software deployment, update, repair, and reclamation to reduce risk and cost.

NIUM
New Package
_
Package Files Add -
Origin: Vgadcfl/datalappslChromelgooglechromestandaloneenterprise.msl
googlechromestandaloneenterprise.msi <u>4</u> Stor: 44.48 MB (46,641,152 Bytes)
8HA-259: c39c71f3696bae0fb461584a3d3ff00a48e408879f3aa0c78b4e8c1fc2ee7a8b
Extract Available
MSI Information: peoglechromestandatoneenterprise met  Extract
General Information
Onieral mitrimation
Product Vendor: Google, Inc. OS Platform: Wedows \$
Product Name: Google Chrome
Product Version: 66.208.49227
Deploy Operations Select what operations will be available for this software package.

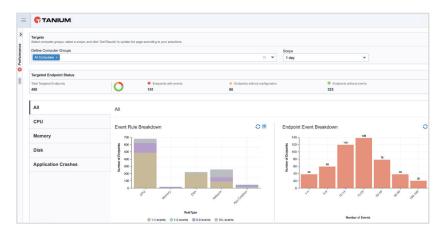
#### **Tanium Map**

Quickly and precisely understand your application infrastructure and interrelationships between endpoints. Prevent self-inflicted outages, identify single points of failure, provide redundancy, and segment applications.

Map Home	<	Home > Maps Tanium Server Map 10.70.144.75 Englante: 10.70.144.75 Englante: 10.70.145.75 Englante: 10.70.145.75 Englante					
Applications		Endpoints: 10.70.144.76 Duration: Leel 30 days Min # of Connections: 1 EDIT Selected Endpoints					
Maps		126 (100%)					
		<ul> <li>Filter Results:</li> </ul>					
		Group By: Operating Bystem *	deselect al   collapse all	>	Endpoints	Defined Applications	Processes
		internet (123)     Windows Server 2018 Standard (5)			Ik Name	* Search	0
					Applications 4		
					C + Christen	ome tic 1 2	
					Tani     Endpoint	ium Full Stack	
		<b>.</b>			C > Splu Endpoint		
		-			• MS     Drdpoint	SQL Server	
						ans: MS SQL	Actions +
		()					

#### **Tanium Performance**

Monitor, investigate, and remediate endpoint performance issues, quickly at scale.





#### **Tanium Protect**

Manage native operating system controls at enterprise scale. Simplify application control, anti-malware, and exploit mitigation to reduce the cost and complexity of endpoint security.

AppLocker			
Mode:	Blocking	de logs AppLocker activities in the Windows Event Log and does not p will prevent processes from launching.	prevent processes from launching.
Support URL:		Optional	
	Displays a custom UI	RL when users try to run a blocked app.	
Import Rules From XML:	Please choose the Ap preview will be provid	ppLocker file below. Note that Protect will not be able to create all Rul led of the exclusions.	es depending on their configuration. A
	Choose File	KML file only	
Deny: These rules specify denied executables.	+ Add another		
Allow: These rules specify allowed	Name:	(Default Rule) All files located in the Program Files folder	Default Rule
executables.	Rule type:	Path	_
	Path:	%PROGRAMFILES%\*	
	Windows user:	Everyone	
	Exceptions:		
	Name:	(Default Rule) All files located in the Windows folder	Default Rule
	Rule type:	Path	-
	Dath:	«/////////////////////////////////////	

#### **Tanium Threat Response**

Hunt, detect, investigate, contain, and remediate threats and vulnerabilities with speed and scalability. Quickly piece together the story of what happened on a single endpoint and remediate endpoints across the enterprise in seconds.

Ξ			
0	Detect	<	Hone Alerts
Home			
Alerts			Status: @Unvescrived Billin Progress Billinescrived Odder By: 4 Alex Time •
By Ale	rt		Filter Results
Manage	ment		Showing: 49 of 49 airsts  Reset Filters O Bittor M
			** I SOWMARH kund geh 2017-12-08 kadet in Runnig Processes in Mar 14, 1039 AM     / File 0.108ex11kaki.an/kgr04ex1Masaang/07exila8ex1/yeev eee
			C * Aphibatises frond diph-0071-11:04 baskshift via Taritum Index on Mar 14, 15:00 AM     Fills 0: Utileas/Util_AbdisAluppEatAlisasLapforesLaberal.ysear.ess
			** Aphabeter hund diph-007-10-06 baskelf via Terum Index on Mar 14, 1000 AM     * Fille C: \UBershallbackstatested vigebets (MassalightStrateshalls);
			Yel COMMAND low dight 2017-12-04 backet in Nurring Processes in Mar 14, 1030 AM     Yellie C. \Ulterest \Laskinglichet klassinglichet kl
			** EDWMADFLund Quark Add 11/172017, 22:04 PM in Running Processes on Feb 24, 321 AM     Pails C: \Ulterarl\LaskimulgeData.\LaskimulgeData
			C *2 EDRWald Sund Quick Add 11/17/0017, 925-42 PM via Ruming Processes on Feb 24, 320 AM



### **Tanium Comply**

Check endpoints against standard security benchmarks to simplify security hygiene, compliance, and audit preparation.

🚱 Comply	< Home Confie	guration Com	pliance Reports			Refresh Statistics Create Report
Home		guration com				
Reports	Results 6					1F Last Run 👻 Pitter by title or hash C
Al	> Filter I	Results:				
Configuration Compliance	O Sele	ict All				Expand Al
Vulnerability			mpliance - Windows 1	0		
Report Exports		Compliant 38%	Average Failed	Averaga Passed	Endpoints 🙆 2	
		E Windows Serv Compliant 32%	er Compliance Average Failed 190 (68%)	Average Passed	Endpoints 💌	
			Compliance Report		l	
		Compliant 57%	Average Failed = 68 (43%)	Average Passed  S0 (57%)	Endpoints 🛞 5	
		il' Windows 10 C	ompliance Report			
		Compliant 28%	Average Failed 225 (74%)	Average Passed	Endpoints 🙆 2	
		If Windows Cust	tom Report - Minimal S	Settings Compliance		
		Compliant	Average Failed	Average Passed	Endpoints 🥘	

#### **Tanium Integrity Monitor**

Improve regulatory compliance by linking file integrity monitoring with active alert investigation, configuration compliance, and vulnerability scanning.

Integrity Monite	or		Manage Homepage
Required Integrity Monitor Set	tings: Three required steps still	need to be completed. Comple	te Now
Welcome			
98% Roughly 98% of Endpoints are recording from total Endpoints deployed. See all	changes are detect	egrity Monitor) to simplify regulatory comp e-wide by consolidating tools, while taking	liance and make file integrity
🛶 Set Up 🛛 🔪 🛶	Set Un Set	Up Der	Monitor
Set Up Watchlists           Set Up Watchlists           Seteut Watchlists from the left ne New Watchlist.	Set Up Monitors Set Rule		toy hitors Changes
Watchlists Set Up Watchlists Select Watchlists from the left na	Monitors Rule	ts page, click Create a	Set Up Watchlists
Set Up Watchlists Select Watchlists New Watchlist.	Monitors Rule	ts page, click <b>Create a</b>	H Set Up Watchliets
Watchlists     Set Up Watchlists     Select Watchlists from the left ne New Watchlist.     Sample Watchlist     Add predefined templates to your	Monitors Rule	Its page, click Create a	H Set Up Watchliets



#### **Tanium Reveal**

Reduce risks of data exposure, mitigate the impact of breaches, & meet regulatory compliance.

	G TAN	NIUM.
	Home > Rulese	ets
Ruleset Details		
	Revision: 4	Description: PCI standards help companies that accept, process, store, and transmit credit card information maintain a secure environment.
	Ruleset Re	
	Rules List	S - Cardholder Data for credit card numbers in Microsoft Word, Excel, and text documents.
	Rules List	Computer Groups Affected Endpoints 3 - Cardholder Data
	Rules List	Computer Groups Affected Endpoints  3 - Cardholder Data for credit card numbers in Microsoft Word, Excel, and text documents.
	Rules List	Computer Groups Affected Endpoints  3 - Cardholder Data for credit card numbers in Microsoft Word, Excel, and text documents.  Matching Endpoints: Rulesets:
	Rules List	Computer Groups Affected Endpoints  3 - Cardholder Data for credit card numbers in Microsoft Word, Excel, and text documents.  Matching Endpoints: 124  2 - System Passwords

# **F**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
- 灯 @Tanium
- info@tanium.com