



## Sample Tanium Use Cases

The Tanium systems management solution allows you to query for data and make changes across every machine in any sized network in seconds. This powerful, yet simple-to-use solution can lead to benefits across numerous systems management capabilities including asset and software license management, outage management, patch management, unmanaged asset tracking, and more. Take a look at a small subset of use cases that our clients are seeing today.

### Use Case Table of Contents

- [Inconsistent Environment Causing Application Outage](#)
- [Monitoring for Advanced Persistent Threat/Data Leakage](#)
- [Killing a New Worm or Blacklisted Application](#)
- [Unmanaged Asset Tracking](#)
- [Real-Time Property Collection](#)
- [Real-time Patch Requirements](#)
- [Windows Management Instrumentation \(WMI\) Diagnostics and Remediation](#)
- [Patching and SLA Requirements](#)

### Additional Resources

- [Tanium Web Demo](#) - Get a quick overview on what Tanium is and how it can help your enterprise.
- [Frequently Asked Questions \(FAQ's\)](#) - Read answers to the most common customer questions.
- [Tanium System Requirements](#) - See a list of the system requirements for the Tanium Server, Client, and Console.

## Inconsistent Environment Causing Application Outage

**Use Case:** A customer is experiencing an application outage on a client-server based application. The customer suspects that older versions of the client application have been reintroduced into the environment in the last hour and are causing the outage, perhaps because of build revisions or an old package in a deployment tool.

How can the customer instantly determine exactly which versions of the client application are in use currently in the environment?

**Solution:** In Tanium, assuming the customer is looking for an application named "AppX", they could simply type in a question like:

What are the versions of installed applications with names that contain AppX

Installed Applications	Count
AppX Player 11.5   11.5.7.609	143
AppX Player 11.6   11.6.0.626	114
AppX Player 11.6   11.6.1.629	32
AppX Player 11.5   11.5.9.620	27
AppX Player 11.5   11.5.8.612	19
AppX Player 11.5   11.5.9.615	13
AppX Player 11.5   11.5	10

Within 15 seconds, Tanium can return a list of the versions and counts of AppX that are in use in the environment. With existing systems in use today, the process to determine existing versions would take hours or days and would require advanced knowledge of the tool sets, rather than a simple question in English.

## Monitoring for Advanced Persistent Threat/Data Leakage

**Use Case:** A customer is concerned that they have a data leakage issue that stems from an advanced persistent threat (APT), but they are unaware which machines might be affected or even the APT's application name.

As such, they wish to know the names of every application that currently have an established network connection to a location outside of the corporate network.

**Solution:** In Tanium, assuming that they wanted to know those from only the machines in the "Development" Organizational Unit, the customer could ask question like:

What are the established connections by application on computers where the organizational unit is Development

Established Connections[True]	Count
OUTLOOK.EXE 176.16.10.45:1169	9
Term.exe 33.230.191.66:23	6
winlogon.exe 162.16.10.23:524	6
OUTLOOK.EXE 16.2.8.12:1026	5
OUTLOOK.EXE 13.2.8.12:2123	5
System 15.2.8.12:445	5
System 15.2.8.4:445	5

Within 15 seconds, a list of the applications, as well as the target IP addresses and ports that they are communicating with is presented. The commonly found applications are likely IE and other approved applications, but the bottom of the list are likely applications whose names are unknown to the administrators, and represent likely APT risks.

With existing systems, the best information available often comes from network monitoring tools which can tell you which ports are in use and perhaps what the contents of the traffic look like, but cannot accurately distinguish the client-side applications generating the traffic. As such, an HTTPS connection to an external location looks exactly the same, regardless of whether it is an APT sucking data out of the network or someone buying shoes from an online vendor. In contrast, from the application level, Internet Explorer is easily distinguishable from an unknown named application that the organization has not approved, allowing the organization to far more effectively identify dangerous traffic. Please see the next use case for how to kill those applications within seconds using Tanium.

## Killing a New Worm or Blacklisted Application

**Use Case:** A customer wishes to kill all instances of a disallowed application within 30 seconds across every machine in the environment that has it.

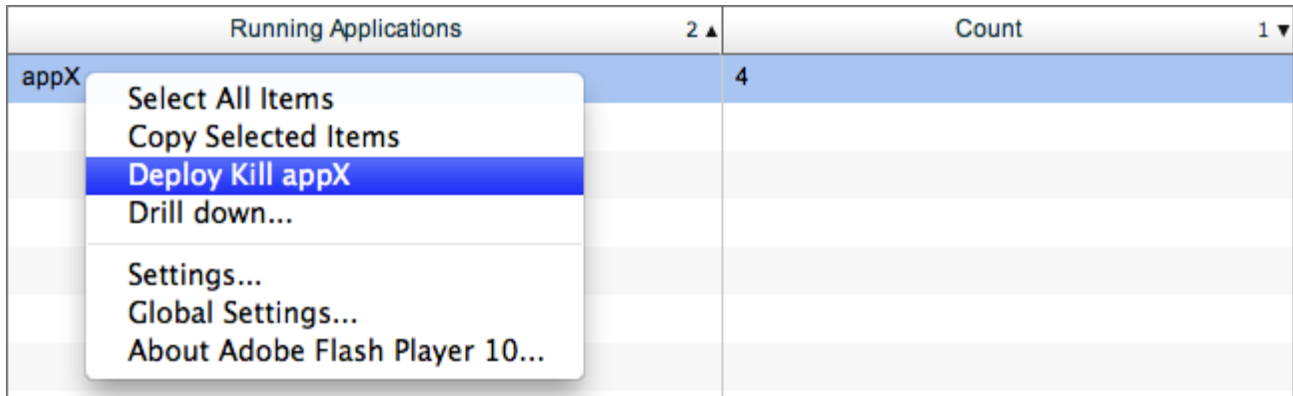
**Solution:** In Tanium, the customer would first define an action to kill AppX. Tanium packages are specified with exactly the same command as the customer would type into the command prompt if they were going to kill the application on a local machine. For example:

```
taskkill /F /IM AppX.exe
```

Then, the customer would ask a question like:

What are the computer names of computers running AppX

The customer can then fix all (or a subset of) the computers by simply clicking a button to target the action to those machines. Tanium can execute that action on any subset of machines, in networks up to 400,000 computers, in about 20 seconds and confirm success.



Running Applications	Count
appX	4

The customer can also use Tanium to monitor in real-time if the Blacklisted app ever returns and get notifications within 15 seconds if it does. Furthermore, the customer can create another action to remove AppX, update anti-virus (AV) software, or perform any other actions that may be required within seconds.

In existing systems, finding and fixing these assets would likely take hours or days at best, and would require substantial knowledge of those systems to accomplish.

## Unmanaged Asset Tracking

**Use Case:** A customer wishes to know every asset that is connected to the network which is not actively managed by the enterprise. It is often common for up to 15% of the assets in the environment to fall into this category and they represent the most dangerous security threats to the network, since they are often not properly patched, do not have AV, data loss prevention (DLP), or management agents, or do not have Active Directory Group Policy Object (GPO) policies enforced.

**Solution:** In Tanium, each Tanium agent can scan the area between it and the next Tanium agent every minute to determine if a new asset has been added to the network and is unmanaged by the corporate environment.

Unmanaged Assets	2 ▲	Count	1 ▼
100.17.100.167	1		▲
100.17.100.170	1		
100.17.100.171	1		
100.17.100.172	1		
100.17.100.176	1		
100.17.100.178	1		
100.17.100.179	1		▼

Traditional network scanners can often take hours or even days to traverse the network, and unable to scan through some firewalls, NAT devices, and routers. The Tanium agent scan is in the local subnet which bypasses these firewalls and network devices, and can therefore provide a more complete unmanaged asset picture. Tanium also scans each minute with no impact on the WAN, and minimal impact on the LAN. As a result, rather than learning about a new device days or even weeks after it was introduced (particularly if it is a laptop that transitions on and off the network), Tanium can find it within an average of 30 seconds of connection.

## Real-Time Property Collection

**Use Case:** A customer wishes to determine the values for a particular fast-changing registry key across all machines that are using the new Windows 7 Enterprise build.

**Solution:** In Tanium, the customer would ask a question like:

Registry Key Value from computers where operating system is Windows 7 Enterprise

Registry Search[TestKey,Software\Tanium\Tanium Client,HKLM]	Count
Value not found	137
4	121
1	94
3	3
0	1
512:17472:172.16.101.48_512:0:65.100.48.248	1

Tanium would then prompt the user to supply the value and key name, and would collect all values from those machines across the environment in 15 seconds. The user can then save that question to have it track the history of that registry key over time, monitoring changes with real-time accuracy across up to 400,000 assets.

In existing systems, collecting that registry key value would take hours or days at large scale and would require substantial knowledge of those systems. If the registry key is expected to change, administrators will never have a solid idea of the current state of the environment; instead, they're always days behind.

## Real-time Patch Requirements

**Use Case:** A customer is concerned that they are not able to confirm that patches were successfully applied during their maintenance windows - instead, information about success and failure is coming back hours later, often after the machines are outside of maintenance windows. The customer wants minute by minute status on the state of their assets for all patches that are required, or have been deployed.

**Solution:** In Tanium, the customer could simply ask:

What are the Required Microsoft Patches from all computers

Name	2 ▲	Sev 1 ▲	Bulletins	Date	Download	Coun
Microsoft SQL Server 2005 Express Edition Service Pack 4		None	None	2011-06	http://dowr	1
Microsoft SQL Server 2005 S				2011-06	http://dowr	1
Microsoft SQL Server 2008 F					http://dowr	1
Project 2003 Service Pack 3					http://www	1
Update for Windows XP (KB					http://dowr	7
Visual Studio 2005 Service P				2011-06	http://www	1
Windows Internet Explorer 9				2011-06	http://dowr	1

Tanium would return every patch that is required, as well as the patch's severity, date of release, and a variety of other information, for all machines currently in maintenance window. Since that data is 15 seconds old, the user can see exactly what is happening now, rather than hours ago. And since Tanium uses the Windows Search WSUS API to do the diagnosis of patch state, the information is 100% consistent with the Microsoft standard patch validation parameters.

In existing systems, the data would likely be days latent in most environments. By the time that the customer learned that a patch had failed, the maintenance window would be long closed.

## Windows Management Instrumentation (WMI) Diagnostics and Remediation

**Use Case:** A customer uses Microsoft SCCM and Tanium to manage its systems. However, WMI does not work on 10% of the machines in the network. Since SCCM is dependent on functional WMI, the customer is unable to reach these 10% of machines with SCCM.

**Solution:** Tanium can use a multitude of querying languages to accomplish tasks. Using a different language, the customer can use Tanium's WMI diagnostics questions and dashboards written in VB Script to discover any potential problems with WMI on every machine in the network:

[Get WMI Diagnostics from all machines](#)

WMI Diagnostics	1 ▲
(CheckWMIFeatures) : 0x80041002 - (WBEM_E_NOT_FOUND) Object cannot be found.	
The following WMI system file(s) is/are missing: 3 ERROR(S)!	
WMI GET operation errors reported: 30 ERROR(S)!	
WMI System file 'C:\WINDOWS\SYSTEM32\WBEMFRAMEDYN.DLL' is MISSING or is access DENIED.	
WMI System file 'C:\WINDOWS\SYSTEM32\WBEMPROVTHRD.DLL' is MISSING or is access DENIED.	
WMI System file 'C:\WINDOWS\SYSTEM32\WBEMWBEMCOMN.DLL' is MISSING or is access DENIED.	

In addition to identifying these WMI problems, the customer can use Tanium actions to run the appropriate WMI command line tools to reset, fix, or reconstitute the broken WMI repositories in question.

Tanium can also ask something like this to get which versions of WMI are in the environment:

[What are the operating systems and WMI versions from all computers](#)

Operating System	2 ▲	WMI Version	Count	1 ▼
XP Professional		5.1.2600.0	23	
Server 2003, Standard Edition		5.2.3790.3959	2	
7 Enterprise		6.1.7600.16385	1	
Server 2003, Enterprise Edition		5.2.3790.3959	1	
Server 2008 R2 Standard		6.1.7600.16385	1	

Tanium's out-of-the-box functionality can dramatically increase SCCM's stability and speed through fixing WMI and related errors on each endpoint. Tanium can also take the application usage and inventory information collection requirements out of SCCM's lap, which cuts the data that needs to move through SCCM by a large factor.


## Patching and SLA Requirements

**Use Case:** A customer has a critical outage on its enterprise servers caused by a faulty patch from a 3rd-party software vendor. To make matters worse, the customer has an SLA agreement with its own clients that requires they remediate all outages within 8 hours. How can the customer get out an updated patch to every enterprise server in the environment within the 8 hour window?

**Solution:** In many large environments, there is no way to install new software quickly. Instead, the IT department needs to wait until the appropriate software deployment window to push new software patches. Furthermore, it can be difficult or time consuming to identify which servers have the faulty patch and need the update.

Tanium can deploy files across hundreds of thousands of machines in a matter of seconds. First, to locate which servers need a particular patch, the customer can simply ask:

[Get ip addresses and installed applications containing AppX](#)



IP Address	Installed Applications
272.16.100.72	AppX  3.0.314.6807
272.16.100.74	AppX  3.0.314.6807
272.16.100.82	AppX  3.0.314.6814
272.16.100.89	AppX  3.0.314.6814
272.16.100.91	AppX  3.0.314.6807
272.16.100.92	AppX  3.0.314.6807
272.16.100.94	AppX  3.0.314.6807
272.16.100.97	AppX  3.0.314.6807
272.16.100.100	AppX  3.0.314.6807
272.16.100.101	AppX  3.0.314.6807

Select All Copy Export Deploy New AppX Patch 342 items

This identifies every machine in the environment and returns the IP address and AppX version within seconds. Now that these machines have been identified, the customer can create a Tanium Action called "New AppX Patch" to deploy the new patch.

Once the action has been created, the customer can very quickly deploy to any or all machines that require the patch. Again, this deployment will occur in a matter of seconds and would easily allow the customer to meet its client SLA requirements.