Tanium Endpoint Management – Cross platform lifecycle management from a single console

Value Proposition:

Tanium is fast and flexible, it's endpoint management for the modern enterprise. Achieve centralized and automated management of your systems in minutes — not weeks or months.

- Identify missing operating system patches and software updates and remediate them in minutes.
- Provision devices, whether local or remote in minutes instead of hours.
- Automate patching and software deployment without additional tools or infrastructure.

Ideal Customer Profile:

For Prospects/Customers who:

- Struggling with long patching times (over 30 days?)
- Recently experienced security incident involving unpatched vulnerability
- Looking to improve endpoint lifecycle management

NOT for Prospects/Customers who:

MDM support a must have criteria or those only looking for OT/IoT

Competitive Differentiators:

- Ability to provision Windows and Linux with 1 platform.
- Ability to provision off domain remote endpoints.
- Deploy patches and software efficiently without additional distribution servers.
- Built in package gallery of hundreds of common applications

Compelling Stats:

- Patch 350,000 Endpoints or more in a day.
- Provision a new endpoint in as little as 15 minutes anywhere.
- Managed or User Self Service Portal for installation of Patches, Software and OS upgrades.
- See and Remediate vulnerabilities at 99+% Efficacy with Tanium!
- Before Tanium, endpoints typically go unpatched for more than 150 Days!

Customer Benefits:

- Significant time and resource savings when imaging systems
- Quickly install software at scale saving days/weeks each month by using pre-packaged gallery of hundreds of common enterprise applications
- Reduce cyber risk and administrative time by keeping systems up to date with highly efficient and scalable patching solution that has a 99% success in first pass with confirmation.
- Save staff time and get operational efficiency by fully automating patching and software deployment.
- Robust reporting on state of entire environment (Windows, Mac, Linux) in a single pane of glass

Modules Included in this Solution:

- Patch
- Deploy
- Provision

TANIUM

Tanium SBOM – Find and Remediate Software Supply Chain Vulnerabilities

Discovery Questions:

- How long does it typically take for a patch to be implemented for a newly discovered vulnerability? Are you able to reach 99% patch efficacy?
- How long does it take to provision a new machine to where it is operational for the user? Are you able to provision machines remotely that are not connected to a domain and if so, does it require an additional tool? If a machine becomes corrupted, how long does it take to re-image that machine? (Does it require another tool?)
- Are your users able to self-select approved applications from a library to install on their machines? Do you use separate tools for managing software applications on Mac or Linux vs. Windows? Is IT able to automatically uninstall applications from endpoints? (For example, non-approved apps added by the user)
- How do you know if you've identified all the endpoints on your network that need to be patched? (Visibility is typically ~80% with other tools). Are you able to patch Windows, Linux and Mac from a single console?

Objection Handling:

Objection:

We already have tools to manage our endpoints (SCCM, InTune, BigFix, Avanti, etc)?

Answer:

We typically want to avoid a feature/function battle with another tool, however, when it comes to items like patching we are by far the best tool for patching and can achieve higher patching efficacy rates, higher first time patch success rates and a broader reach than any other patching tool. This may also be a situation where a prospect/customer is using multiple tools and could consolidate onto a single platform with Tanium. They may be using one tool to patch Mac, another for Windows and yet another for Linux. Uncovering the customers priorities and pain points are key to understanding whether the Endpoint Management solution can achieve positive ROI for the customer.

Objection:

Tanium doesn't manage iOS or Android devices

Answer:

This is true, we currently do not, however, how important is this to the customer? Are iOS and Android devices being used to accomplish business objectives or are they simply being carried by workers for convenience? For example, receiving an email about a document, the worker is not likely to edit the document which could result in malware embedded in the document via a macro. In short, our answer is that we have partners we integrate with (Microsoft InTune) that can manage these devices and that we are continuing to strengthen our partnerships to provide a holistic solution that works for our

Common Use Cases:

- Create new endpoints in accordance with internal policies via bare metal imaging along with the ability to refresh endpoint images anywhere at any time.
- Repurpose/Refresh endpoints by re-imaging to same or different OS.
- Establish an enterprise-wide, automated scheduled OS patch methodology for Windows, Mac, and Linux endpoints including a complete and up to date understanding of OS patching status across targeted machines to decrease risk and reduce the attack surface.
- Install, Update and Remove 3rd party applications across all managed endpoints (Windows, Linux, macOS) to reduce risk and harden endpoints.
- Enable end users to control aspects of 3rd party software management.

Key Competitors:

Microsoft (InTune/SCCM) also a Partner

VMware (Workspace ONE)

IBM/HCL (BigFix)

Symantec/Broadcom (Asset & Client Management Suites)

Cisco (Secure Endpoint)

Ivanti (Ivanti Endpoint Manager)

Citrix (Citrix Endpoint Management)

TANIUM