Tanium Tale:

Welcoming More Efficient Windows Upgrades and Patching

When a global $13b business protecting the most critical information assets of thousands of customers sought to take greater control over its Windows workstation environment for 13,000 employees, it turned to Tanium.

When Tanium sought to engage the best partner to enable its customer's long-term success with the platform, it tapped Chuco. We'll take a closer look at some of the highlights of that collaboration over the past year.

Slipping Through the Closing Window on Microsoft Windows 7

After standing up Tanium Server and key modules (Patch, Deploy, Discover and Asset), Chuco had rolled out clients across the organization's server (6,500 Windows and 3,500 Linux) and workstation infrastructure.

Chuco then turned to address one of this business's most critical challenges — efficiently upgrading upwards of 8,000 workstations from Windows 7 to Windows 10.

With support ended in early 2020, and Microsoft only offering limited security updates through a costly Extended Security Update (ESU) program, continued use of Windows 7 presented intolerable levels of risk and expense.

In addition to the cost of support and the security exposure presented by continued use of Windows 7, there was also considerable risk in managing the dependencies of specialized applications running on those systems, as those tools halted their own support for that retired operating system.

This dynamic created uncertainty, pain and inefficiency for the IT teams responsible for supporting an increasingly complex technical landscape, as well as the end users relying on critical applications running on out-of-date Windows 7.

However, updating thousands of machines to Windows 10 posed its own set of serious risks and potential costs. The project could not be undertaken lightly.

Many “Panes” Make for Greater Risk and More Pain

A massive upgrade process in this scenario is complex. Even basic steps like distributing operating system update files (e.g. ISO images) and managing the bandwidth to distribute them present significant challenges.

In this case, the organization had a global presence, including offices situated in remote locations with multiple machines served by tightly limited bandwidth.

That global footprint presented a number of cascading constraints. When configuring upgrades, managing languages, language packs and associated dependencies can be overwhelming.

Consider that locations have systems with the “expected” localized version of Windows for that geography. Now consider scenarios in which users further customize their own machines — or shared accounts on the same machines — with language packs that are not standard to that geography.

For example, one would expect Canadian users to expect an integrated option for French in Windows 10. And Microsoft does just this in its OS configuration. What’s less expected is a scenario in which an individual who prefers to work in French Windows is based geographically in China and installs a one-off language pack to parlez-vous français on their particular workstation. Or, making things even more interesting, on a workstation shared by several accounts and individuals.

This scenario represents just one “known unknown” in terms of system configuration details that have to be mapped, identified and accounted for in any upgrade plan.

Application and OS Complexity Compounds the Challenge

The same principle applies at the application layer. In this client’s environment, machines often supported mission-critical applications – such as scanning software vital to information management — that would not work on Windows 10 “as is.” Either those were out-of-support legacy tools themselves, or they would require additional upgrades to work on a more modern operating system. Again, this required another map of potential pitfalls to develop and plan for as part of an upgrade program.

Adding a further twist, one of the applications this client used on many machines was a third-party disk encryption solution.

The net implication for those systems would be that absent an automation solution, someone would have to physically enter decryption keys any time the system was rebooted. And reboots tend to be part of any Windows OS update activity…

All taken together, facing a plethora of problems to navigate, one can see why it would make sense to maintain a Windows 7 status quo as long as possible. If everything went right in the transition, without absolutely no surprises or disruptions, the net change in experience for end users would be the status quo (with a new UI to get used to).

But by engaging Chuco and taking advantage of our extensive experience executing complex Tanium projects, this organization was able to set sights on and reach a new vista swiftly and smoothly.

Updating Windows, Working in Waves, Learning Lessons, and Scaling

Given the complexity of this client's environment, Chuco took full advantage of the broad range of tools and capabilities Tanium provides, adding our own innovations and enhancements along the way.

Core to our success was establishing comprehensive visibility across workstations and their configurations, and working iteratively in waves to group and update those systems.

Tanium gave us the power to effectively use available bandwidth for ISO distribution, and to configure upgrades mapped to the OS-level language and add-on language pack requirements of each system.

The same held true for application-level updates that these system upgrades necessitated, though sometimes with some system-level manual intervention.

By grouping systems, we were able to check our work, resolve any issues, learn some technical lessons, and make some exciting discoveries along the way to accelerate our progress.

Depending on the nature of the systems and the updates at hand, Chuco would work with the client to update as many as 1,000 systems at a time.

Because of the significant shift from Windows 7 to Windows 10, we took care to communicate clearly with end users. That included multiple email notifications that included escalation paths for them to raise issues or ask questions. We also took advantage of Tanium's ability to present users with a system-level "pop-up" and ability to defer their scheduled upgrade for two days.

As we brought more systems live on Windows 10, we also worked with the client to push Windows 10 updates as well, as those became available (e.g. version 1909, version 2004, version 21H1). In many instances, these updates could be executed in a way that was completely transparent to end users.

As expected, this scale of project wasn't "push button" — but it was one we were able to plan and execute within the client's time and on budget constraints.

Results, ROI and Lessons Learned

- Expect Technical Challenges (and Expect to Overcome Them). In an exercise of this scope and scale, scenarios requiring a bit of troubleshooting are going to be a given. One interesting obstacle we encountered we the client's use of third-party full disk encryption (McAfee). Thankfully, we were able to configure our process to bypass that temporarily without requiring intervention from the user upon reboot. Similarly, navigating some system-level driver requirements posed the occasional challenge.

- Early and Continued Visibility Brings Victory. The best problems to solve are the ones that don't pop up as unexpected, time sensitive surprises. When executing a large scale patch and update initiative, it's critical to assess your environment to identify as many of these issues ahead of time.

  Thankfully, Tanium makes gaining this level of comprehensive visibility possible. The corollary here is "don't get cocky" — defining a reporting, remediation and response plan for dealing with the unexpected you encounter along the way — before your you push the first update — will serve you well. And help you sleep easier.

- It Pays to Connect with a Tanium Expert. Tanium provides a solid framework for updating default environments. But no enterprise environment is ever "default." That's why connecting with expert consultants, even in an advisory capacity, can deliver significant value.

  Not only will this help you avoid potential pitfalls as you develop an upgrade methodology specific to your organization and environment, it can also pay surprising dividends.

  For example, in this instance during the planning process we conducted a review of the Microsoft knowledge base, and discovered a game-changing detail in KB4023057. Turns out, Microsoft had bundled files and data for Windows 10 version 21H1 in an earlier update. By building a custom script to activate those already present but dormant files, we were able to bypass the need to push nearly 5 gigabytes of data to each system. Instead, we were able to activate that version update by delivering a customer 1 megabyte update.

  The time and bandwidth savings this discovery delivered were significant. It was a rare example of a true "push button" solution that proved our earlier rule that this never happens — and was cause for great celebration by both the client and the Chuco project team.

To Learn More

If you'd like to learn more about how we work to support organizations get the most from their Tanium investments, we'd love to connect. Through years of hands-on experience, working both at Tanium and now as independent consultants, the Chuco team has developed a deep understanding.

So whether you're just starting to work with Tanium, or looking to really push things to the next level, we have experience, insight, and hands ready to assist — be that offering some seasoned advice, working to help execute a specific project, or taking on a role as a virtual member of your internal Tanium team.