When a $30 billion dollar transportation company with 10,000 endpoints and hundreds of servers adopted Tanium, they realized that improving their patching capabilities, efficiency and overall compliance levels could have a significant impact on their ROI. Tanium introduced them to Chuco, and we got moving — fast.

Getting Ready to Go Fast

We started first by listening closely and then carefully charting our course. We always want to develop and validate a clear understanding of each client's specific goals and objectives.

Of course, everyone wants to achieve "successful outcomes." But "success" means different things to different people. Making assumptions and skipping validation Is like embarking on a critical journey without an accurate map — a sure way to encounter dead-ends, detours, and even disaster.

In this case, we identified the client's top priorities and concerns. These included a pressing need to address server patch management specifically, and a general vision to improve three key areas over time: compliance, "stakeholder sensitive" reporting, and custom notifications.

Determining a (Managed) Mode of Transport

When we plan with clients, we jointly explore not only the specific technical and process outcomes we're setting out to achieve, but also the engagement model best suited to deliver those results.

In this case, early client discussions made it clear that there was plenty to do in the short term, and a far-reaching runway of opportunity in the long term. That realization was important, as it shaped how the client chose to structure its relationship with Chuco.

Specifically, rather than hire us for a one-off project, our client saw the value in our managed services approach. We offer several options and the flexibility to engage at a level of sustained involvement suited to diverse needs and budget levels.

The advantage of a managed services approach is that Chuco engagement, availability, and activity is consistent and dependable:

- We can place hands on keyboard (or not) practically on demand
- We are regularly touching, tuning, and tending Tanium
- We can manage and allocate staffing, so familiar faces are facing the client

We develop a deeper understanding of the client's environment, preferences, and even culture — all of which enable more greater productivity and success

A managed model means we are consistently engaged, evaluating, adjusting, and extending Tanium for the organizations we serve. And in the case of our transportation client, this model really accelerated our pace and progress. Let's look at three key milestones on that journey.

Destination #1: Patch Plateau

Before Tanium entered the picture, our client had patch processes in place, but they weren't able to get them where they really needed to be.

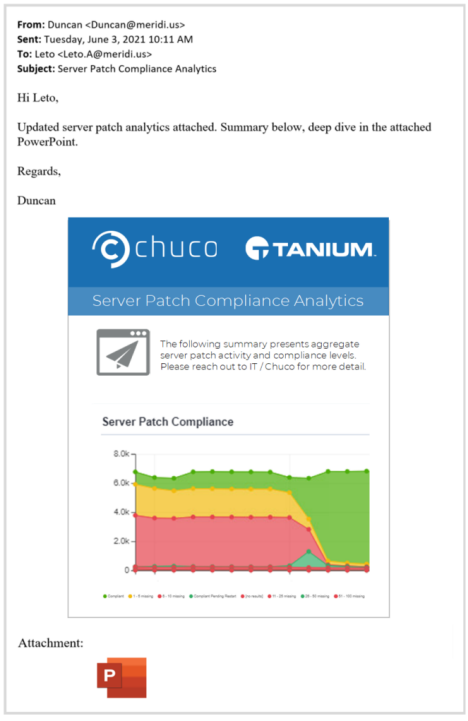
For one, relying on native Microsoft tools (System Center Configuration Manager / Endpoint Manager) left them unable to address an extensive Linux server landscape. Nearly 400 Red Hat Enterprise Linux servers were 100% non-compliant, most missing over 100 patches.

With Tanium offering unified command and control over patch management across environments, the trick and challenge is configuring updates to address an organization's specific needs and constraints.

In this case, we created a centralized server patch management regime for both Windows and Linux systems, navigating the limits of defined maintenance windows and other dependencies, working with application custodians on the client's IT team. Those constraints include updating dependent servers in the right order.

Consider a solution comprising multiple application servers, database servers and web servers: To keep production services up and avoid surprises during patch/reboot operations, it's prudent to patch in a deliberate order, incorporating QA validation along the way, rather than take all application servers offline at the same time.

Today, our client has achieved its compliance objectives; see Figure 1 for a snapshot of "before and after" server patch levels. And we continue to provide ongoing patch support as part of our managed services engagement — across its hybrid server environment and Microsoft workstations — to keep things on safely and consistently on track.



(Figure 1)

Destination #2: Reporting River

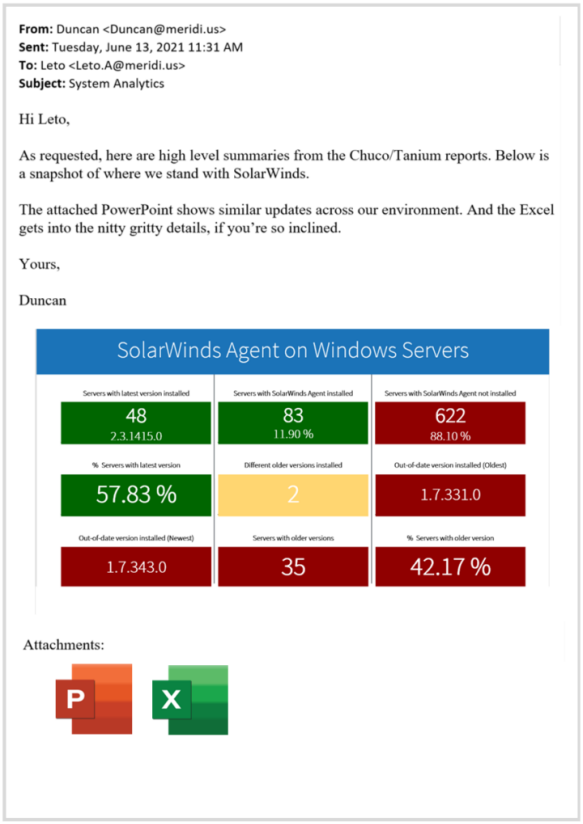
With compliance under closer control, the client wanted greater visibility. And while Tanium provides solid native reporting capabilities, using these requires building multiple queries using the Console, and performing a number of manual steps.

To meet this organization's more advanced needs, we developed a custom solution, taking advantage of Tanium API access, to build, run, and deliver tailor-made reports automatically. Most importantly, these are designed to provide the right levels of technical detail, rolled-up summaries, and delivery format best suited to three specific internal audiences:

- Senior Executives — who want a "bird's eye" view of key stats, delivered in a PowerPoint-level of abstraction
- Operational Directors — who want a more "Excel-like" view of system data, including the ability to manipulate and explore that data directly themselves
- Technical IT Custodians — who want machine-level, granular detail at the push of a button, without having to log into machines or the Tanium Console to build queries and screens or gather data

As highlighted in Figure 2, our solution offers just this — from executive-level slide summaries, to nitty-gritty details.

And as part of our managed services support, we are on deck to add, expand, and adapt these summaries as the client's needs evolve. The net result is they can focus their time on understanding, evaluating, and acting on the insight these reports provide — rather than on building, running and processing them.



(Figure 2)

Destination #3: Notification Oasis

With patching under control and reporting providing operational teams and management with faster and deeper insight into the state of their internal land-scape, the client's third wish was to get key technical updates and progress reports delivered to their inboxes.

To enable greater efficiency for operational teams, we developed a system that delivers both scheduled and event-driven updates via email.

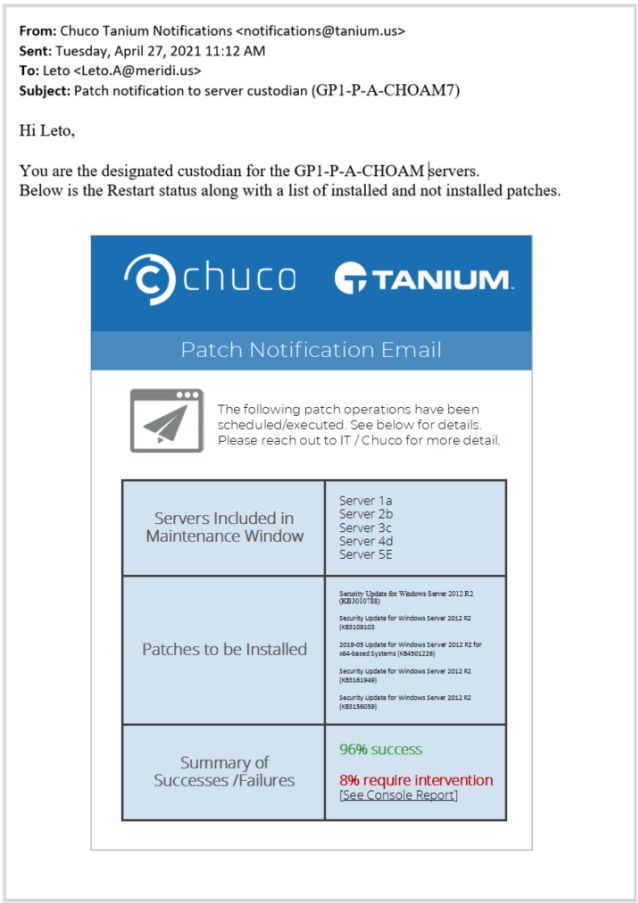
Our client wanted to address two key scenarios. The first is pre-patch notifications. These let server custodians know in advance that updates are coming. Think: "In two days, Server A is going to receive these 18 patches and Server B is getting these 23 patches."

For our client, this visibility increases awareness, and avoids internal surprises (like updates mistakenly scheduled outside of proper maintenance windows).

Similarly, this system also sends post-patching email summaries. See Figure 3.

These are important as they remind server and application owners to address any tasks they need to execute after servers and applications are updated, including validating system integrity and executing any manual changes specific patches may prompt.

With the average custodian managing 30-50 servers, these automated notifications have been a big hit.



From: Chuco Tanium Notifications <notifications@tanium.us>
Sent: Tuesday, April 27, 2021 11:12 AM
To: Leto <Leto.A@meridi.us>
Subject: Patch notification to server custodian (GP1-P-A-CHOAM7)

Hi Leto,

You are the designated custodian for the GP1-P-A-CHOAM servers.
Below is the Restart status along with a list of installed and not installed patches.

chuco TANIUM

Patch Notification Email

The following patch operations have been scheduled/executed. See below for details. Please reach out to IT / Chuco for more detail.

Servers Included in Maintenance Window	Server 1a Server 2b Server 3c Server 4d Server 5E
Patches to be Installed	Security Update for Windows Server 2012 R2 (KB3010788) Security Update for Windows Server 2012 R2 (KB3109103 2019-05 Update for Windows Server 2012 R2 for x64-based Systems (KB4501226) Security Update for Windows Server 2012 R2 (KB3161949) Security Update for Windows Server 2012 R2 (KB3156059)
Summary of Successes /Failures	96% success 8% require intervention [See Console Report]

(Figure 3)

The ROI, Lessons and the Larger Opportunity

The key takeaways here are three-fold:

- Tanium provides a powerful platform for centralizing patch management across diverse environments. But what the story above really highlights is the added value of increased visibility. Without a comprehensive and accurate picture of your patch landscape, you could be driving activity based on false assumptions, facing risks in the road you may not even be aware of. It's better to identify and resolve those issues on the horizon then encounter unexpected potholes — which Tanium can enable quite effectively.

- Expanding on Tanium's native reporting capabilities opens broad new landscapes of possibility. As illustrated by this example, adding new reporting and notifications can really help organizations effectively realize the potential Tanium offers to address the practice IT and management needs their organizations face.

- It pays to work with a seasoned guide and pathfinder that's integrated into your internal team and operations. In this instance, taking advantage of a managed services approach enabled our client to accelerate their journey, adjust direction when needed, and continue to build on their Tanium success.

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. The Chuco team has developed a deep understanding and stands ready to support your success with Tanium.