Tanium Tale:
Trading Tripwire Toll for Tanium Treasure

A healthcare provider serving over 12 million members nationally recently seized a tremendous opportunity to achieve significant cost savings, simplify its IT infrastructure, and reduce internal support costs by replacing Tripwire File Integrity Manager with the equivalent capabilities in Tanium Integrity Monitor.

Now, this organization already had seen great value from Tanium, which it uses to manage and configure over 500,000 endpoints. But it knew that migrating to a new file integrity solution posed some level of material risk.

Given the sensitive nature of the compliance requirements driving file integrity management in highly regulated industries, and the complexities of the existing software and configuration parameters in place, this was not a journey without potential challenges and traps.

I'd like to share the highlights of how Chuco quickly tackled those issues, set our client up for long-term success, and delivered significant budget savings in the process.

Understanding Scope and Defining Success

With a Tripwire license renewal deadline approaching, and an opportunity to dramatically reduce that expense with a swap out, this healthcare provider engaged Chuco in late 2020, based on a recommendation from Tanium.

The client had an aggressive deadline in mind, and we love a challenge — particularly when we can put our team's skills to effective use (in this case, literally in the fourth quarter, with the clock ticking).

While the organization had over 500,000 endpoints, there were 2,500 key systems subject to file integrity management requirements. And they wanted to bring over the specific and exact configuration of the monitoring rules, reports and other key parameters they already had in place.

In many respects, success looked like the status quo — but with a significant license cost slashed from their budget, and one less software system to administer and wrestle with.

Assessing a Complex Compliance Landscape

File integrity management plays a critical role in addressing regulatory, compliance and security requirements.

On relevant systems, monitoring rules define folders and files where operations need to be actively logged (e.g. create, delete, write, rename, change permissions). And reporting rules communicate summaries and alerts to key stakeholders on an event-based or scheduled basis.

So if the signature of a file changes, particularly outside of a normal upgrade window, someone can actively intervene and execute any security review procedures.

And in Tripwire, those systems are categorized in a massive tree structure where servers are tagged with relevant criteria labels. Those labels determine the specific rules and reports that may be applicable to any given server. It's a many-to-many relationship — there are a lot of leaves in this forest and none can be left out

Chuco Automates Endpoint Configurations (Without Any Changes)

To smoothly execute this migration, Chuco developed a set of custom tools to analyze existing Tripwire data and provide the automation necessary for a quick, error-free, and exact import into Tanium.

Our toolkit addressed several critical stages of the journey. But, fundamentally, we built a solution for parsing the enormous Tripwire dataset describing the system node structure: all the endpoints, configuration details and descriptive tags, and then re-creating the Tanium compatible equivalent data structure for import into Tanium Integrity Monitor.

By taking the time to solve the hard technical problem, we made the actual migration look easy. Put otherwise, we had collectively agreed that a manual process to do the extract, reconfiguration and loading into Tanium would have taken 4-6 months.

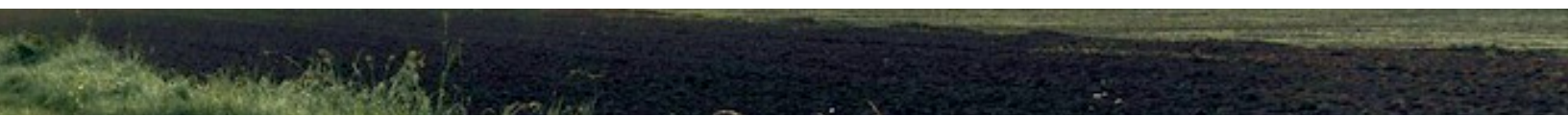
Our approach — which resulted in the creation of 200 system groups and configurations for all 2,500 endpoints, including different 1000 custom tags — took about 15 minutes.

And what's more, by avoiding a manual process, we eliminated the risk of human error.

The ROI, Lessons and the Larger Opportunity

Here are some key takeaways to consider:

- There is significant, hard ROI to be had from swapping out Tripwire for Tanium. And the savings can be tremendous — with a switch to Tanium, organizations can cut their license fees by 66% compared to Tripwire.



- Beyond the budget, there is softer return worth considering as well. One fewer system to manage means a simplified IT architecture, one less tool to manage, update, reconfigure and train staff to effectively use.

  Put otherwise — taking greater advantage of Tanium makes both economic and operational sense.

- This is a repeatable journey and Chuco can help you achieve similar success.

  Having navigated this journey swiftly and successfully with a client, Chuco now stands ready to apply the knowledge and tools we've developed to other organizations looking to achieve similar results.

  (We expect that systems and objectives will vary. So we're not promising a pushbutton, fifteen minute migration without laying some necessary groundwork. But we are confident in our ability to execute, and ready to work with all comers.)

Finally, a Tripwire-to-Tanium swap out is yet another great case for Tanium — either adding Integrity Monitor to your existing solution configuration, or justifying an initial Tanium investment in the first place.

And it's another great way for IT, security and compliance teams to deliver a budget win for the business, while also making their own operational lives easier.

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.