CASE STUDY

TANIUM

How Honeywell improves endpoint patching and consolidates tools with Tanium

Honeywell

Industry
Manufacturing

Size
103k employees

Headquarters
Charlotte, NC, USA

Tanium products
Discover, Asset, Patch, Deploy, Comply

Results

Compliant patching
With Tanium, Honeywell has surpassed 90% patch compliance for three months in a row, a service level the company was previously unable to meet.

Consolidating tools
Using Tanium has allowed Honeywell to consolidate and, in some cases, eliminate other patching tools, saving both money and time.

Better reporting – both up and down
By providing Honeywell with a "single pane of glass," Tanium provides accurate reports on patch compliance, both the overall figures needed by senior executives and more detailed results that servicelevelmanagers can use to improve compliance in the future.

Using Tanium's 'single pane of glass,' the company improved endpoint security while also eliminating costly software tools.

The more software tools, the better? Not necessarily. There's such a thing as having too many tools.

That was the situation at Honeywell International. The 138-year-old industrial supplier, with nearly 100,000 employees in over 80 countries, is supported by some 15,000 server endpoints. And keeping those servers up to date with the latest security patches is absolutely vital.

"Whenever we're unable to meet our patching-compliance benchmarks, that opens an avenue for bad actors," says Manish Chopra, a Honeywell IT director who joined the company in 2007.

Those compliance benchmarks are Chopra's main measures of success. If his staff hits the marks, all is well. But they were falling short of the benchmarks, in part because they lacked full visibility into those thousands of endpoints. After all, you can't secure an endpoint you can't see.

What's more, Chopra's team had accumulated a glut of management tools, many of which couldn't share important data with others. That also limited reporting. Chopra wanted to report Honeywell's endpoint-patching compliance numbers to the company's various operational teams.

> “We’re letting go of some solutions because Tanium can perform the work for us – and do it very well.”

Manish Chopra
IT Director, Honeywell

But these reports required data from at least four or five sources. “This was extremely challenging for us,” Chopra recalls. “It became difficult to know how well we were doing.”

Better patching

To improve the security situation, Chopra and his staff asked Tanium for a proof-of-concept (PoC) solution. One of Chopra’s superiors had used Tanium in a previous job and was excited at the prospect of using it again. “He was super-excited,” Chopra remembers. “He told me not to worry about the Tanium solution at all.”

Indeed, Tanium completed the PoC quickly, and the results were positive. Now Honeywell uses Tanium exclusively as its patch-management solution. The company also uses Tanium to enrich data in its configuration management database (CMDB), essentially a central store for information about its hardware and software assets. And Honeywell uses Tanium to create connections among systems running Splunk, a software platform it uses to search, analyze and visualize data gathered from the company’s IT infrastructure.

To further support Honeywell’s security, Chopra and his colleagues are using Tanium to build what they call patching portals. These will empower Honeywell end users to schedule patching for their systems. This self-service option will let users both select a time for their endpoint to be patched and choose whether they want the device rebooted after patching.

“Tanium gives us a single pane of glass,” Chopra says. “That makes it a lot easier to bring together data from four or five sources, and then report back to the particular service owner their compliance numbers.”

Saving time & money

Honeywell is saving money with Tanium by consolidating and, in some cases, eliminating its patching and visualization tools. “We’re letting go of some solutions because Tanium can perform the work for us – and do it very well,” Chopra says.

That saves not only the cost of licensing those additional tools, but also the time needed to monitor, update and upgrade them. Chopra says it’s also helping Honeywell create a Center of Excellence model, a community where staff can share security best practices.

Another improvement has been an end to disagreements over compliance numbers. Prior to using Tanium, Honeywell’s security and IT operations

teams each used different metrics, and disparities between them were fairly common. Now, with Tanium providing a single source of truth, those disagreements have become a thing of the past.

"Now we're able to bring the real numbers to our executive leaders," Chopra says. "Plus, we can drill down and show patch-compliance numbers to the service owners who, after all, are responsible for making sure their endpoints are fully patched."

Those results have been both remarkable and quantifiable. "Prior to using Tanium, our patch compliance was low," Chopra says. "Now, with Tanium, we've crossed the 90% patch-compliance mark for three months in a row. That's significant."

> "Prior to using Tanium, our patch compliance was low. Now, with Tanium, we've crossed the 90% patch-compliance mark for three months in a row. That's significant."

Manish Chopra
IT Director, Honeywell

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.