CASE STUDY

Whirlpool Corporation takes Tanium out for a spin

Tanium use cases

- Cyber Hygiene
- Incident Response
- IT Operations Management

Challenges

- Limited ability to discover and act on IT challenges
- Reliance on local IT staff to administer updates
- Not fully leveraging current security software investments
- Long delays to update patches and inability to ensure all patches were completed

Benefits to IT

- Improved response time to 83% and up to 99% faster
- Increased patching success rate and faster time to patch systems
- Overall increased ability to discover and act on IT challenges within one platform
- Ensure full-disk encryption is deployed and working on 100% of systems
- Better leverage of existing IT security investments

Global manufacturing businesses have good reason to have cybersecurity on their mind: industrial espionage, connected production lines, and thousands upon thousands of hard-to-find endpoints. Whirlpool understands the massive challenge of securing their business. As the number one selling major appliance manufacturer in the world, Whirlpool Corporation employs almost 100,000 people and has 70 manufacturing and technology research centers around the globe – not the easiest environment to keep an eye on.

Like many multinational businesses, Whirlpool used a variety of different security tools in a lot of different places. In 2015, the team turned to Tanium to help them find a single source of truth for their environment. “Lots of tools let you report on problems or manage problems, but Tanium gave us the ability to both discover and act,” said Greg Fisbeck, Senior Manager of Cyber Security Operations at Whirlpool Corporation. “That was key.”

Integration, integration, integration

What was important for Greg and his team was not a product that worked well on Windows, or Mac, or Linux, but a product that worked well on everything from desktops to servers – something they found difficult before Tanium. “We were genuinely surprised at the level of integration,” Greg recalled. “Being able to take data out of Tanium and put it into Splunk or take data from Palo Alto Networks and put it into Tanium – basically take all the tools I had and make them work together. That is where the value of Tanium is for me.”

Tanium integrations, such as with Palo Alto Networks Wildfire, allow Whirlpool to export data from Wildfire. Once Wildfire detects malware, Greg’s team forwards that alert to Tanium. Tanium Threat Response leverages the data to understand if the malware exists anywhere else on the network. The team then uses Tanium to remdiate the incident, initiating quarantine rules instantly.

Visibility and speed

With their industry leading appliance designs, intellectual property protection is of critical importance and full disk encryption controls is a requirement at Whirlpool. At Whirlpool Corporation, computers are required to have full disk encryption enabled. Scans from Tanium help ensure 100 percent compliance with Whirlpool Corporation's encryption policy. Tanium was able to provide real-time visibility into a problem that Greg and his team didn't even know existed.

In addition, Tanium's patented decentralized approach to endpoint management enables real-time control and access to data at unparallel speed and scale. "I expected it to be fast, but it's still amazing to go and ask how many copies of a program are on machines and be told the answer in a matter of seconds." said Greg.

All of this ultimately saves Greg and his busy team precious time, enabling them to handle more cases, more efficiently.

Cyber hygiene

One area that a company is never satisfied with is their cyber hygiene efforts. In the days before Tanium, security teams would manually pull a report from their antivirus tools, and send out emails asking people to update their systems. If the emails from Greg's team went unanswered, the next step was to reach out to the local IT team to track the person down – but this only worked if the person was in the same office as the IT team. Previously, Greg could push updates through their AV vendor console, but the results were unreliable. With Tanium, Whirlpool can ensure updates are completed quickly. Now Greg can automate the scan and remediation response across multiple security products without switching consoles.

"Tanium allows me to automatically remediate the machine," says Greg. "I just have to send a communication to the end user if my automated action fails. Before Tanium we were always behind the curve with virus definitions. We were always playing catch up. It wasn't unusual for 5–10 percent of our devices to be out of compliance with our policy. Once we deployed Tanium, our average went down to less than one percent almost overnight."

Greg's team has slashed incident response times since installing Tanium, improving the best case average discovery period by 83 percent and response time by 99 percent. This doesn't just save Greg's team time, it also saves time for the local teams in China, Brazil, and Germany, proving Tanium's value across the organization beyond the reduced risk of IP loss.

What's next?

According to Greg, Tanium provides Whirlpool "a world of possibility." So, what do they do next?

"Today we're using Tanium primarily for hygiene, but where I would love to go with it is proactive threat hunting," he said. "I have yet to bring a scenario to my Technical Account Managers that they couldn't find a way to accomplish with Tanium."

"Every time I've said: 'Hey could we look for…' or 'Hey can we do…' Anything I've brought to them and said could we do this with Tanium, there's a way to do it. That flexibility and ability to do virtually anything we need it to do is pretty powerful."