CASE STUDY

TANIUM

International Justice Mission secures remote field devices with Tanium

The nonprofit organization, an organization that protects people in poverty from violence by transforming justice systems keeps its laptops and data safe and secure with Tanium's remote management.

ORGANIZATION

International Justice Mission

LOCATION

Washington, D.C.

In some of the world's most impoverished communities, providing social-justice services is a tough but important job. So is protecting and securing the laptops and other endpoint devices used to provide those services.

That's the double challenge taken up by the International Justice Mission. This Christian faith-based nonprofit organization works to protect impoverished people from violence. IJM does this work with the help of nongovernmental organizations, local governments, and community partners in 26 countries, including Cambodia, Ghana, India, and Myanmar.

Specific IJM campaigns fight forced labor slavery, sex trafficking, violence against women and children, online sexual exploitation of children, police abuse of power, and land theft. IJM says that since its founding in 1997, the organization has protected some 10.8 million vulnerable people worldwide.

Also vulnerable at times are the laptops used by IJM's field workers to record and save interviews, notes, and photographs. Laptops have been stolen, in one case with data needed for a legal trial set to begin in less than a week.

"Our field workers rely on their devices to communicate, collaborate, and share data with external partners," says IJM cybersecurity analyst James Thompson. "While they're great investigators and great counselors, many are not the most tech-savvy."

‘Don’t Worry’

Thompson first became aware of Tanium about three years ago. This was during the height of the Covid- 19 pandemic, when most of IJM’s office staff had been told to work from home. From a security perspective, this created a new issue. With few of the working-from-home employees connected to a VPN, how could IJM ensure that their Windows PCs were fully updated and patched?

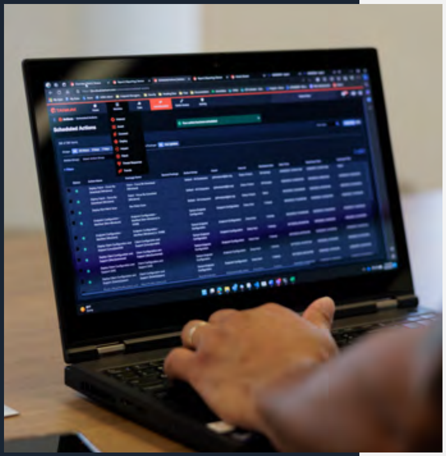
“We have a solution for that,” Thompson announced. “Don’t worry about it, we’re covered.”

That solution was Tanium, which Thompson had been evaluating. “I was immediately blown away by how expansive and capable the tool was,” he says.

CIO Barry Bonso-Bruce was similarly impressed, in part due to his background in IT infrastructure and desktop management. “We realized Tanium would make us able to manage our endpoints globally, push out updates, and roll out application packages,” he says. “It’s so much easier to manage and maintain.”

One big selling point was Tanium’s ability to handle plain English queries. Not having to learn a new programming language, Thompson says, was “amazing.” In a few hours, he had a working model for testing, piloting, and deployment. “It made me look like a magician,” Thompson says. “Mostly because Tanium’s engineers had already done all the work for me.”

> **“I didn’t think Tanium could get better, but every time I log in, I’m blown away.”**
>
> **James Thompson**
> Cybersecurity analyst, International Justice Mission



Remote Protection

One big issue for IJM is securing endpoint devices used in the field. When Thompson joined the organization, he discovered that none of the field laptops had disk encryption. This layer of protection is needed because, in the poor regions IJM works in, laptops can get stolen. Now, using Tanium, he has reversed the situation with an estimated 95% of field laptops now encrypting their data. "I know that figure because of the visibility Tanium gives us," Thompson says.

A recent incident put this approach to the test. An IJM worker's laptop, which contained data that was to be used as evidence in a legal trial, was stolen just days before the trial began. Using Tanium, Thompson was able to remotely lock the stolen device, download the needed files, and then email those files to the field worker. "We did add notes for the chain of custody," Thompson says. "That way, even though the data had gone through several channels before reaching law enforcement, we could prove it was still protected."

Tanium also helps IJM keep the software on those field laptops patched and updated, and to do this remotely. "Some of our users are in areas where it's hard to get to the office," Thompson explains. "So, it's just a matter of getting them connected to the internet. To them, it's magic; for me, it's just routine work."

Thompson can even use Tanium to support devices IJM doesn't directly manage. "I don't touch their data, but I can make sure their Zoom is updated, their Office is updated, that they can get information on and off the device," he says. "And if something happens, I can troubleshoot from my end. Because Tanium doesn't have to be part of our domain. It just needs to be installed."

Looking ahead, IJM has committed itself to rescuing millions and protecting half a billion people by 2030. Part of that effort, says CIO Bonso-Bruce, will involve Tanium. "It's great to have a product that provides us with certainty," he says. "That way, we can focus on our mission." Adds Thompson: "I didn't think Tanium could get better, but every time I log in, I'm blown away."

Results

Fully encrypted

Prior to using Tanium, IJM knew that many of its devices in the field were unencrypted and unprotected. It just didn't know which ones. With Tanium, 95% of all endpoint devices are fully encrypted and protected.

Updated and patched

Using Tanium, IJM can remotely ensure that important software used on its field laptops is up-to-date and fully patched. This capability is important because some IJM field staff work from locations far from a central office.

Unmanaged devices, too

Tanium allows IJM to support devices in the field that the central security team doesn't manage. That lets IJM make sure their Zoom software is up to date and ensures that their devices are running the most recent version of Microsoft Office. They can also get data on and off any device. If a device has a problem, IJM can use Tanium to troubleshoot and fix the issue. "Tanium just needs to be installed," says IJM cybersecurity analyst James Thompson. "It's the greatest thing."

Stolen data restored

After a field laptop containing important legal data was stolen, IJM used Tanium to freeze the device, download the important files, and then email them to the field worker — all in time for an important legal trial.

> "Tanium provides a level of automation and ease-of-use that allows us to update things on the fly — and also get reporting and information on what's actually installed on our endpoints."

Barry Bonso-Bruce
CIO, International Justice Mission

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.