CASE STUDY

TANIUM

How BIMA went from zero endpoint visibility to full control with Tanium

BIMA

Industry
Healthcare

Size
1000—5000 employees

Headquarters
Holborn, London

Tanium products
Discover, Asset, Patch, Deploy, Comply

The results of BIMA collaborating with Tanium.

- BIMA discovered more than 85,000 critical vulnerabilities. And then eliminated more than 90% of them in just seven weeks.
- BIMA has gained complete visibility into more than 2,500 endpoint devices, and the ability to easily keep all operating systems and applications up-to-date and running smoothly.
- BIMA now has quick, efficient, and up-to-date patching, dramatically reducing the company's cyber risk.
- Compliance has been dramatically improved, thanks to the new ability to push security rules to individual devices.

The leading digital healthcare solutions provider in emerging markets across Asia and Africa had a serious problem: no visibility into its 2,500 laptops in 12 countries.

How BIMA used Tanium to turn that around.

Not having visibility into your endpoints can be downright scary. What software is running, and is it up to date? Is everything patched? Are there any open vulnerabilities? Any IT manager who lacks the visibility needed to answer such basic questions is also risking a lot of sleepless nights.

That was the situation at BIMA, which provides digital healthcare and insurance solutions to consumers in emerging markets. BIMA's offerings include all-in-one health solutions comprising telemedicine, medicines, laboratory testing, hospital cash back and insurance, all delivered affordably.

Business is brisk. Founded in 2010, BIMA today has a userbase of 30 million customers, mainly in Asia and Africa. Looking ahead, BIMA has set a goal of 100 million users by 2026.

The fly in the ointment? Zero visibility into its endpoints, mainly laptops used by BIMA's 3,000-plus remote employees across 12 countries. How many IT assets did the company actually have? Did any of them need to be updated, or maybe even replaced? How many were properly patched? How many were running Linux, how many Windows, and how many MacOS? Which applications were being run, and were they up to date, too? Without visibility into its endpoints, BIMA simply didn't know. Worse, it had no way of finding out.

New job, new visibility

To solve this and other related issues, BIMA created a new position — Global head of technology operations — with Mitch Islin taking on the role in the summer of 2021. His mission was to gain control over all of BIMA's systems, and do it in time for the company's

“With Tanium, we’ve gone from riding a bicycle with one wheel missing to racing in a Ferrari.”

Global head of technology operations, BIMA

“Tanium on the cloud is easier for us, and less hassle. Tanium spins it up for us, and then we can access it from anywhere. That saves us time and money and adds flexibility.”

Mitch Islin,
Global head of technology operations,
BIMA

next audit and risk committee (ARC) meeting. Islin had only three months to deliver.

The search began for a device-management solution. One of BIMA’s consultants (Ricoh) suggested Tanium, and Islin immediately liked what he saw. Next, BIMA went through a proof-of-concept (PoC) test, deploying it to 20 machines for a week before fully deploying it to BIMA’s full base of 2,500 machines. With the hard deadline approaching fast, Islin didn’t have time for anything less.

The BIMA team opted for Tanium’s cloud-based option since their company believes in a cloud-first approach. The company has different operating environments – a mix of shared and owned office spaces with limited IT infrastructure of its own.

“Tanium on the cloud is easier for us, and less hassle,” Islin says. “Tanium spins it up for us, and then we can access it from anywhere. That saves us time and money and adds flexibility.”

In case you’re wondering, Islin met his deadline of gaining control of BIMA’s systems before the ARC meeting. What’s more, Islin says, the ARC team was “blown away” by Tanium’s capabilities.

The good, the bad, the ugly

BIMA’s results from the Tanium PoC were eye-opening for Islin and his team. It revealed that BIMA had more than 85,000 critical or high vulnerabilities, putting the company at serious risk.

“We knew it was going to be bad,” Islin says. “But we didn’t know it would be to this extent.”

Over the next six to seven weeks, Islin and his team used Tanium to eliminate more than 75,000 of those vulnerabilities, shrinking the total list by more than 90%. The remainder will soon be history, too.

“Nothing else could have done that,” Islin says. “The more we use Tanium, the more impressed we are.”

What’s more, with Tanium, Islin and his team now have visibility into every machine, every patch and all software. And if a PC is running slowly, the team can do a deep dive to figure out why. In one case, they discovered that a slow-running laptop in Ghana was being surreptitiously used to mine cryptocurrency.

Tanium also showed Islin that about 200 of the company’s Windows laptops — nearly 10% of all — were at end-of-life. Rather than replace all 200, a costly prospect, BIMA plans to migrate them to the open-source Ubuntu Linux OS.

At a high level, Tanium gives the BIMA team complete control over all endpoints, tons of details, the ability to patch quickly and effectively, and device-level enforcement of security rules.

For our security team,” Islin says, “Tanium has been a real game changer.”