How GenesisCare secured 16,000 endpoints on three continents

Healthcare leader turns to Tanium to address its growing array of networked devices while unifying its security and IT operations on a single endpoint management platform.

Industry Healthcare	Revenues $3.5 billion
Headquarters Alexandria, Au	Endpoints 16,000
Employees 5,000	Tanium products Tanium Cloud

GenesisCare, the largest cancer and cardiac healthcare provider in Australia, Europe, and the United States, recognized the need to invest in a security platform that could help properly safeguard its devices and the data they contained.

The company's Head of IT Security Mike Kleviansky found a platform that could deliver the necessary visibility and control, but it came right before the company acquired 21st Century Oncology in the U.S., which overnight added another 400+ clinics to its organization.

It was a major acquisition, expanding GenesisCare's reach across the globe. The endpoints Kleviansky's team had to cover jumped from 6,000 to 16,000.

Fortunately, Kleviansky found the Tanium Platform, which easily supports the scale his team needed to manage GenesisCare's rapidly growing business risk and digital footprint.

At the Tanium Converge Conference in November 2020, Kleviansky explained why the Tanium Platform was the ideal solution to support GenesisCare's growing data security requirements.

Finding quality care for endpoints

In 2020, GenesisCare's Kleviansky set out to boost the organization's NIST Cybersecurity Framework score. Developed for the U.S. government to reduce risks to critical infrastructure, the NIST Cybersecurity Framework represents a kind of gold standard for cybersecurity best practices.

But Kleviansky recognized he didn't have the tools he and his team needed to comply with the NIST standard.

Step one for NIST compliance is understanding what IT assets an organization has, and where. Back in 2018, GenesisCare had realized asset identification was a missing piece of its NIST compliance puzzle, but none of the tools the company had were up to the job.

"We were dealing with islands of information," Kleviansky says.

In other words, the information was out there in the organization, but not in one place. Instead, it remained siloed in individual point tools.

GenesisCare had up to two dozen separate security tools deployed across the IT stack, and wrangling them all to extract and combine the necessary data was daunting, if not impossible. It would have required an awkward kludge and would have been challenging to set up and difficult to maintain.

❝

I think any fast-growing global organization is looking for cloud options. It's a no-brainer. If you move your operations into the cloud and get somebody else to manage that, you can then focus on the business.

Mike Kleviansky
Head of IT Security, GenesisCare

"Whatever we came up with would certainly not have been an integrated solution," Kleviansky says.

Kleviansky's task was also complicated by a continually evolving endpoint landscape across multiple regions and scores of locations. And it wasn't just visibility the team needed.

"The main motivation was certainly identifying assets," Kleviansky says. "But we had other requirements, too. Vulnerability management was another."

Starting small with a proof of concept

As Kleviansky explains, he was able to select the right platform because he knew where he wanted to go and what capabilities the organization needed to achieve its goals. That's why he advises others undertaking similar journeys to make a roadmap.

"My initial thinking was that we needed a security tool," he says. "But we realized we required more than a security tool. A lot of our use cases are operational efficiency."

With this guidance in mind, Kleviansky sought out help, and he found Tanium. Once he saw how Tanium equally supports security and IT operations, his decision "was a no-brainer."

As soon as he realized what Tanium could provide, Kleviansky and his team set up a POC. Starting small was key for success, he says. But Tanium's ability to scale up from there was also critical. "I didn't want to re-architect my very complex environment," Kleviansky says.

Instead, he was looking for a platform that would work with GenesisCare's rapidly evolving digital infrastructure, now and in the future.

Kleviansky and his team made the POC as simple as possible. The team started with a virtual backend server. They then deployed Tanium agents to manage those cloud endpoints. From there, it was an easy matter to extend the Tanium Platform to more devices from a central console, achieving the scale the organization ultimately needed.

"The POC went very, very smoothly," Kleviansky says, crediting his Tanium account team with keeping them on track.

Scaling up and improving performance with software-as-a-service

Only a few weeks after the initial POC, GenesisCare acquired U.S.-based 21st Century Oncology, adding many more locations and endpoints to the stack — a potential stumbling block to the deployment already underway.

However, Kleviansky and his team were prepared. They had known additional acquisitions were in the cards. In just the three years Kleviansky had been there, the company had doubled in size, which was why he had scalability as a key requirement for a new endpoint management platform.

Getting the necessary scale as quickly as possible meant going with Tanium Cloud, the company's new zero-infrastructure, cloud offering. Besides the ease of building out the service across its global network, Tanium Cloud supported GenesisCare's goal to move much of its IT infrastructure to the cloud.

"I think any fast-growing global organization is looking for cloud options," Kleviansky explains. "It's a no-brainer. If you move your operations into the cloud and get somebody else to manage that, you can then focus on the business."

Tanium Cloud also proved a good fit for addressing the intense regulatory demands faced by healthcare providers like GenesisCare. The Tanium Platform's compliance capabilities helped the company meet regulatory requirements in the U.S., Europe, and Australia equally well, further easing the strain on the GenesisCare team. Finally, Tanium Cloud provided additional, unexpected benefits.

"My initial concern was performance," Kleviansky says. "If anything — which is absolutely phenomenal — the performance is actually better in the cloud than it was on-premises."

That was all the more remarkable to Kleviansky considering that Tanium Cloud is hosted in the U.S. and GenesisCare's servers and much of its operations are in Australia.

Looking to the future of endpoint management and security

Kleviansky says the support and partnership from Tanium has been a big factor in the success of the project. "One thing I found is that Tanium is incredibly responsive," he adds. Case in point, medical devices.

"One of our challenges as an organization is getting visibility [into] our medical devices across the network because they are hidden behind important firewalls," Kleviansky explains. Those firewalls, in place to protect lives as well as devices, had to remain.

To find ways to address this issue, Kleviansky asked for meetings with senior managers at both Tanium and the manufacturers of GenesisCare's medical devices.

"These talks could be groundbreaking," he says Groundbreaking not just for GenesisCare but also for Tanium and the medical device manufacturers, who could end up with new ways to secure a large class of vital devices.

In conclusion, Kleviansky advises other companies seeking greater visibility into their endpoints to see beyond the primary tasks of asset protection.

"Don't only look at it through security eyes," he says. "I can tell you our operational guys are probably more excited than I am, which is saying a lot."