CUSTOMER SPOTLIGHT

How VITAS Healthcare's Endpoint Management System Paid for Itself in Six Months

Largest hospice care provider in U.S. turns to Tanium to dramatically streamline software updating and patching processes while uniting IT and security

VITAS Healthcare

Industry
Healthcare

Revenues
$1 billion

Headquarters
Miami, Florida

Endpoints
5,000

Employees
12,000

Tanium Products
Tanium Platform

The last thing anyone involved in end-of-life care wants to worry about is the security of the devices used in supporting patients and their loved ones. Yet that was the situation faced by engineers at VITAS Healthcare.

VITAS (pronounced VEE-tahs) is the largest hospice care provider in the United States, serving more than 19,000 patients — most of them at home — in 14 states and Washington, D.C.

In 2019, its IT department realized the company needed to find a better way to update software for its more than 5,000 employee laptops and other devices. To carry out major operating system upgrades, the company's IT technicians had to manually update machines. Such a process could take as long as a year to complete.

VITAS was also struggling to keep pace with monthly patching cycles. Using its current set of endpoint management tools, the software patching process took more than 30 days.

But VITAS found a way to eliminate virtually all these issues by turning to the Tanium Platform, says Mitch Teichman, senior manager of client engineering at VITAS.

Teichman discussed how Tanium transformed its endpoint software management process in a session at the Tanium Converge 2020 conference .

Problems updating and patching remotely

One of the key challenges faced by the VITAS IT department was updating its in-house electronic medical record (EMR) system to comply with ever-changing regulations. The required changes came even faster with the pandemic crisis.

"Unlike some updates, which might not be critical, this is how we run our business," Teichman explains.

The team's existing tools were too slow to keep up with the rapid-fire changes, didn't provide real-time feedback, and couldn't deliver the reporting the team needed.

"When you pushed software, you just sat there hoping that it got to where it needed to go," Teichman says.

The team also had to contend with endpoint management tools that could provide visibility for devices only when they were connected to a company VPN. That further slowed software updates and patching.

"We were facing long patching cycles, typically over 30 days, which essentially means we were perpetually patching," Teichman says.

©2021 Tanium. All rights reserved.

> We now live in complete harmony when it comes to reporting with the security team. It's a beautiful thing. The numbers we see are the same numbers they see.

Mitch Teichman
Senior Manager of Client Engineering, VITAS Healthcare

Before the IT team could finish one patching cycle, it had to start the next one. What's more, data in their reports didn't match those the security team saw. Each group was using a different reporting tool.

"We'd present reports to the security team, and they'd have completely different numbers," Teichman laments.

These problems were compounded by services that require care providers to work at the bedsides of patients in their homes. Even more than other companies under lockdown, VITAS had to deal with widely diverse devices and connections into the corporate network.

Software deployments in less than 24 hours

Teichman recalls the anticipation of the first EMR system update deployed using Tanium. "The EMR system is incredibly important to our business," he explains. "So there were a lot of nerves around here."

But the updates rolled out across the company's network in less than 24 hours, Teichman says. Plus, the team had full visibility into nearly all of its endpoints, allowing team members to track each stage of every update.

A dashboard showed which endpoints were currently downloading updates, which updates had completed, and which devices were current.

Teichman appreciates how the Tanium Platform also flags which endpoints fail to update and why.

"This real-time visibility is a boon for the IT team and leadership," Teichman says. "It allows us to report right away about something vital to the business with accurate numbers."

The VITAS IT team also caught up on software patching almost as quickly. The first patching cycle deployed more than 60,000 overdue patches yet was completed in just two days.

Since then, the VITAS IT team has cut the time needed for the ongoing patching process from 30 days to 2 weeks. If necessary, they can complete a patching cycle even quicker, but the extra time allows the quality assurance group to vet patches before they're widely released.

As the system of record for the company's endpoints, Tanium is bringing ongoing benefits to VITAS.

"We live in complete harmony when it comes to reporting to leadership with the security team," Teichman says. "It's a beautiful thing. The numbers we see are the same numbers they see."

These days, Teichman and his team can feel confident that VITAS devices are up-to-date and protected. That means the company's professionals and volunteers can look after patients without worrying about their laptops. "Despite having people and their devices scattered across the country, Tanium makes endpoint management business as usual for us," Teichman says.

TANIUM

Tanium offers an endpoint management and security platform built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

©2021 Tanium. All rights reserved.