CASE STUDY

Dental services provider secures 30,000 endpoints with Tanium

Healthcare organization gains visibility and control of thousands of endpoint devices across 800 offices in 24 U.S. states.

Business goals

Many companies provide end-user tech support, but few do it while a dental patient anxiously waits to be treated.

That's among the challenges facing a national dental services provider based in California's Orange County. Since 1994 it has provided business services that include IT, accounting, tax, legal and human resources (HR) to U.S. dental offices.

The approach lets these customers focus on what they do best — providing dental services — instead of running business processes. But the approach creates enormous challenges. These dental offices operate some 30,000 endpoint devices, including Windows personal computers (PCs) and embedded medical devices, from approximately 840 offices in 24 U.S. states.

To keep all these devices running smoothly and safely, the services provider turned to Tanium. The benefits include:

- Fast, effective tech support for in-network dental offices. Tanium products help keep customers' endpoint devices current, safely patched and performing well.
- Lower costs for IT security and operations, earned by consolidating IT tools and replacing others with Tanium's low-bandwidth platform.

Industry
Healthcare

Revenues
Privately Held

Headquarters
California, USA

Endpoints
30,000+

Employees
12,500 + 1,000 independent consultants

Tanium products
Core, Performance, Asset Discovery, Patch Management

Key benefits

- Greatly improve visibility into approximately 30,000 endpoints at some 840 dental offices
- Dramatically lower the impact of patching and other endpoint updates on the corporate network
- Provide excellent support for work-from-home migration, including the implementation of hundreds of new laptops, as part of the COVID-19 pandemic response
- Support the company's own digital transformation
- Improve customer experience, minimize effects of performance issues

> We needed a platform that was efficient, lightweight, and able to run with only minimal resources — yet still able to get the job done. That's why we turned to Tanium.

Nemi George
VP & Information Security Officer, Service Operations, National Dental Services Organization

Technology challenges

- Improve endpoint visibility and patching while also lowering the impact of these operations on both the network and its endpoints.
- Respond quickly and effectively to known vulnerabilities by quickly identifying and patching out-of-date software.
- Centrally upgrade remote older Windows 7 PCs to the current Windows 10 — without sending technicians into the field for manual upgrades.
- Keep the IT infrastructure up and running, even when the IT team is not present.
- Gain visibility into dental offices non-PC endpoints, chiefly embedded medical devices, for centralized software updates and vulnerability patching.
- Apply effective identity access and management to remote users, ensuring that customer networks, applications, and data are limited to authorized users only.
- Support a COVID-19 technology response, including supporting remote employees and treating homebound patients with new telemedicine systems.
- Support the service provider's digital transformation, including refreshed servers, all-in-one PCs, and an artificial intelligence (AI) imaging process.

How Tanium helped

Working from the maxim that "you can't protect what you can't see," Nemi George turned to Tanium for greater visibility into his company's devices. As its chief digital security officer, George appreciates how Tanium's hub approach places what he calls a "light touch" on his network.

That also enhances patching and software deployment. Thanks to a custom dashboard known internally as "Nemi's board," the IT staff can see which endpoint devices for both its employees and customers need either a software upgrade or patch.

Tanium's unified platform with its rich portfolio of capabilities also lets George eliminate and consolidate tools, which lowers license costs and simplifies operations.

Patch-download times are now 80% faster than before, he estimates.

Supporting WFH tactics

During the COVID-19 pandemic, the company relied on Tanium to manage and secure endpoint devices used by work-from-home (WFH) employees. Most of the company's employees typically use all-in-one PCs in the office. But once the pandemic hit, these employees shifted to WFH, and about two-thirds of them needed new laptops.

> Tanium Performance is probably the most important tool we have for operations. It gives us clear visibility into what's happened. When a customer has a problem, we essentially roll back the clock.

Nemi George
VP & Information Security Officer, Service Operations,
National Dental Services Organization

That also meant these PCs were off the corporate network. Tanium could help here, too; as long as a device is online, it's detectable by Tanium.

During the pandemic, Tanium also helped the company stand up a teledentistry platform for its customers. With many dentist offices closed except for emergency treatments, and many dental patients sheltering at home, there was a need to connect the two with video consultations. In this way, dentists could determine whether a patient needed to come for treatment urgently, or whether they could wait. To support this, the dental services provider stood up a teledentistry platform, and with Tanium's help, it did so in just 10 days. Tanium was the engine that pushed out and installed the unified communications product at dental offices.

Digital transformation

The company also relied on Tanium, particularly Discover, to support its digital transformation, which George describes as "massive." That includes a recent move to SD-WANs, refreshed servers and all-in-one PCs. To better support its customers, the company has also moved from 2D to 3D dental imaging. That's supported with a custom AI tool to provide a single view of a patient's dental images.

With so much changing, when a dental office calls with a performance issue, identifying the cause can be complicated. And unlike in many corporate settings, there's an additional source of urgency — a dental patient waiting uncomfortably in the chair. But with Tanium Performance, George and his team can gain visibility into the network's recent behavior, For example, maybe the performance issue started at 2 p.m., but Performance reveals a backup 10 minutes earlier that may have caused the problem. "With Tanium Performance," George says, "we're essentially able to roll back the clock."