TANIUM

GRAND Mental Health maintains 24/7 availability with Tanium

To protect sensitive data and serve clients, this provider of crisis, community, and addiction services sought greater visibility into its endpoints.

ORGANIZATION

GRAND Mental Health

LOCATION

Oklahoma

Something grand is happening in Oklahoma. In that U.S. state's northeast and north-central regions, GRAND Mental Health, a nonprofit organization, operates more than 30 clinics and offices across 13 counties. Each year, GRAND — an acronym for Grand Response Access Network on Demand — offers crisis, community, addiction recovery, and specialty services to some 30,000 residents.

To meet its mission of providing immediate access to quality care in the least restrictive environment, GRAND has developed an operating model based on three pillars. First, it's distributed some 10,000 Apple iPad tablets with an integrated app that lets users quickly connect with GRAND mental-health professionals. Second, GRAND maintains its clinics, known as Urgent Recovery Centers (URCs), on a 24/7/365 basis. Third, GRAND ensures that all incoming calls from patients are answered by a human working at an open URC.

It's an approach many clients appreciate. "People at GRAND could see the ways I wanted help, and they were willing to meet me there," says one past client, Laura Moses. "GRAND is not one individual person, it's a community."

Still, GRAND's IT security group faced a challenge. Due to a lack of network visibility, the team was slow to identify and remediate vulnerabilities on endpoint servers and workstations. That exposed the organization to unnecessary risk. And with healthcare data a highly attractive target for cyber crooks, the level of risk was serious.

"If something were to happen where we had downtime due to a cyberattack… it wouldn't just represent a lack of revenue, it would represent a lack of ability to provide high-quality care," says Josh Cantwell, GRAND's chief executive officer. "For those we serve, it could mean the difference between life and death."
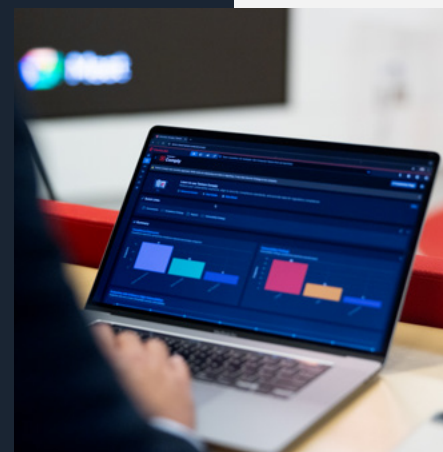
Deploy and Comply

Fortunately, GRAND CIO Rony Gadiwalla had in a previous job seen a demo of Tanium. He'd been impressed by the way Tanium handled remote clients and by its ease of use. Gadiwalla also liked the way Tanium played well with other vendors' tools. And at GRAND, he realized this Tanium feature could support his "multilayered" approach to cybersecurity.

"There should be a diversity of intelligence in your ecosystem," Gadiwalla explains. "If you go with a single-vendor ecosystem, you risk that single blind spot."

GRAND now uses Tanium's Deploy module to install and manage third-party software, as well as to help onboard new employees. The Tanium Comply module helps GRAND ensure its adhering to HIPAA (the U.S. Health Insurance Portability and Accountability Act) and other regulatory guidelines. Further, GRAND uses Tanium Patch to keep all its endpoints — a mix of servers and end-user workstations — current with the latest security updates.

Jeffrey Johnson, GRAND's director of systems, cites Tanium for being easy to install and just as easy to manage. Johnson also appreciates Tanium for being highly effective. "It ensures my confidence that the vulnerabilities are being managed and patched the way they should be," he says.

Super-fast detection

By using Tanium, CIO Gadiwalla and his staff at GRAND now enjoy some big benefits. One important gain is enhanced visibility into the security status of endpoint devices – it's now "fantastic," Gadiwalla says.

Importantly, that gives his security team data in real time, allowing them to make decisions based on the latest information. "Data security is where Tanium really shines," Gadiwalla says.

Tanium also helps GRAND's security team find vulnerabilities quicker than ever before. "Utilizing Tanium's Deploy and Comply modules, we were able to reduce the time it takes to address vulnerabilities by approximately 96 percent," says Johnson. "This allows us to then focus on more strategic improvements in our organization to better help our clients in various ways."

Without Tanium, Johnson adds, GRAND would have to spend "hundreds of hours" contacting end users to update their endpoint devices and address any vulnerabilities. "The time saved," he says, "is astronomical."

Looking ahead, the GRAND IT team plans to adopt more cloud-based systems. With fewer workstations and servers always connected to the organization's own networks, Johnson explains, the organization should become more agile.

For now, Tanium's single-platform approach helps to keep GRAND's endpoints safe and secure. Tanium, Johnson says, "allows my team to more easily and cohesively address vulnerabilities and software updates." Those kinds of gains are grand.

> "Data security is where Tanium really shines."

Rony Gadiwalla
Chief Information Officer
GRAND Mental Health

Results

Faster responses

Using Tanium, GRAND Mental Health has quickened its response time to endpoint vulnerabilities by an impressive 96 percent.

More time, higher value

By automating security measures, Tanium frees GRAND's IT staff and clinicians alike to focus on the strategic improvements that can help clients.

Safer operations

Before using Tanium, GRAND's security team couldn't always see where vulnerabilities lurked. Now, with Tanium, those vulnerabilities get identified and remediated quickly.

> "Utilizing Tanium's Deploy and Comply modules, we reduced the time needed to address vulnerabilities by approximately 96 percent. This allows us to focus instead on more strategic improvements in our organization to better help our clients in various ways."

Jeffery Johnson
Director of Systems
GRAND Mental Health