CASE STUDY

Arizona gains whole-of-state cybersecurity protection with help from Tanium

To protect the IT resources of smaller counties, cities, and districts, the state shares information, strategies, and tools – Tanium among them.

ORGANIZATION

The State of Arizona

LOCATION

Arizona, United States

When it comes to cybersecurity, smaller state and local governments can feel the cards are stacked against them. Thanks to the ubiquity of the internet, these public sector offices are vulnerable to attacks from large, sophisticated cyber criminals and hostile nation-states. Yet, with their limited budgets, state and local governments often lack the resources needed to keep their systems and data safe.

Case in point: Navajo County, Arizona. The county's sprawling area of 9,950 square miles, located in Arizona's northeastern corner, is home to just 111,000 residents. (For comparison, the U.S. city of Peoria, Illinois, has a similar population yet covers a mere 48 square miles.) The county's IT director, Ken Dewitt, gets by with a staff of just 15.

“How are we going to protect ourselves from nation-states that are trying to attack us every day?” he asks. “We might think we're the smartest people in the room, but if they throw 1,000 people at us, our 15 IT employees can't keep all the county's information safe.”

Colleen Flannery, CTO for Arizona's Chandler Unified School District, faces a similar situation. Her district, located in the southeastern part of the Phoenix capital metro area, has some 44,000 students in K-12 public schools.

However, with limited resources, Flannery has found that the cybersecurity tools needed to provide world-class cyber protection are prohibitively expensive.

“We have to do more with less,” Flannery says, “yet we’re a prime target. We have a lot of data on our students, parents, and employees. Bad actors know we’re under-resourced.”

At the state level, Arizona CISO Ryan Murray describes the challenge as existential. “If one of our cities or school districts were taken offline by a ransomware attack, they wouldn’t be able to provide their services,” he says. “In fact, they’d cease to exist.”

A whole-of-state solution

To ensure that Arizona’s smaller counties, cities, and districts get the kind of cybersecurity protection they need but probably can’t afford, the state adopted a whole-of-state strategy roughly six years ago. This approach, previously adopted by a few U.S. states, brings an entire state up to a common security baseline and then protects that baseline by training all state employees in security awareness.

“An attack against one of us,” Murray says, “should be seen as an attack against all of us.”

To achieve this statewide security baseline, Arizona has used funds provided by a U.S. Department of Homeland Security grant to build a collective defense network. The work involves sharing information, strategies, and tools. And one of those new shared tools is Tanium.

Arizona originally implemented Tanium for its state agencies during the COVID-19 pandemic. With many employees suddenly working from home, the state needed a new way to monitor and provide software patches.

“How do we patch a device that’s sitting on someone’s home network, which we can’t see, and which doesn’t touch any of our existing infrastructure?” Murray recounts. “Tanium was one of the technologies that allowed us to do this.”

Once Arizona officials saw how well Tanium protected state-level agencies, they decided to also use Tanium at the county, city, and district levels. “We knew they were struggling,” Murray says. “So, we said, ‘Let’s take this vetted technology and expand it out.’”

“A huge win”

How has Tanium worked out for Arizona? Very well. “In the last six months, we’ve used Tanium to patch over 40,000 vulnerabilities across the state’s local agencies,” Murphy says. “These are school districts and cities that were literally trying to patch these things manually. They see this innovation, this thing they’ve never been able to do before.”

Dewitt of Navajo County is among these pleased users. “Tanium allows us to see all our individual endpoints and update those,” he says. “And it cost us nothing but the time to implement. That’s a huge win.”

Prior to using Tanium, Dewitt and his staff never knew precisely how many endpoints they had, what those devices were running, or whether their patches were up to date. “Before,” he says, “we kind of guessed.”

That guesswork led to big gaps. The county has about 1,000 endpoints, including a mix of laptops, desktop PCs, printers, and other devices. Before using Tanium, the team’s best guess was about 700. That was not good, as Dewitt points out: “If an endpoint’s out there, but you can’t reach it and touch it, that’s a problem.”

Flannery of the Chandler Unified School District enjoys an even bigger benefit. She uses Tanium to manage nearly 20,000 endpoints, a mix of student, teacher, and staff laptops, desktops, and mobile devices.

Additionally, the school district’s original Tanium implementation provided asset management. “We need to know what software we have in our environment, whether it needs to be updated, and then be able to update it,” Flannery explains.

Tanium has also helped the district do more with less. “That’s important,” Flannery says, “because we’re not well-resourced. With Tanium, we saved manual labor. And even more important, we mitigated our risk.”

> “Tanium lets us see what updates we need to apply, and then apply them. Before, we kind of guessed.”
>
> **Ken Dewitt**
> Director of IT, Navajo County, Arizona

Results

Power patching

In just six months, Tanium helped the State of Arizona patch over 40,000 vulnerabilities across its local agencies.

Know, don’t guess

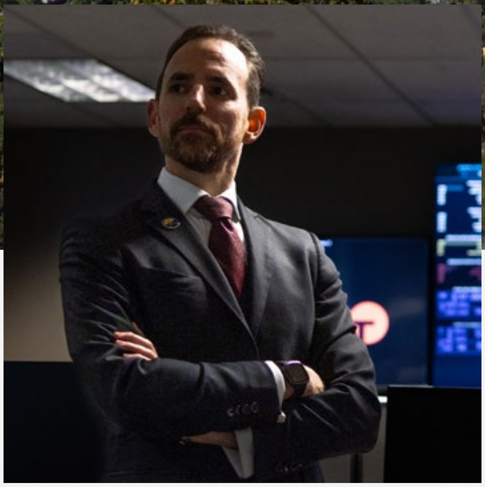
Using Tanium, the IT department of Arizona’s Navajo County discovered that its endpoints numbered closer to 1,000 than the 700 devices previously guessed at.

Identify, evaluate, update

Arizona’s Chandler Unified School District uses Tanium to identify software being run on some 20,000 endpoints, determine whether updates are needed, and then apply those updates as needed.

> “In the last six months alone, we’ve used Tanium to patch over 40,000 vulnerabilities across our local government entities. These are local school districts and cities that were literally trying to patch these things manually.”

Ryan Murray
Interim CISO, State of Arizona



Tanium delivers the industry’s only true real-time cloud-based endpoint management and security offering. Its converged endpoint management (XEM) platform is real-time, seamless, and autonomous, allowing security-conscious organizations to break down silos and reduce complexity, cost, and risk. Securing more than 32M endpoints around the world, Tanium’s customers include more than 40% of the Fortune 100, 7 of the top 10 U.S. retailers, 9 of the top 10 U.S. commercial banks, all 6 branches of the U.S. military, and MODs and DODs around the world. It also partners with the world’s biggest technology companies, system integrators, and managed service providers to help customers realize the full potential of their IT investments. Tanium has been named to the Forbes Cloud 100 list for eight consecutive years and ranks on the Fortune 100 Best Companies to Work For.

TANIUM™

For more information on The Power of Certainty™, visit www.tanium.com and follow us on LinkedIn and X.