CASE STUDY

Phoenix keeps over 20,000 endpoints safe and secure with Tanium

As the Arizona city grew, so did its cyber risk. With Tanium, endpoint patching has become robust, quick, and effective

City of Phoenix

ORGANIZATION

The City of Phoenix

LOCATION

Phoenix, Arizona

How is cybersecurity like a game of darts? The bigger the target, the easier it is to hit. Just ask the fast-growing City of Phoenix, where its growth has increased its cyber risk.

The Arizona city has grown from fewer than a million people in 1990 to nearly 1.7 million today, making it the fifth-largest city in the United States. The greater Phoenix metro area, known as the Valley of the Sun, is home to nearly 5 million people.

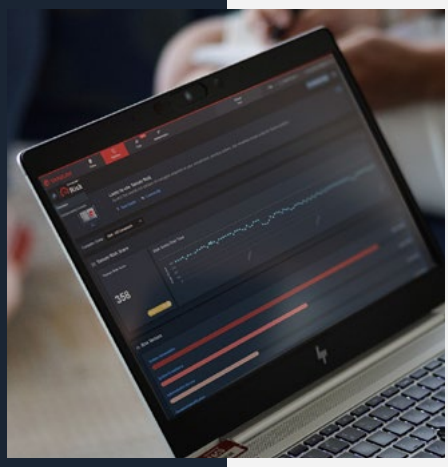
The city's dry, warm climate attracts both businesses and tourists. Four Fortune 500 companies are headquartered in Phoenix, not to mention U-Haul, Best Western, and the semiconductor manufacture, TSMC. Last year, 19 million people visited Phoenix, many of whom stayed in the city's nearly 28,000 hotel rooms. It was also the busiest year ever for the local Sky Harbor International Airport, which handled more than 48.8 million travelers.

Governing all that growth requires both a big staff and a robust IT infrastructure. The city government employs over 14,000 people, and they use more than 20,000 endpoint devices.

To keep these devices secure, the Phoenix cybersecurity group has grown five-fold, from a staff of just four people five years ago to 20 today.

The city now boasts a Security Operations Center (SOC) as well as groups for cyber strategy and planning, security architecture and engineering, and risk management and compliance.

"You have to operate with the mindset that someday, we'll have an incident, breach, or compromise of some kind. It's inevitable," says Phoenix CISO Shannon Lawson. "We want to make sure we're in a good position, that we're not negligent with the data, and that we're protecting the information of our citizens and employees."



Protecting with patching

A major component of any endpoint security strategy is patching. Before implementing Tanium, the City of Phoenix patched with no fewer than four separate tools. ""That meant staff had to understand and manage a far more complex environment to patch systems across the City," says Steen Hambric, the city's CIO.

Multiple patching tools also required more training. While the tools functioned similarly, they delivered those functions differently.

In addition, Phoenix had quite a lot of old legacy hardware and software. Compounding the issue, CISO Lawson wasn't always able to locate or even identify these systems.

"We had hardware that wasn't even made anymore, plus unsupported operating systems with unsupported applications, all with direct access to the internet," Lawson recounts. "The bad guys were saying, 'Thank you for making our job so easy.'"

All that changed when Phoenix adopted Tanium. Initially, the city implemented Tanium for patching. Later, the city implemented Tanium further to include asset management. "With Tanium we can ask, 'What do we have, and where is it?' That's important," Lawson says.

The city also uses Tanium for software license reclamation, to discover software that's licensed but isn't being used. Rather than simply renewing all its software licenses, which would be both common and costly, Phoenix now uses Tanium to identify this unused software. Then the city lowers its costs by allowing those software licenses to expire.

Faster patching

Tanium has transformed patch management for the City of Phoenix. For one, it's allowed the city to consolidate all its patching, formerly done on four separate tools, onto a single platform.

"I don't want to have to grab all these different tools and stitch together what our patch structure looks like," Lawson says. "That's where Tanium has helped us. We got rid of a lot of these disparate tools that were not working well together. Now Tanium is our ground truth for where we're at."

Tanium also gave Phoenix a patching cycle that is repeatable, reliable, and fast – reducing the patching cycle by an impressive 75 percent.

"Where in the past we were always playing catch-up, now with Tanium, we're not only able to catch up but also do it in significantly less time," says CIO Hambric. "Tanium makes patching significantly easier. Standardizing on Tanium also ensures we're getting the right skill set and coverage."

Phoenix is now also using Tanium for asset discovery and management. That's helped to identify old, unsupported systems that need to be either disconnected or replaced. "With Tanium," Lawson says, "I know what assets are out there, the status of those assets, what applications run on them, and whether they're up to date."

That level of success has led other Phoenix departments to adopt Tanium, too. The vulnerability team, for one, now uses Tanium to cross-check reports from its main tool. "Our main vulnerability tool will tell you something, but it might not be totally true," Lawson explains. "With Tanium, we have another tool to verify that information."

This has led to better collaboration among the city's departments. "When you have one team using one tool and another using something else, that's just chaos, not to mention expensive," Lawson says. "Now Tanium helps to bring these teams together."

> **"Where in the past we were always playing catch-up, now with Tanium, we're not only able to catch up but also do it in significantly less time."**
>
> **Steen Hambric**
> CIO, City of Phoenix

Results

Faster patching

Using Tanium, the City of Phoenix has reduced its patching cycle by 75 percent. With over 20,000 endpoints in use, the time savings add up quickly.

Easier collaboration

The City of Phoenix originally used Tanium solely for patching, but it's since been adopted by the vulnerability team and Security Operations Center (SOC). That eliminates organizational silos by encouraging the groups to work together.

More efficient training

Standardizing on Tanium has eliminated Phoenix's need to train staff across multiple tools. Instead, the city trains people on just one tool, creating the needed skill set and coverage.

> "With Tanium, I get an authoritative source on where we're at with our patching."

Shannon Lawson
CISO, City of Phoenix

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.