A GOVERNMENT TECHNOLOGY CASE STUDY | TANIUM

State of Arizona:

Making Good on Fiscal Responsibility and Cybersecurity Mandates

Fiscal responsibility and cybersecurity are cornerstones of Arizona Governor Doug Ducey's administration and are guiding principles for the state IT department. To meet the governor's directives in these areas, IT must maximize its investments in devices, software and other assets while minimizing vulnerabilities and cybersecurity risks.

To better manage IT assets and limit cybersecurity risks within the enterprise, the state's IT team needed clear visibility into the asset inventory and endpoints, as well as a way to remediate vulnerabilities as quickly as possible. The existing tools and approaches could not provide anywhere near the level of accuracy, detail and functionality required for the scale and complexity of the enterprise.

Poor Visibility into Agency Silos

When the state approached Tanium, it had been struggling with visibility into the assets on statewide systems for some time. Each state agency operated in its individual silo with its own toolset, making it difficult to consolidate information and manage assets across the enterprise.

"Our biggest challenge was inventory management. We didn't have a good sense of what or how many devices we had, or where they were — let alone the software or amount of memory that was running on them. We were concerned that we were wasting money on licenses and devices that weren't being used," says Arizona Deputy CISO Ryan Murray.

The IT team's few enterprise-wide tools couldn't provide the type of information needed, so they would send out surveys to agencies and rely on them to gather the information. Besides impeding inventory management, agency silos and lack of visibility put the enterprise and individual agencies at greater risk of cyberattack. It was difficult to identify and address vulnerabilities on compromised devices or on older software. And with fragmented patch management, the risk of cybercriminals exploiting vulnerabilities rose.

The state decided to work with Tanium on a proof of concept for an enterprise platform to solve these critical issues. Then the pandemic struck. Besides shifting the initiative into high gear, it made the cybersecurity component of Tanium's solution even more imperative.

Eight-Fold Increase in Number of Remote Workers

As government offices shut down, the state's remote workforce grew by a factor of eight — from five percent of total workers in February 2020 to more than 40 percent. That massive expansion meant more endpoints to manage, patch and update — with the same number of IT personnel as before and no ability to remediate devices that were not logged in to the state network or a VPN.

Meanwhile, cybercriminals were taking advantage of pandemic-related disruptions to attempt a variety of attacks against the state. Their attack attempts increased by about four times what the IT team saw prior to the pandemic. In addition, employees engaged in more risky behavior when working at home. The IT team was blocking three to four times more websites and risky web traffic than before the pandemic.

"The cybersecurity side of Tanium's solution became much more urgent. It became: Yes, we want to continue to be more efficient and save money, but we're in a position now where we have to identify, patch and remediate these vulnerabilities immediately or somebody will find them and exploit them against us," says state CISO Tim Roemer, who also serves as the director of the Arizona Department of Homeland Security.

The Tanium Solution: Massive Remediation in Record Time

As the project committee went through the proof of concept, the security aspects of the solution became even clearer.

“We saw that we could save a lot of money but realized the biggest win would be a more secure state. We’d be able to get risky devices off, update the software — even in a teleworking environment — and automate patching,” says Roemer. “We’d be able to patch faster, better and more efficiently than we ever could have dreamed and that in turn would help protect our systems and the personal data of the people we serve.”

The state soon moved from a proof of concept to a formal deployment of the Tanium solution. The highly scalable, enterprise-wide solution can support all state agencies and will provide a common platform for managing the endpoint environment. An integrated suite of tools includes asset management, patch management, risk auditing and compliance, automated remediation and more.

The IT team is still in the process of bringing in all agencies that want to be in the production environment. It has installed Tanium agents on more than 56 percent of devices so far. Better visibility and tools have already enabled the state to improve its security profile by identifying assets and risks, coordinating responses to discovered risks and performing patching in real time.

“The metrics we’re seeing have us smiling ear-to-ear. In a single 72-hour push, we were able to patch and remediate more vulnerabilities — almost 90 percent of known vulnerabilities — than we did in the previous six months combined,” says Roemer.

An important aspect of the Tanium solution is that it expedites remediation and frees up hours of staff time by automating many patching and remediation tasks. In doing so, it will help the IT team meet state policies related to remediation times. In addition, the solution allows the agencies to remediate vulnerabilities on devices that aren’t logged into the state network or VPN. As long as the user is connected to the internet, an IT team can monitor the device and make corrections to it.

Visibility is King

As the state brings more agencies and devices into the Tanium production environment, it looks forward to expanding its visibility and control even further to improve operational efficiency and save taxpayer dollars.

“Visibility is king, and we now have visibility that we never had before,” says Murray.

With centralized visibility into devices and software, the state can take a closer look at enterprise software licensing. Instead of each agency paying a premium for a few licenses, the state can buy them at the enterprise level to get a better rate. Centralized asset management will also reduce costs by enabling administrators to identify underutilized or inappropriately assigned devices and software licenses and by consolidating and reducing the number of asset and vulnerability management toolsets that exist in agency silos.

As the state CISO, Roemer is pleased with the remediation metrics his team has captured so far. “They help me and other team members sleep better at night. We don’t know what’s going to happen tomorrow, but this solution and the quality of Tanium’s team, products and customer service have put us in a better position to address whatever we might face. Part of our success is that we view vendors as partners, and I cannot think of a better partner for this initiative than the Tanium team.”

This piece was developed and written by the Government Technology Content Studio, with information and input from Tanium.

Produced by: government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation’s only media and research company focused exclusively on state and local government and education. **www.govtech.com**

For: TANIUM™

Tanium offers a unified endpoint management and security platform that is 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 several branches of the US Armed Forces, rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium has been named to the Forbes Cloud 100 list of “Top 100 Private Companies in Cloud Computing” for five consecutive years and ranks 10th on FORTUNE’s list of the “100 Best Medium Workplaces.” Visit us at **www.tanium.com** and follow us on LinkedIn and Twitter**.**

IMAGE PROVIDED BY SHUTTERSTOCK.COM