CASE STUDY

Government agency replaces BigFix with Tanium to improve cyber hygiene

With IT modernization top of mind, a federal government agency had an immediate need for more visibility into all assets with real-time speed at scale and the ability to meet CDM requirements — something their existing solution could not do.

Tanium solutions

- Threat Hunting
- Asset Discovery and Inventory
- Sensitive Data Monitoring
- Risk and Compliance Management
- Client Management

Challenge

Lack of confidence in asset and endpoint data demanded a new tool.

Solution

Tanium enabled confidence in asset data, resulting in significant cost savings and risk reduction.

Result

A platform approach that helped reduce tool bloat, fill security gaps by awarding a single source of truth for asset data, and provided visibility with certainty, speed and at scale.

Tanium helped gain visibility, reclaim costs and meet federal requirements.

Federal agency gets visibility and control during a pandemic with Tanium

In early 2020, when much of the world began shutting down in response to the pandemic, a government agency with 100,000+ employees had recently replaced its existing endpoint-management tool in order to address their most critical security concerns – and meet Continuous Diagnostics and Mitigation (CDM) requirements.

They chose Tanium to address their top security requirements — and the pandemic validated that choice — giving them the visibility and control they needed to manage their new remote workforce.

The deployment of Tanium seemed daunting as remote work began during the height of the pandemic, but due to the ease of implementing the tool with very few resources needed onsite, the system went live in less than two months, and without putting employees at risk.

As a result, the agency was able to eliminate well over 200 servers from their old solution, along with associated maintenance, resulting in

> Tanium has given us the ability to see 10-15% more endpoints than our prior tool, giving us more comprehensive visibility and control of our organization than ever before.

Cybersecurity Technical Program Lead
Government agency

significant cost savings, while also achieving a single source of truth for managing its many endpoints safely and securely – with just one agent on one platform.

When the agency replaced an antiquated but commonly used endpoint-management tool with the Tanium platform, they not only reclaimed significant costs, and were able to have trend reporting for the first time, but also achieved a single source of truth for all asset data, helping them meet new security requirements mandated internally as well as with Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA).

Challenge

Just before the pandemic started, the agency had prioritized these four top security requirements, as part of an security and IT modernization initiative:

- Report Hardware Asset Management (HWAM), Software Asset Management (SWAM), and Configuration Settings Management (CSM) to the DHS CISA Dashboard for the Continuous Diagnostics and Mitigation (CDM) program.
- Move to a platform-based solution to help eliminate tool bloat while filling gaps in current security solutions.
- Maintain visibility into all IT assets across locations worldwide.
- Implement best practices recommended by the Committee on Foreign Investment in the United States (CFIUS) to reduce reliance on foreign-owned software companies.

They were using an existing tool, BigFix, but it was falling short on meeting these requirements, which prompted the agency to look for a replacement.

The government agency had software tools in place to address some of these requirements and concerns, including BigFix – which is commonly used by government agencies. It generally provides a baseline view of known assets, but could not give the agency complete asset visibility at scale, worldwide. This made it difficult for the agency to make decisions and take necessary actions, as they did not feel confident in the accuracy of their data.

And because the parent company that owned BigFix was now based outside of the United States, they did not meet the best practice set forth by The Committee on Foreign Investment in the United States (CFIUS). The government agency decided it would search for a better solution.

Solution

Though the agency had chosen Tanium before the effects of the pandemic started to take hold in the United States, the project kicked off during a time when offices were shutting down. The very next business day after the contract was signed, six Tanium appliances arrived onsite at the agency's data centers, and the only agency staff person to ever set foot in the agency during the entire project from kick off to go-live was the person who received, racked and stacked the servers – which made it easier for the agency to go-live during the pandemic. The solution continues to be completely supported virtually.

The six servers included a High Availability (HA) design and no additional Tanium infrastructure or design considerations were required to accommodate the massive shift to telework. Over 200 BigFix servers were replaced with three Tanium servers (six for HA). This provided a huge savings in hardware (servers), and associated maintenance costs.

Shortly after go-live, Tanium administrators at the agency leveraged the new tool and its self-service capabilities to significantly reduce Tier 1 help-desk tickets. The platform immediately gave one administrator the ability to patch a critical operational issue with their remote meeting software that was preventing users in one of their units from being able to join meetings – a major issue when the majority of staff was working remotely.

"I've fixed several hundred over the last 24 hours," the admin says, "and the end user is functional in minutes."

> If we did not have Tanium right now, hundreds of end users in one of our units would be forced to drive into the office and wait for an IT specialist to solve their issue. Tanium is able to fix most of these issues — and in a matter of minutes.

Technical Administrator
Government agency

Result

Tanium helped remove many manual efforts associated with patching third-party tools and operating systems. It also acted as a backup patching tool when existing tools fell short.

"Sniper packages are super-useful in Tanium, and they're a real time fix for end users on the internet side with no other options working except Tanium," says an agency admin. "If we did not have Tanium right now, most end users would be forced to drive into the office and wait for an IT specialist to solve the issue. Tanium is able to fix most of these issues in a matter of minutes."

When it came to having a single source of truth for all asset data, the agency no longer needs to rely on the key performance indicator (KPI) reports. The Tanium system identified 10-15% more endpoints that were not visible with their prior tool, giving the agency more comprehensive visibility and control of their enterprise than ever before. With the entire agency now using one Tanium endpoint agent as the single source of truth, administrators can consistently pull information across the organization in real time, with both speed and scale.

The agency also enjoys complete visibility with just one platform and agent. Administrators can easily and quickly check both active directory and non-active directory joined assets, a task that previously required multiple tools. They also have more comprehensive and more high-fidelity data to support CDM and have access to trend reports over time – something they didn't know they needed that they could not do with their previous tool.

Check out Tanium for Federal Government: **tanium.com/federal**

Complete visibility
into both active and non-active directory joined assets

Endpoint Discovery
found 10–15% more endpoints previously not visible with prior tool

Cut costs
from retired servers and maintenance of old solution