CASE STUDY

TANIUM
Federal

Federal agency improves security posture and saves millions of dollars with Tanium

Industry
U.S. Federal Government

Headquarters
Washington, D.C.

Managed endpoints
Over 100,000

Time savings
20,000 hours

Cost savings
over $150 million

Results

Reduced risk

Removed unauthorized and deprecated software at scale.

Time and cost savings

Saved over $150 million and more than 20,000 hours of manual work.

Greater productivity

Reduced time spent looking for software components with access to enterprise-wide, granular endpoint data.

Increased visibility

Discovered 20 times more endpoints containing deprecated software than were previously known.

How a large U.S. federal agency with over 100,000 endpoints uses Tanium to manage software deployments and reduce security risks.

CHALLENGE

Managing unauthorized and custom software

Endpoint management remains a top challenge in the U.S. public sector, with many federal agencies grappling with how to manage unauthorized, custom-built, or unapproved software applications that are difficult to track and secure.

One federal agency was in the process of phasing out a home-grown, mission-critical software using their existing IT operations tools. In alignment with the federal government's IT modernization and cost reduction plan, the agency decided to uninstall the legacy software from all machines across the organization. Altogether the team estimated about 1,000 impacted machines.

What they found in the process of removing the software was that the packages contained components that were going unnoticed. These components posed potential security risks and needed to be removed promptly from the agency's environment as part of their deprecation process.

The agency was using a variety of software applications across thousands of systems and didn't have a way to find and remove all components of the deprecated software across their enterprise.

> The agency was using a variety of software applications across thousands of systems and didn't have a way to find and remove all components of the deprecated software across their enterprise.

SOLUTION

Using Tanium to scan and remove the software

The agency's IT operations group was previously using a mix of management tools to track different assets. However, these tools were unable to pinpoint software and file locations across various user, transaction, management, and machine assets - which put the agency at a disadvantage.

The agency needed a more effective way to find all packages and remnants of this deprecated software with certainty. The IT operations team consulted with their security operations center (SOC) which was using **Tanium Converged Endpoint Management (XEM)** for threat hunting. Based on the SOC team's success using Tanium, the IT operations group decided to see if it could help remove all components of the deprecated software.

While Tanium could scan for software packages at scale and instantly return accurate data out-of-the-box, the agency opted to build a custom script instead, which they were able to do with hands-on partnership from their assigned Tanium expert support manager.

RESULTS

Real-time visibility with less overhead

After deploying the custom script, the IT operations team conducted an initial scan of all their devices and discovered 20,000 devices with the software components that needed to be removed. This was significantly more than the 1,000 they initially estimated.

Tanium made it easy to discover, identify, and remove the software from all 20,000 systems, in a fraction of the time it would have taken their existing software management tools to simply find the software, and with far greater accuracy. This saved the agency over 20,000 hours that would have been spent manually removing the software from each field workstation

In addition to deprecated software removal, the agency also looked to Tanium to help with their Log4j discovery and software licensing true-ups.

Addressing Log4j vulnerabilities

The agency successfully used Tanium to identify and remediate nearly 80,000 unique vulnerabilities associated with Log4j, found across nearly 25,000 workstations.

Due to the complexity and prevalence of the Log4j vulnerabilities, Tanium's precise scanning methods provided the only way to identify all instances of the unpatched framework - including hundreds inside a patch for a third-party enterprise platform.

With Tanium's continuous reporting, the agency could swiftly monitor for out-of-date software dependencies and keep them up to date.

Software license true-ups

When it came time for an agency-wide audit of an enterprise software used across their environment, none of the agency's existing tools could reliably find all instances of that software.

Using Tanium, they were able to scan their entire network for the software usage data and discovered they were heavily under-licensed and over-installed. This meant they would be required to pay for the extra, unused licenses if they did not remove them within the month.

Using Tanium, they quickly removed the software across the enterprise which saved them over $150 million in software licensing costs.

Converged endpoint management for the U.S. Federal Government

With Tanium, the agency rapidly eliminated vulnerability gaps from unauthorized and deprecated software, and reclaimed costs from unused software licenses across their enterprise.

Lastly, Tanium has brought the agency's SOC and IT operations teams closer together because they can collaborate and take action on shared challenges using a single source of truth for real-time endpoint data, across their environment.

Can your team identify supply chain risks at runtime, or identify software bill of material vulnerabilities and their CISA KeV score? Does your organization meet EO 14028, Section 4 requirements for responding to supply chain risks?

Learn more about how Tanium supports the U.S. Federal Government at www.tanium.com/federal.

Learn more