

Achieving IT operational efficiency and cost savings in the government



Introduction

Given the increasing cyber threats targeting all levels of government, there is immense responsibility to efficiently manage and secure diverse environments. Leaders are challenged to do more with less, facing conditions like skills gaps, siloed teams with point solutions, and constrained budgets. With Tanium Autonomous Endpoint Management (AEM), Canadian public sector organizations can meet these challenges head on.

Tanium AEM is instrumental in achieving operation efficiency and cost savings. For example, a large U.S. government organization was recently tasked with reviewing their current systems to identify unused commercial software. Using Tanium, the organization produced a real-time inventory of all software

installed across their enterprise in minutes, allowing them to remove unused instances, with an associated cost-avoidance of \$150 million department-wide, showcasing the power and efficiency of the Tanium platform.

Tanium AEM

Tanium AEM's patented architecture delivers intelligent, real-time automation of IT and security operations, increasing efficiency, improving security, and reducing costs. Tanium supports 34 million endpoints globally, including those of our public sector customers and allies across Australia, Canada, Japan, the United Kingdom and the United States, among others. Tanium enhances operational efficiency and security posture while addressing cybersecurity threats from nation-states and other bad actors.

Tanium capabilities to achieve efficiency and cost savings

Software inventory and usage tracking

Tanium provides real-time insights into software usage and distribution to streamline audits, reclaim unused or underutilized software, and manage entitlements effectively, resulting in significant savings.

Intelligent automation

Tanium AEM delivers intelligent, real-time automation of IT and security operations, safely and reliably executing changes, increasing efficiency, improving security, and lowering costs. Examples of Tanium AEM automations include:

- Reclaiming unused or underused software licenses
- Patching endpoints for OS and third-party software updates in a phased manner
- Identifying, prioritizing, and remediating vulnerabilities

Unified platform

Relying on point solutions across IT and security teams leads to siloed data, inefficient operations, increased risk, and underutilized resources. With Tanium AEM, organizations can replace point solutions with a unified platform that supports IT operations and security teams. This single source of truth aligns teams, enabling them to operate more efficiently.

Comprehensive reporting

Tanium AEM delivers comprehensive, customizable real-time reports to inform actions and share insights with leadership. Tanium AEM also provides natural language support to ask questions about the environment and get answers in as little as seconds.



Deployment options

Tanium is available on premise or zero infrastructure in the cloud with Canadian data centers. Additionally, Tanium was chosen through an open procurement process for the Endpoint Visibility and Awareness Solution for the Government of Canada, for more than 120 departments, with millions of endpoints. Tanium has a presence with organizations across five provinces in numerous industries.

We continue to meet the expectations and contract requirements of our customers, who see Tanium as an essential partner to enhance their cybersecurity posture, streamline IT operations, and reduce long-term technology debt.



Tanium Cloud has been compliant with the required security controls applicable to the processing of highly sensitive Protected B information in the cloud for the Government of Canada since 2023.

[LEARN MORE →](#)

