PULSE POLL RESEARCH & LEAD GENERATION CAMPAIGN

TANIUM × GOVEXEC INTELLIGENCE

Autonomous Defense: Closing the Remediation Gap Against AI-powered Threats

Original federal research, engineered into a two-part, sales-ready lead generation campaign

Andrew Mullen Scott
Sr. Content & Digital Strategy Manager – Public Sector, Tanium

GOAL

Federal IT and security leaders are under constant pressure to modernize endpoint security while managing a growing mix of environments — IT, cloud, mobile, and operational technology (OT) — with constrained budgets and staff. Tanium set out to generate original, first-party research that would validate this challenge in federal decision-makers' own words, positioning Tanium's Autonomous IT Platform as the answer to a data-backed problem rather than a vendor-asserted one.

To do this, Tanium partnered with GovExec Intelligence (Market Connections) to design, field, and publish a “Pulse Poll” survey of federal government IT and security decision-makers, then translated the findings into two distinct, gated lead generation assets: a co-branded research report and a companion infographic.

OBJECTIVES

- Partner with a trusted, editorially independent research firm to co-develop a survey instrument that captured meaningful signal on federal endpoint security maturity, without steering respondents toward a specific technology or vendor
- Translate the primary research into a data-backed report and a companion infographic, each built as a standalone, top-of-funnel lead generation asset
- Use the resulting data to reinforce Tanium's core platform narrative — closing the gap between detection and remediation — with third-party validated evidence rather than internal claims

STRATEGY & PROGRAM DETAILS

Survey Design & Collaboration

Beginning in February 2026, I led Tanium's side of a multi-week collaboration with GovExec Intelligence's Director of Research Services to build a survey instrument that would serve both editorial and pipeline goals. I set the strategic intent up front, framing the survey around four directional signals we wanted the data to capture:

- Organizational operational resilience and readiness
- Maturity of automation and AI-enabled workflows
- Current effectiveness in identifying and responding to cyber risk
- Overarching modernization priorities and areas of potential pipeline growth

Rather than hand off a finished questionnaire, I supplied GovExec with intended signals and outcomes mapped to each question and asked for their editorial judgment on execution — including how to frame the opening, scene-setting question so it established a maturity baseline without steering respondents toward a specific technology domain.

One exchange from that process is a good example of the back-and-forth: I pushed to make sure the automation question explicitly captured both “AI” and “autonomous” capabilities, since that distinction matters to how Tanium's platform is positioned. GovExec's research lead flagged that stacking “AI and/or autonomous” risked creating a double-barreled question that would muddy the data. We landed on a cleaner construction — “intelligent automation (including AI-driven and autonomous capabilities)” — that kept the question methodologically sound while still preserving the language Tanium needed for downstream messaging.

Fielding & Delivery Timeline

Milestone	Owner	Date
Draft poll delivered	Market Connections	Feb 27, 2026
Feedback provided for revisions	Tanium	Mar 2, 2026
Poll finalized & approved	Both	Mar 5, 2026
Programming & testing	Market Connections	Mar 5–11, 2026

Milestone	Owner	Date
Fielding (n = 100 federal IT/security decision-makers)	Market Connections	Mar 12–25, 2026
Rapid results delivered	Market Connections	Mar 30, 2026
Draft report delivered	Market Connections	Apr 10, 2026
Infographic development kicked off	Both	Early Apr 2026
Final report published for lead gen	Market Connections	Apr 2026

Two-Part Content Strategy

Rather than publish a single report and move on, the program was scoped from the outset to produce two assets from the same dataset, each suited to a different stage of the funnel:

- Federal Endpoint Security Landscape report — a two-page, GovExec Intelligence–branded research report presenting the full findings alongside a dedicated "Tanium's Perspective" section connecting the data directly to the Tanium Autonomous IT Platform
- "Autonomous Defense" infographic — a visually designed companion piece, "Autonomous defense: Closing the remediation gap against AI-powered threats," built for scroll/skim audiences on digital and social channels, restating the same proprietary data with a clear "Learn more" call to action

A Third Life for the Data: Mythos Sponsored Article

When Anthropic's Claude Mythos Preview broke as a fast-moving federal cybersecurity story in late April 2026, I secured and wrote a sponsored article placement on NextGov/FCW (part of GovExec), run under existing ad spend rather than increased incremental budget for this campaign. The piece covered the news itself while featuring insights from industry leaders alongside Tanium Federal Executive Client Advisor, Ed Debish, and wove in the Pulse Poll's own investment-priority data to give the research a third life in an entirely unplanned news cycle.

Program Investment

The program was budgeted at $30,000 under Tanium's FY27 federal marketing plan — booked to the GovExec content syndication line for Q2 FY27 (May 2026) — covering survey design, fielding, and both lead-generation assets.

KEY FINDINGS

The survey (n = 100 federal government IT and security decision-makers and influencers, fielded March 2026) surfaced a clear storyline: agencies have made real progress on visibility and detection, but a meaningful gap remains between detecting a risk and fully remediating it — exactly the problem Tanium's platform is built to close.

41%
Fully integrated visibility, detection & response

45%
Strong detection, but response not fully coordinated

12%
Uneven visibility / manual processes in some areas

2%
Lack consistent visibility & response

9%
Independent AI action with human oversight

42%
Automation widely used, but needs approval

43%
Used only in limited areas / pilots

6%
Operations still fully manual

Top investment priorities for the next 12–24 months:

Investment Priority	% Selecting
Exposure and vulnerability risk reduction	55%
Security operations and incident response automation	51%
Increasing the use of AI to assist operational decision-making	48%
Patch and configuration management automation	34%
Managing and securing OT alongside IT assets	31%
Improving asset inventory, configuration, or CMDB accuracy	25%

Defense respondents were significantly more likely than federal civilian agency respondents to prioritize exposure and vulnerability risk reduction (71% vs. 48%) — a distinction pulled directly into audience segmentation for the infographic's follow-on distribution.

RESULTS

Both assets were published for lead generation and tracked independently. As of June 30, 2026 (roughly ten weeks post-launch), the campaign had generated:

Asset	Leads Generated
Federal Endpoint Security Landscape report (Pulse Poll)	101
“Autonomous Defense” infographic	10
Total	111

Leads skewed toward exactly the audience the survey was designed to reach — federal civilian and defense IT and security decision-makers, including program managers, systems engineers, and IT project leads across agencies such as the Department of Veterans Affairs, the FAA, and other federal civilian and defense organizations.

$30,000
Total program investment (FY27 federal marketing budget)

~$270
Cost per lead generated (111 total leads)

PARTNERS

GovExec Intelligence / Market Connections: Elizabeth Lowery, Director of Research Services, led survey design, fielding, and reporting.

Tanium: Program led by Andrew M. Scott (Sr. Content & Digital Strategy Manager, Public Sector), in partnership with Kristin Starkel (Sr. Director, Public Sector Marketing) and Danielle Sloan (Sr. Regional Marketing Manager, Federal).

PULSE POLL

Underwritten by TANIUM

Federal Endpoint Security Landscape

Capabilities, Performance, and Investment Focus

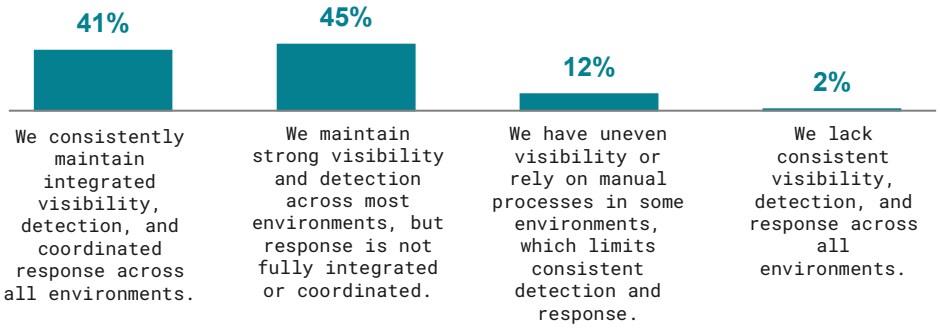
Introduction

As federal agencies work to strengthen endpoint security, they must manage a mix of systems and environments while responding to ongoing security risks and pressure to improve visibility and response. In March 2026, GovExec Intelligence surveyed federal government professionals involved in IT and security decision-making to assess current capabilities across endpoint environments, how quickly organizations identify and remediate risks, the use of AI and automation in security operations, and the priorities shaping future investment.

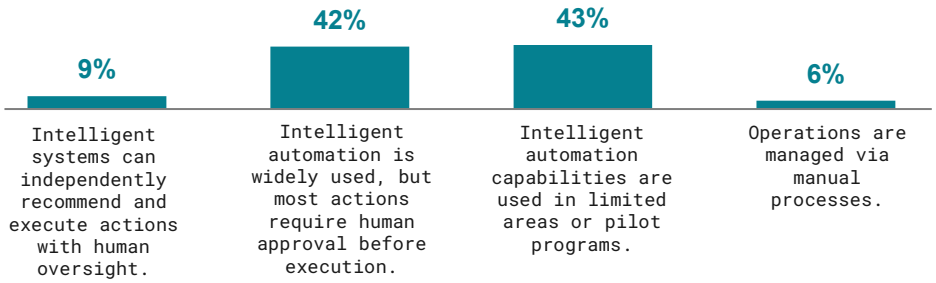
Findings

Respondents report generally strong visibility and detection capabilities, though many lack a fully integrated response. AI and automation are in use, but most report using them in limited areas or requiring human approval.

Which of the following best describes your organization's visibility, detection, and response capabilities across your endpoint environments (IT, cloud, mobile, and OT)?



Which of the following best describes the level of intelligent automation (including AI-driven and autonomous capabilities) in your organization's IT and security operations?



Tanium's Perspective

These findings reveal a federal endpoint security landscape at an inflection point. Most agencies have made real progress on visibility and detection — but visibility alone isn't enough. The data makes clear that the critical challenge is no longer seeing risk; it's acting on it fast enough to matter.

The response gap identified in this survey is exactly the problem Tanium was built to close. When 45% of respondents report strong detection but fragmented or uncoordinated response, and when remediation across enterprise IT and OT environments routinely extends into days or weeks, the cost of that gap compounds with every hour an exposure goes unaddressed.

The Tanium Autonomous IT Platform addresses this directly—unifying asset intelligence, exposure management, security operations, and automated remediation into a single platform driven by AI and real-time endpoint intelligence. Rather than connecting disparate tools after the fact, Tanium provides decision-grade data at the source, enabling agencies to move from identifying risk to remediating it without the manual handoffs that slow response.

The survey's top investment priorities — exposure and vulnerability risk reduction, security operations automation, and AI-assisted decision-making — reflect exactly where Tanium is focused. Our approach to governed autonomy keeps human oversight in place for mission-critical decisions while automating high-volume, repeatable actions like patching and configuration enforcement at speed and scale.

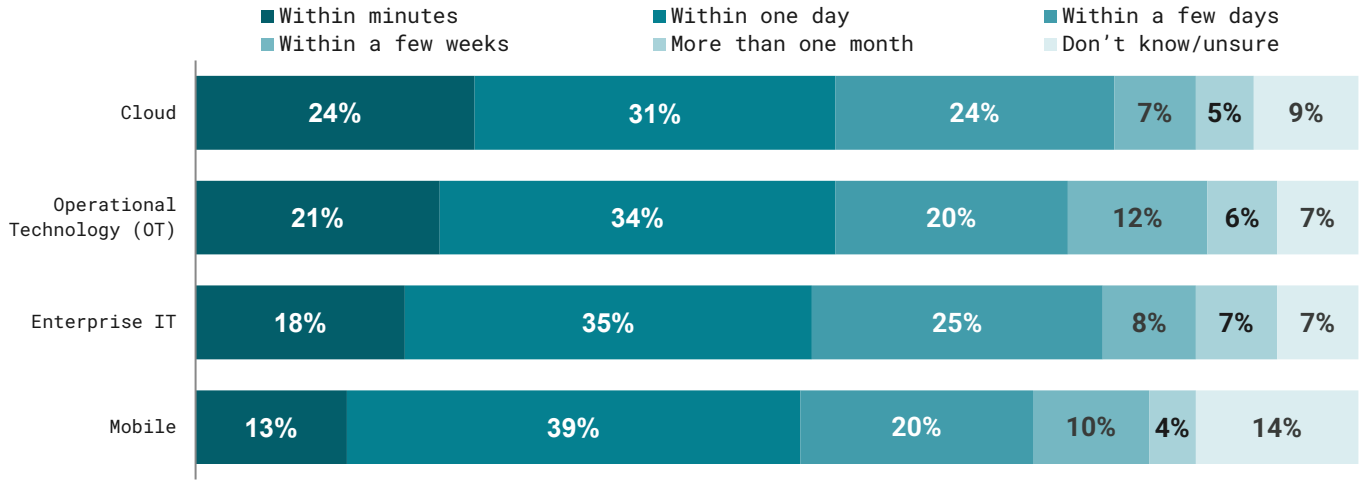
For federal agencies navigating expanding attack surfaces with constrained resources, the path forward isn't more tools. It's a unified platform that continuously reduces risk in real time.

PULSE POLL

Underwritten by TANIUM

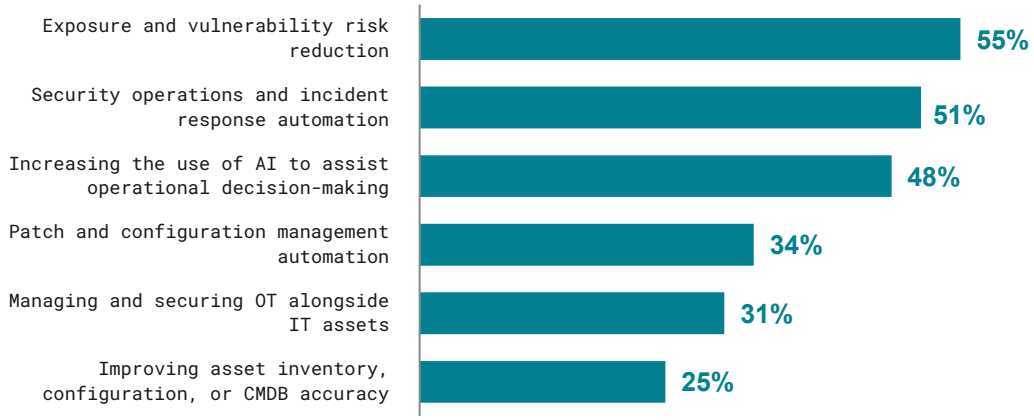
Remediation timelines are generally consistent across environments, with cloud leading in speed.

How long does it typically take your organization to identify and fully remediate endpoint security risks in each of the following environments?



Reducing exposure and vulnerability risk is the top investment priority, with security operations and incident response automation and AI-supported decision-making also among the top focus areas.

Which of the following areas are the highest priorities for modernization and investment within your organization over the next 12–24 months?



71% vs. 48%

Defense respondents are significantly more likely than **federal civilian agency respondents** to prioritize **exposure and vulnerability risk reduction.**

Note: Respondents were asked to select up to three

Methodology

GovExec Intelligence deployed a 4-question poll to a random sample of 100 federal government IT and security decision-makers and influencers, fielded in March 2026.

About GovExec Intelligence

GovExec Intelligence delivers actionable data and insights for businesses serving the public sector. The market research firm is a sought-after authority on preferences, perceptions, and trends among federal civilian, defense, and state and local decision makers.

About Tanium

Tanium is the Autonomous IT company. Driven by AI and real-time endpoint intelligence, Tanium Autonomous IT empowers IT and security teams to make their organizations unstoppable.

The company is recognized as a Leader in the inaugural 2026 Gartner® Magic Quadrant™ for Endpoint Management Tools and as a Leader in the IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Device Management 2025–2026 Vendor Assessment.

Many of the world's leading public sector and defense organizations trust Tanium's single, unified platform for endpoint management and security to innovate faster, stay resilient and move business forward with confidence, at scale.

To learn how Tanium delivers Autonomous IT for unstoppable government – visit www.tanium.com and LinkedIn.

Autonomous defense: Closing the remediation gap against AI-powered threats.

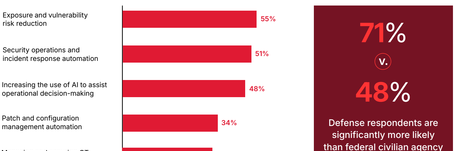
According to a recent GovExec Intelligence survey fielded in March of 2026, 45% of all respondents have made real progress toward endpoint visibility and detection, **but gaps remain**.

TANIUM

While respondents report generally strong visibility and detection capabilities, many lack a fully integrated response.

Which of the following best describes your organization's visibility, detection, and response capabilities across your endpoint environments?

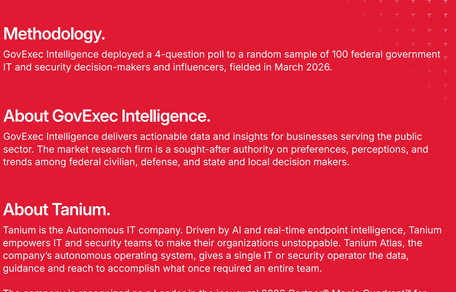
Which of the following best describes the level of intelligent automation (including AI-driven and autonomous capabilities) in your organization's IT and security operations?



Tanium helps agencies close this gap.

In an era where AI models can identify zero-day vulnerabilities at a scale and speed unmatched by humans, visibility is no longer sufficient. Reactive, fragmented approaches to remediation across enterprise IT and OT environments extend patch times and increase agencies' risk profile.

How long does it typically take your organization to identify and fully remediate endpoint security risks in each of the following environments?



Which of the following areas are the highest priorities for modernization and investment within your organization over the next 12–24 months?

The Tanium Autonomous IT Platform helps federal IT leaders reduce this gap and meet key goals by consolidating asset intelligence, exposure management, security operations and automated remediation onto a single platform. Powered by AI and driven by real-time intelligence, Tanium equips federal users with **decision-grade data**, enabling teams to move from risk identification to automated remediation at scale while eliminating manual handoffs that would otherwise impede a

See how your agency can move from reactive to resilient with Tanium's Autonomous IT Platform.

Learn more

Methodology.

GovExec Intelligence deployed a 4-question poll to a random sample of 100 federal government IT and security decision-makers and influencers, fielded in March 2026.

About GovExec Intelligence.

GovExec Intelligence delivers actionable data and insights for businesses serving the public sector. The market research firm is a sought-after authority on preferences, perceptions, and trends among federal civilian, defense, and state and local decision makers.

About Tanium.

Tanium is the Autonomous IT company. Driven by AI and real-time endpoint intelligence, Tanium empowers IT and security teams to make their organizations unstoppable. Tanium Atlas, the company's autonomous operating system, gives a single IT or security operator the data, guidance and reach to accomplish what once required an entire team.

The company is recognized as a Leader in the inaugural 2026 Gartner® Magic Quadrant™ for Endpoint Management Tools and as a Leader in the IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Device Management 2025-2026 Vendor Assessment.

Many of the world's leading public sector and defense organizations trust Tanium's single, unified platform for endpoint management and security to innovate faster, stay resilient and move their missions forward with confidence, at scale.

TANIUM