EXPERT-LED WEBINAR ACTIVATION

TANIUM × GOVERNMENT TECHNOLOGY

Autonomous Security: Next-Gen Strategies to Meet Today's Evolving Threats

Expert-led, independently moderated — and built to score sales-ready pipeline

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

GOAL

Tanium sponsored "Autonomous Security: Next-Gen Strategies to Meet Today's Evolving Threats," a webinar produced with Government Technology (e.Republic), to reach state and local government IT and security leaders managing the same core problem: expansive, hybrid IT environments and mounting compliance demands outpacing what manual tools and stretched teams can handle.

This activation program was scoped to do more than fill a registration counter. Working with e.Republic's enhanced jurisdictional data layer, the goal was to walk away with an audience that was pre-scored on real buying signal — IT budget, active opportunity volume, seniority, and stated maturity with autonomous/AI-driven tools — so Tanium's SDR team could prioritize follow-up by fit and readiness rather than working the list in registration order.

OBJECTIVES

- Scope and co-develop webinar content with Tanium subject matter experts — pairing an executive/strategic perspective with a hands-on security research perspective — rather than handing off a generic sponsor slot
- Partner with Government Technology / e.Republic to reach a qualified state and local government IT/security audience beyond Tanium's own house list, and hit a 200-registrant qualified target
- Capture enhanced jurisdiction-level data (IT budget, 12-month opportunity history, population, employee count, branch/org/job function) on every registrant so the audience could be segmented and prioritized, not just counted
- Convert live engagement — polls, post-event survey, live Q&A — into qualitative signal on where prospects actually sit in their autonomous security journey, and route the full list to SDRs for direct follow-up

STRATEGY & PROGRAM DETAILS

Program Scoping & Speaker Collaboration

I led and scoped this webinar on behalf of Tanium. The topic and angle were shaped in direct discussion with Claire Bailey, Tanium's Public Sector CIO, and Melissa Bischoping, Sr. Director of Security & Product Design Research — pairing Bailey's state-government operating experience with Bischoping's technical research background so the session could speak credibly to both the strategic and the practitioner audience in the room. Content was co-developed jointly between the three of us rather than built by one team and handed to speakers to deliver.

Deborah A. Snyder — a Senior Fellow at the Center for Digital Government and former New York State CISO — moderated. Bringing in an independent, recently-serving state CISO as moderator gave the session a level of government credibility that a vendor-only panel couldn't, and kept the framing solution-focused rather than product-focused.

Distribution & Promotion

e.Republic (publisher of Government Technology and parent of the Center for Digital Government) owned promotion and audience acquisition. All 200 qualified registrants came through e.Republic's promotion of its public-sector subscriber base — the program hit its full registration target on e.Republic reach alone, with no supplemental sponsor-driven promotion required.

Sales-Ready Data Capture

Every registrant record was enriched through e.Republic's Industry Navigator / Smart Leads layer before it ever reached Tanium: jurisdiction IT budget, logged IT opportunities over the trailing 12 months, jurisdiction population, employee count, and standardized branch-of-government, org-function, and job-function/role fields. That meant registrants arrived pre-segmented for pipeline scoring rather than as bare contact records SDRs would have to research themselves.

Nurture & Follow-Up

Post-webinar, the full registrant list — live attendees, on-demand viewers, and registration-only contacts alike — was routed directly to Tanium's Sales Development Representatives (SDRs) for direct follow-up, using the enhanced firmographic and opportunity data to prioritize outreach rather than working the list in raw registration order.

Program Investment

The program was budgeted at $20,000 — averaging roughly $100 per qualified registrant across all 200 registrants.

KEY FINDINGS / RESULTS

As of the registration report cutoff (08/13–08/21/2025), the webinar had generated the following registration, engagement, and audience-quality data:

200 / 200
Qualified registrants vs. e.Republic target (100%)

58.5%
Attendance rate (117 of 200 viewed live or on-demand)

38.5%
Registrants at Exec/Senior Mgmt/Supervision level

144
Unique government jurisdictions represented

$20,000
Program investment (SLED marketing budget)

~$100
Cost per qualified registrant (200 registrants)

Registration & Engagement

Metric	Total
Qualified registrations (e.Republic promotion)	200
Viewed live	93
Viewed on-demand	24
Total viewed (live + on-demand)	117 (58.5%)
Registered, did not view	90
Live Q&A questions submitted	3
Post-event survey responses	17
Poll respondents	52

Audience Value: What the Registrant List Is Actually Worth

Because e.Republic's jurisdictional enrichment ties back to a defined government entity, the 200 registrants can be rolled up to 144 unique jurisdictions (185 unique organizations, counting sub-agencies separately) with associated budget and opportunity data — turning a registrant count into an addressable-pipeline estimate:

Audience Metric	Total
Unique jurisdictions represented	144
Combined jurisdiction IT budget represented	$24.8B
Logged IT opportunities, trailing 12 months, across those jurisdictions	5,752
Combined jurisdiction population represented	~101.0M
Registrants from state government	106 (53%)
Registrants in an IT job function	132 (66%)

Figures are deduplicated to one record per jurisdiction (using e.Republic's underlying jurisdiction ID) to avoid double-counting shared state-level budget across multiple agencies within the same state.

What the Audience Told Us

Live poll and post-event survey data added qualitative texture to the firmographic data — useful both for scoring individual leads and for shaping follow-on messaging:

Biggest Endpoint Security Challenge (n=43)	% Selecting
Integrating legacy systems with modern tools	26%
Difficulty keeping up with compliance requirements	21%
Alert fatigue and limited staff capacity	21%
Lack of real-time visibility across devices	16%
Manual and time-consuming patching processes	16%

Autonomous / AI-Driven Security Journey Stage (n=36)	% Selecting
Discussed it, but haven't taken steps yet	33%
Early stages of evaluation or pilot	19%
Not sure what's involved	19%
Not currently considering — other priorities	17%
Actively using in production	11%

Nearly 70% of poll respondents had not yet moved past discussion or early evaluation of autonomous/AI-driven security tools, and only 11% reported active production use — a market-immaturity signal that both validates the webinar's premise and gives SDRs a natural opening question for follow-up conversations.

Post-event survey responses skewed toward early-stage intent: the majority of respondents described attending to "learn" or stay current on the topic, a smaller group cited active research for an upcoming project, and one respondent — from the California Department of Corrections and Rehabilitation — attended on a direct recommendation from their Tanium subject matter expert, an organic signal worth flagging to that account's SDR directly.

PARTNERS

Tanium: Program led by Andrew M. Scott (Sr. Content & Digital Strategy Manager, Public Sector), with Claire Bailey (Public Sector CIO) and Melissa Bischoping (Sr. Director, Security & Product Design Research) as featured speakers.

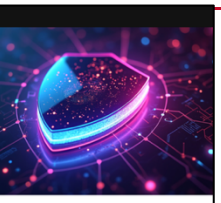
Government Technology / e.Republic: Promotion, registration, and lead generation partner. Deborah A. Snyder (Senior Fellow, Center for Digital Government; former New York State CISO) served as moderator.

MEDIA — WEBINAR LANDING PAGE

< All Webinars

WEBINAR government technology

AUTONOMOUS SECURITY – Next-Gen Strategies to Meet Today's Evolving Threats



Overview

WATCH NOW

State and local governments are facing a perfect storm: expansive IT environments with thousands of endpoints, hybrid workforces using unmanaged devices, mounting compliance mandates, and cybersecurity teams that are stretched to the limit. Traditional tools and manual processes can no longer keep pace with the volume and velocity of modern threats.

In this timely and solution-focused webinar, government technology leaders explore how next-generation cybersecurity approaches—rooted in real-time visibility and automated control—are helping agencies respond faster, operate smarter, and reduce cyber risk—without overburdening staff. Learn how these tools are empowering public agencies to detect vulnerabilities in real time, continuously monitor endpoint health, and accelerate response with AI-driven automation.

What You'll Learn:

- How autonomous cybersecurity solutions work—and where they fit in your existing toolset
- How to achieve real-time visibility across endpoints, applications, and users
- Ways to accelerate threat detection, triage, and remediation using automation
- Strategies for meeting NIST and CIS compliance mandates with fewer manual processes
- How autonomous systems can ease the strain on understaffed IT and cyber teams

Who Should Attend:

- Chief Information Officers (CIOs)
- Chief Information Security Officers (CISOs)
- IT Directors and Managers
- Cybersecurity Program Managers
- Risk and Compliance Officers
- Network and Endpoint Security Professionals

Join us to explore how autonomous endpoint management can help your organization stay one step ahead—no matter how fast the threat landscape evolves.

Sponsored By

TANIUM

Speakers

Claire Bailey
Public Sector CIO, Tanium

Claire Bailey is the Public Sector CIO at Tanium, supporting the company's North America Government business. Her more than 41 years of experience includes driving modernization, security, and transformation initiatives for federal, state and local governments, in both private and public sector leadership roles. Some of her most prominent positions include serving as Chief Technology Officer for the State of Arkansas, and several industry vice president and director roles at Veracode, KWR Strategies, and Compuware, among others. Bailey's contributions to public service and innovation have earned her honors and recognition from several institutions including the Governor's Quality Award (Arkansas), Government Technology, StateScoop, and the Arkansas Academy of Computing.

Melissa Bischoping
Sr. Director, Security & Product Design Research, Tanium

Melissa Bischoping is a dedicated security advocate. She blends her academic background in human psychology with extensive technical expertise to address complex technical challenges for businesses and individuals. Melissa focuses on emerging operational and security risks, zero-days, and vulnerabilities. Her passion lies in leveraging data-driven insights to enhance threat mitigation strategies, optimize risk and vulnerability management, and excel in digital forensics and incident response methodologies.

Deborah A. Snyder — Moderator
Senior Fellow, Center for Digital Government

Deborah is an accomplished C-level influencer, with a broad range of experience in government, policy, cybersecurity, privacy and information technology. An experienced and highly respected thought leader who has held executive roles for over two decades.

She recently retired from her position as New York state's chief information security officer (CISO) after over 35 years of public service.

In that role, as part of New York state's information technology transformation and consolidation initiative, she helped redesign how the state protects its data. As state CISO, she directed the state's comprehensive cybersecurity governance, risk management and compliance program, providing strategic leadership and vision, and assuring business-aligned, risk-based investments that maximized business opportunity and minimized cybersecurity risk. She also directed the NYS Cyber Command Center, hotline, procedures for reporting and response to cyberthreats, and digital forensics.

She holds multiple industry certifications including Certified Information Systems Security Professional (CISSP); Certified in Risk and Information Systems Control (CRISC); SANS Strategic Planning, Policy, and Leadership (GSTRT) Global Information Assurance Certification; and Project Management Institute certified Project Management Professional (PMP).