TANIUM

Building more resilient networks with autonomous technology

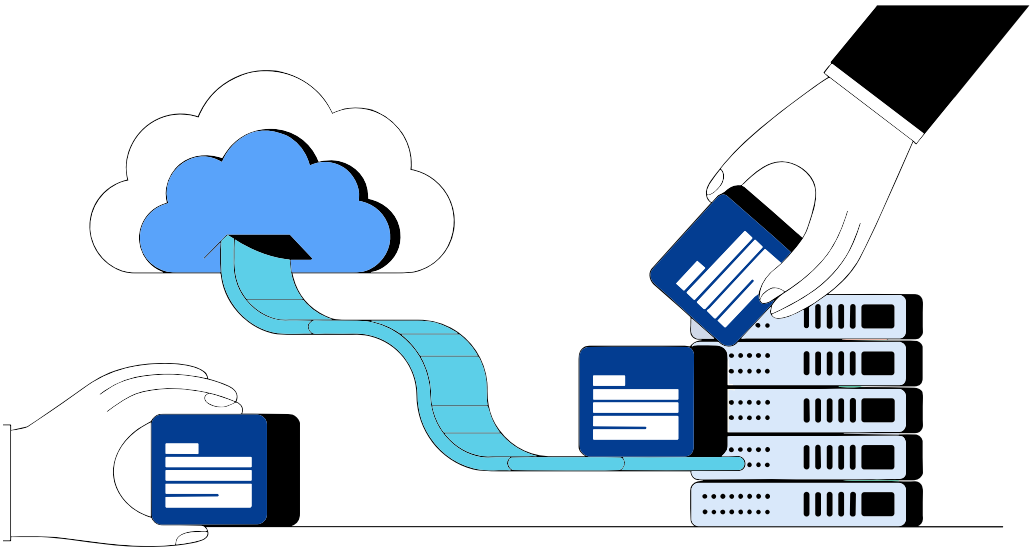
By automating complex IT and security tasks, agentic AI helps agencies recover more quickly from performance issues and cyberattacks

Melissa Bischoping | Tanium

In 2016, Matt Swann introduced the Incident Response (IR) Hierarchy of Needs to illustrate the essential capabilities for IR professionals. At its foundation are asset visibility and telemetry from endpoint assets. If an organization is not doing endpoint management thoroughly and in real time, then everything else—whether incident response, modernization or zero trust implementation—will be a struggle. This challenge remains especially acute for federal agencies operating across hybrid, distributed and highly regulated environments.

Fortunately, the revolution in artificial intelligence is opening the door to automating capabilities and workflows that until 10 years ago could only be done by software engineers or people with advanced scripting backgrounds. Now those professionals can focus on strengthening infrastructure resilience, reducing risk exposure and supporting mission outcomes.

Furthermore, the promise of agentic AI lies in its ability to execute bounded, policy-constrained actions that previously required highly skilled human intervention—such as monitoring performance metrics, proposing deterministic code or configuration changes, and making recommendations to improve routine operations or intervene early during a network intrusion.



Importantly, this form of autonomous decision-making is not without guardrails; it is designed to operate within clearly defined parameters, with observable decision paths and explicit human oversight.

Why we need to trust but verify

Burnout among technology professionals in the federal government is a serious concern. I have high hopes that we can leverage agentic AI as a way to relieve some of that mental fatigue and empower people to do more with less while not burning out in the process.

Agentic AI solutions must be designed with the human in mind to avoid creating additional administrative burden or a new kind of alert fatigue. For example, IT professionals can focus on specifying what they want to accomplish with their workflows, and then agentic AI can determine how to accomplish it. The technology can prototype workflows much faster than humans can, and users can continually improve those workflows by asking: "If I change this attribute or this input, how would that affect my outcome?" Agentic AI can make recommendations based on real-time information.

Of course, success hinges on our ability to trust but verify. Human oversight, auditability and clear lines of accountability remain essential.

Well-designed agentic tools will ensure the human remains in the loop without over-engineering proposed solutions or governance processes.

Getting back on mission as quickly as possible

Tanium's Autonomous IT Platform combines agentic workflows with real-time endpoint data and enterprise-wide visibility while providing the human-in-the-loop governance that allows agencies to make better decisions faster. The goal is faster, more informed action with reduced operational risk.

For instance, confidence scoring allows IT teams to ask, "If I do this, am I confident it will be successful and won't cause an outage in my environment?" We've also given people control by providing step-by-step explanations and progressive roll-outs to prevent unsuccessful changes from deploying further. Those safeguards are important for keeping bad code or configurations from cascading all the way through the IT environment.

Looking ahead, agentic AI workflows will support the security operations teams of the future by triaging security alerts and providing the context necessary to make decisions faster and stop attackers before they reach their target. Furthermore, agentic AI can provide the context for agencies to understand how to prevent future intrusions.

Ultimately, the objective should not be the unrealistic elimination of all outages or intrusions. Resilience—not perfection—is the standard. In a mission-driven federal environment, recovery time directly affects citizen services, national security and continuity of operations. With autonomous IT grounded in real-time data and governed execution, government networks can restore operations faster and with greater confidence. ■

Melissa Bischoping *is senior director of security and product design research at Tanium.*

> **"Well-designed agentic tools will ensure the human remains in the loop without over-engineering proposed solutions or governance processes."**

TANIUM

Autonomous IT. Unstoppable Government.

With real-time endpoint intelligence and control, federal agencies can innovate faster, stay resilient, and protect critical data with confidence.

- Save time and money with intelligent automation
- Remediate risks before they can be exploited
- Reduce regulatory risk by staying continuously compliant
- Retain complete control of every autonomous action

tanium.com/federal

ADOBE STOCK//PNG-JPEG-VECTOR