IDC Link
Real-Time IDC Research® Opinion on Industry News, Trends, and Events

Tanium Empowers IT and Security to Be Unstoppable with Autonomous IT

December 03, 2025

By: Michelle Abraham, Philip D. Harris, CISSP, CCSK, Phil Hochmuth, Grace Trinidad

IDC'S QUICK TAKE

Tanium announced several advancements at its 10th annual Converge conference aimed at accelerating the shift toward autonomous operations and security.

EVENT HIGHLIGHTS

At Tanium's 2025 Converge conference, which was held November 17–20, 2025, Tanium introduced new features and expansions across its Autonomous IT Platform. The company unveiled Tanium Ask in AI mode, an agentic experience that integrates AI-driven workflows for operational efficiency, allowing administrators to manage data discovery, software, and security operations within a single interface.

Tanium also expanded its endpoint management capabilities to include operational technology (OT) devices and Apple mobile endpoints, such as iPhones and iPads, enhancing visibility and control across diverse environments. Tanium will not stop there; it is planning to add IoT devices and additional observability in Kubernetes environments. The Tanium Connector for Microsoft Intune further unifies device management by integrating telemetry from Intune-managed endpoints and allowing Tanium to take action on Intune-managed macOS, iOS, and iPadOS endpoints.

In the realm of security operations, Tanium introduced Jump Gate, which enforces zero trust principles by providing just-in-time and just-enough access to sensitive resources, and HuntIQ, which embeds Tanium experts into customer environments to optimize security performance and proactively detect threats.

Tanium has announced the general availability of its Security Triage Agent and Security Triage Agent with Identity Insights within Microsoft Security Copilot, which leverage Tanium's real-time endpoint intelligence and Microsoft's AI capabilities to help security analysts investigate and respond to threats. The Tanium agents collect endpoint artifacts, analyze context — including identity data from Microsoft Sentinel and Microsoft Entra ID — and recommend next steps. The agents are available for purchase and deployment through the Microsoft Security Storefront, where users with appropriate Azure roles can easily discover, buy, and configure them for use in their environments.

IDC #lcUS53968725

Also on the partner front, the Tanium AI Agent for ServiceNow streamlines incident response by providing real-time endpoint intelligence and actionable recommendations directly within ServiceNow's Now Assist chat interface.

IDC'S POINT OF VIEW

Expanding into new endpoint categories will bring Tanium's capabilities in endpoint management, exposure management, and security operations to a broader part of the company's customers' organizations, reducing customers' gaps in asset visibility. With the addition of iOS and macOS devices, Tanium is now officially in the unified endpoint management market, the fastest-growing segment of the overall $10.7 billion-dollar client endpoint management software market (for CY24). This will allow Tanium customers to ingest and analyze more endpoint data into their security, operations, and digital experience platforms and foster more convergence of endpoint management roles and capabilities (Although the announcement leaves out Android endpoints, which are expected to be supported in the near future.).

With the addition of OT device support, Tanium becomes one of the few IT and security solutions that can assist organizations in demystifying protection and equipping IT and OT staff with the visibility needed to protect critical infrastructure and manufacturing environments from cyberattack. In addition, Tanium's compliance enforcement and anomaly detection offerings require in-depth knowledge of how devices operate when in true compliance, driving deeper and richer device-class intelligence for Tanium. Paired with Tanium's sensor fabric, the company is positioned to command the highest-resolution data available to help organizations manage all endpoints with confidence.

Relatedly, Tanium also indicated in keynote remarks efforts to enhance the Tanium Confidence Score. At this moment, the Tanium Confidence Score provides real-time data aggregation to help customers assess the safety and reliability of IT changes. As security and IT teams become more tightly integrated, tools like Tanium Confidence Score are invaluable to organizations that must make quick decisions about risk and reliability. The planned enhancements include Confidence Score personalization — tailored insight based on the enterprise environment and tolerance for risk. In the meantime, Tanium is building an enviable set of telemetry with its vendor device partnerships and sensor fabric.

As its customers become more comfortable with automation, Tanium plans to lean into exposure remediation as the differentiating feature of its exposure management solution. In November 2025, Tanium became a CVE Numbering Authority (CNA), demonstrating its continued focus on exposure management and increasing efforts in threat and vulnerability research.

Tanium's approach leverages AI and real-time endpoint intelligence, enabling organizations to transition from reactive to autonomous operations through a unified platform built on Tanium's linear chain architecture. For security, AI will be embedded throughout detection and investigation, enriching alerts and guiding next actions. Today, over 50% of Tanium's customers are using the company's automation features as well as interacting with Tanium Ask to gain insights into their environment more quickly.

In the past three years, Tanium's customer base has grown by 200%+, as it moved to support a wider range of customers beyond the company's original large enterprise target. This effort brings autonomous IT to more organizations that may have fewer security and IT practitioners to manage and secure their IT environment. Tanium has been at the forefront of the convergence of security and IT operations tools and teams, which was evident by the many conversations at the event among attendees who said they wore "multiple hats" in terms of security/management responsibility. This shift is also seen in IDC's recent survey data, where half of the U.S. enterprise endpoint IT operations team respondents said they are also responsible for their organization's security operations on endpoints.

Subscriptions Covered:

Endpoint Device Management and Enterprise Mobility, Governance, Risk and Compliance Services, SIEM, Exposure Management and Related Artificial Intelligence Technologies, Trust Measurement and Metrics