INTEGRATION BRIEF

Tanium and Microsoft Sentinel

Integrated solution that expedites incident response using real-time data and control.

Member of
Microsoft Intelligent Security Association

Microsoft

Key benefits

FASTER INVESTIGATIONS

Complete investigations and hunts more quickly using real-time data and experiences that will help you accurately access the full depth, breadth and impact of an attack.

AUTOMATED REMEDIATION

Use real-time data and control to prevent configuration drift and enforce compliance. After an investigation, confidently execute automation at scale to remediate and bring your organization back to a complaint and healthy state.

SINGLE PANE OF GLASS

With Tanium-powered Playbooks and real-time data hosted directly within Microsoft Sentinel, incident response teams will resolve incidents more efficiently and accurately without the need for console switching.

Customer challenges

Organizations face a broad range of challenges as complex and highly targeted attacks increase in parallel with rapidly growing attack surface areas. Some of the most important for security operations teams include:

- A lack of real-time comprehensive visibility is preventing organizations from managing and securing all endpoints, leaving gaps for attackers to exploit.
- Incidents and investigations can't be efficiently resolved due to the lack of real-time data, actionable insights and automated remediation capabilities.
- After an attack has been successfully stopped, bringing endpoints and the environment back to a healthy state takes too long, leaving them vulnerable to the next attack.

Solution

Tanium's integration with Microsoft Sentinel provides organizations with an opportunity to reduce the complexity of their environments and achieve higher levels of incident response efficacy than either of the solutions can achieve on its own.

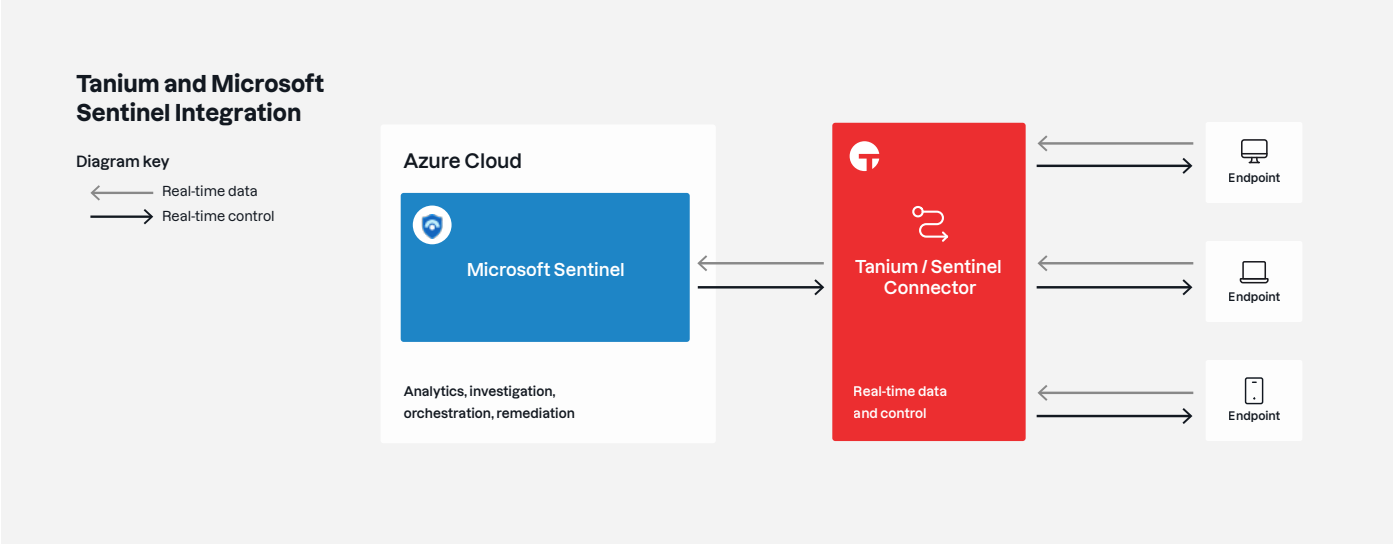
Security teams will benefit from enriched Microsoft Sentinel capabilities that enable them to better triage, prioritize, and investigate alerts using Tanium's real-time endpoint data. The data — and the additional context that come with it — are surfaced directly within the Microsoft Sentinel console. This eliminates the need to switch between multiple tools to investigate incidents and gain complete visibility.

Additionally, analysts will be able to hunt, investigate and perform remediation procedures using a range of fully integrated Microsoft Sentinel Playbooks (e.g., quarantine devices) powered by Tanium. These Playbooks can be executed at scale to resolve incidents when the shortest time to resolution is mission-critical.

> "I think the ability to bring in Tanium's real-time visibility and data into Microsoft Sentinel is powerful. The visibility I get across my entire IT estate is unprecedented. When I imagine having Tanium's integration with Microsoft Sentinel for the next Log4J type incident, I will have rich, real-time data directly from the endpoint to help me investigate, identify, triage, and remediate threats and quickly stop active exploits, all without leaving the Sentinel console."

Mark Wantling
CIO, University of Salford

Together, Tanium's real-time data and distributed architecture coupled with Microsoft Sentinel transforms security leaders' and practitioners' abilities to secure and perform incident response.



Use case	Solution	Benefit
Equip analysts with real-time endpoint data	With Tanium and Microsoft Sentinel, customers will be able to take advantage of Tanium's linear chain technology to bring rich real-time endpoint configuration and state data directly into their investigation processes.	Reduces the time it takes to assess an attack's impact on organizational endpoints and complete investigations procedures.
Expedite your investigations	Tanium and Microsoft solutions work together to drive expedited investigations and stop attacks before additional damage can be done. Analysts using Microsoft Sentinel will be able to more quickly investigate attacks using Tanium-powered Playbooks that have been integrated directly into the Microsoft Sentinel user experience.	Investigate incidents using a broader range of fully integrated automation that will help you complete investigations more quickly and accurately.
Real-time remediation	Customers using the integrated solution can execute Tanium remediation actions directly from the Microsoft Sentinel console using Tanium-powered Playbooks (e.g., quarantine devices) at scale.	Reduce the time it takes to stop attacks and bring the environment back to a complaint and healthy state.
Reduce console switching between solutions	Tanium and Microsoft Sentinel are integrated in a way that enables Microsoft Sentinel to remain the primary experience for incident response. Tanium's investigation and response capabilities are fully integrated into the Microsoft Sentinel console experiences.	With less switching between product consoles analysts can more quickly and accurately perform incident response from within Microsoft Sentinel.

SEE TANIUM IN ACTION

Experience visibility, control and trust on the industry's only Converged Endpoint Management (XEM) Platform.

Schedule a demo Learn about our Microsoft partnership →

Tanium, the industry's only provider of Converged Endpoint Management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. Visit us at www.tanium.com.