Tanium's integration with Azure Active Directory enables enhanced conditional access and simplifies Zero Trust

Member of
Microsoft Intelligent Security Association
Microsoft

Implementing Zero Trust without the right tools is challenging

To manage today's increasingly distributed environments, many IT leaders are evaluating Zero Trust strategies that conditionally grant access to applications or services based on an endpoint's user and device risk. But while denying access to a device with compliance gaps or vulnerabilities sounds good in theory, IT leaders struggle with two key challenges: limited or stale data available to make conditional access decisions and the potential productivity impacts associated with denied access for users across an organization.

Tanium's integration with Azure Active Directory enables you to do it right

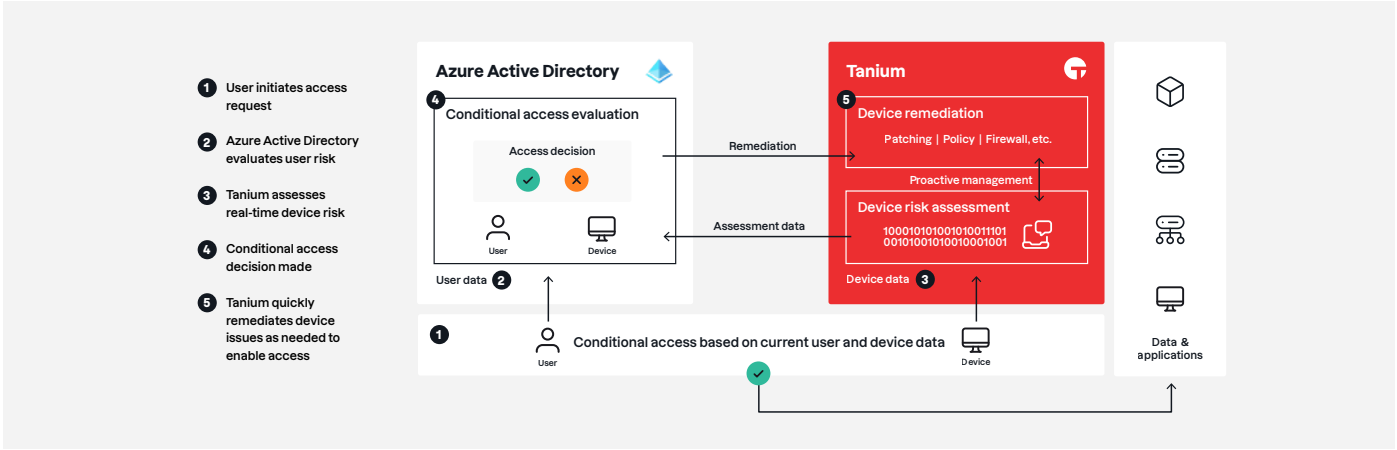
Tanium's Zero Trust with Azure AD now enables customers to update Azure AD Windows devices with custom Extension Attributes. The custom Extension Attributes are updated in real time and are created based on the complete data Tanium has about every Windows device. Customers are now able to enforce fine grained conditional access policies in Azure AD based on reliable data from fully customizable computer groups in Tanium.

Real-time device data

Through Tanium's integration with Azure Active Directory, IT leaders can make enhanced conditional access decisions based on an extensive, dynamic set of real-time device data from Tanium. By limiting or denying access to non-compliant or high-risk devices, Tanium and Microsoft deliver enhanced security across a minimized attack surface.

Real-time remediation

The integration also unlocks Zero Trust at scale for enterprises without significant productivity impacts. Customers can take advantage of Tanium's extensive remediation capabilities to quickly address a device's compliance or other security gaps and enable users to get back to work.



Leverage Tanium for the real-time data and remediation you need to deploy Zero Trust at scale while minimizing productivity impacts from denied application and data access.

Attack surface reduction takes on new meaning with Tanium

Blind spots hide sources of unknown risk. Leverage Tanium's distributed architecture to maintain full visibility and comprehensive management of your environment. Discover every endpoint, bring it under management, and eliminate threat vectors with unparalleled speed before an attack starts.

Proactive management of your estate reduces risk and complexity

With Tanium, configure policies, manage firewalls, deploy patches, enforce compliance, and more with unprecedented speed and at scale. Tanium gives you the ability to get ahead of risk rather than simply managing it.

Use cases

EVALUATE DEVICE RISK BASED ON A DYNAMIC SET OF REAL-TIME DATA

Leverage Tanium's rich real-time telemetry to assess compliance, identify vulnerabilities, verify MDE status, and more.

GRANT OR DENY ACCESS BASED ON BOTH MICROSOFT'S AND TANIUM'S RISK DATA

Base conditional access decisions on a combined assessment of both user and real-time device risk.

REMEDIATE DEVICE VULNERABILITY AND COMPLIANCE GAPS QUICKLY

Use Tanium's real-time distributed architecture to enforce policies, configure firewalls, deploy application or OS patches, and more.

COMPREHENSIVELY MANAGE ACROSS WINDOWS, LINUX, MAC

Extend your ability to deeply see and manage everything with a chip in it.

Microsoft + Tanium: Better Together

Together, Tanium and Microsoft transform your ability to manage and secure your entire digital estate no matter where it exists. Combining Tanium's real-time visibility and control with Microsoft's advanced threat intelligence, analytics, and orchestration capabilities reduces complexity and delivers an environment that is more secure, performant, and automated.

Learn more

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.