DATASHEET

Tanium & Microsoft Entra ID enable Zero-Trust conditional access

Unlock enhanced conditional access and Zero Trust at scale powered by the integration of Tanium's real-time data with Entra ID.

Build a Zero-Trust framework that minimizes the enterprise attack surface. Tanium Zero-Trust rules provide customized data to use in Entra ID conditional access policies.

Organizations can't implement an effective Zero-Trust architecture if they don't fully understand their environment.

To stay secure, today's distributed business models need to easily monitor and control all activities across the network for both users and endpoints. In the wake of hybrid workforces, the explosion of endpoint devices poses major challenges to Zero Trust integrations. A fundamental piece to Zero Trust is data, and organizations are struggling with the challenges of limited or outdated data, creating blind spots for unknown risk to impact the organization.

Conditional access policies enforce Zero Trust based on the user risk, device risk, location risk, type of application, sensitivity to data being accessed and other triggers. Zero-Trust security models are considered the best defense against threats, but it requires every user and device to be identified. To achieve this, organizations are finding themselves with a piecemeal approach to Zero Trust, resulting in gaps, tool sprawl, and long remediation times.

There is an easier way to implement Zero Trust with conditional access, and that's by the powerful integration of Tanium's real-time data with Entra ID (formerly Azure Active Directory)

Tanium and Entra ID provide a Zero Trust practice that reduces risk through continuous compliance where both the user and endpoint are validated.

REQUEST A DEMO TODAY

Try Tanium now.

Learn more

Grant access based on both Microsoft's user and Tanium's device risk data.

Base conditional access decisions on a combined assessment of both user and real-time device risk. This provides secure user access and the ability to create customized endpoint posture checks as a pre-requisite for access.

Evaluate device risk based on dynamic set of real-time data

Leverage Tanium's rich real-time telemetry to assess compliance, identify vulnerabilities, verify MDE status, and more. This enhanced data protection means you can assess, report on, and enforce device configuration while closely monitoring configuration drift.

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. This will stop threats from penetrating the enterprise and allow for quick-deploy recovery actions, patches, or software updates to remediate vulnerabilities at any scale.

Simplify Zero Trust

Tanium's integration with Entra ID enables enhanced conditional access and Zero Trust at scale powered by Tanium's real-time visibility and control. This integration is an out-of-the-box solution, eliminating the need for sprawling security and management tools. Customers can maximize their budget by leveraging their MACC to purchase Tanium through the Azure Marketplace.

With Tanium's visibility to every endpoint, endpoint-focused, Zero-Trust conditional access can be done quickly without disrupting productivity and existing architecture.

Tanium works in the background to continuously monitor device health, checking whether it's patched, secure, compliant, and managed. When users log on to Entra ID, their endpoints are simultaneously checked by Tanium, so that the whole process is seamless to the end user.

The integration makes Zero Trust at scale possible for enterprises. Customers can take advantage of Tanium's extensive remediation capabilities to quickly address a device's compliance or other security gaps and allows organizations to focus on higher-priority work instead of tedious tasks.

The Tanium platform offers comprehensive IT operations and security management from a single agent. It delivers complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium XEM provides the visibility and control needed to help you continuously manage your organization's endpoint risk.