SOLUTION BRIEF

Tanium for Zero Trust

Why validating device posture is as essential as validating identity.

What is Zero Trust?

The concept of Zero Trust is simple: trust no user or device, and always verify. A successful Zero-Trust approach looks at three things:

- A user's credentials
- The data that person is trying to access
- The device (i.e., the endpoint) that person uses

By combining the principle of least privilege (POLP) with a modern approach of contextual access, multi-factor authentication (MFA) and network access, organizations can maintain a more agile security model that is right for a cloud and mobile-first era. The result is that organizations can reduce their attack surface, and ensure sensitive data only gets accessed by people that need it under approved, validated context, which reduces risk.

Device validation is key to a successful Zero Trust result

Traditional Zero Trust practices have focused on network access, and Identity and Access Management (IAM) through Single Sign On (SSO). But with remote work making up a larger portion of end-user access, device posture is increasingly important as devices act as the new perimeter in a perimeter-less world.

By adding a third leg to the stool — device validation, organizations can protect against stolen credentials or even a stolen device used for MFA to gain access to networks. But once in the network, if the environment is monitored for noncompliance, or critical vulnerabilities, then securing the device is the last defense to having compromised sensitive data or worse.

That's why it's pivotal to practice converged endpoint management as the third piece to your Zero-Trust approach.

Seamlessly validate device posture at scale

Tanium provides real-time visibility and control of the new perimeter — your endpoints. Without real-time and accurate endpoint data at scale, your organization can't enforce compliance, or validate device posture as a prerequisite for access. Authentication alone can't look at the device to make sure it's secured, and because you can't have a user accessing your system without a device, you can't secure one without securing the other.

With Tanium, you can continuously check your device posture against policies to have certainty that your Zero Trust approach trusts no one, even after your identity and access policies are in place.

And with Tanium's platform capabilities, organizations can integrate with the Zero Trust tools they already use.

Components of a Zero Trust practice

Device compliance monitoring, and enforcement

Confirms the security posture of the device and gives IT teams the control to take action if something isn't right.

Identity and Access Management (IAM)

Authentication checks confirm an individual's identity and compare their access against role-based rules.

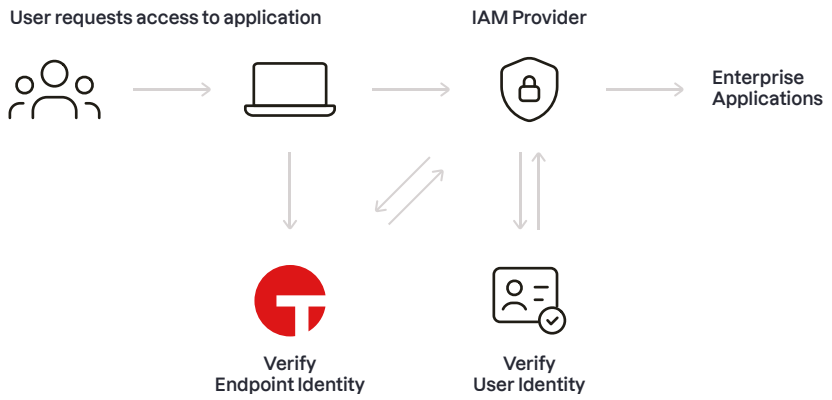
Network access

Organizations can control access to resources and network segments based on the user's persona and device being used.

Learn more about how Tanium can support device validation along with your Zero Trust practice

Benefits of a Zero Trust practice with Tanium

- Get visibility into all your endpoints, and know what's connected to your environment at all times.
- Have a single source of truth for endpoint data at scale in minutes.
- Reduce your attack surface by closing entry points into systems that store valuable data.
- Validate device posture as a prerequisite for access.
- Practice continuous compliance with confidence that policies are being enforced, and have control to diagnose and fix issues as they arise.
- Locate sensitive data and prevent it from being exfiltrated.
- Have the control to take action and respond quickly if something doesn't look right.
- Integrate with tools you already use for your Zero Trust practice with Tanium's API.
- Get real-time insight into your risk profile with risk dashboards that show a risk score for the systems your users and data are interacting with.
- Create a baseline for setting up a Zero Trust approach with full visibility into asset utilization, so you can design an approach that meets the needs of your employees.



If you aren't including device posture in your Zero Trust approach, your organization isn't fully managing risk.

To stay secure, today's distributed organizations need to easily monitor and control all activities across their environment for both users and endpoints. This requires a seamless security model designed for the new reality of remote work, cloud services, and mobile communications. Zero Trust was created for this new reality. And the key to making Zero-Trust security work at scale is endpoint visibility.

To learn how Tanium's Converged Endpoint Management platform can support a robust Zero Trust practice, visit **explore.tanium.com/zero-trust**.

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. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.