Tanium for Zero Trust

Your Trusted Partner in the Journey

What is Zero Trust?

Zero Trust is a simple idea: trust no user or device, and always verify. By combining the principle of least privilege (POLP) with the modern approach of contextual access, multi-factor authentication (MFA) and micro-segmentation, organizations can maintain a more agile security model that is right for a cloud and mobile-first era, while also ensuring that not only are the benefits of POLP recognized, but that sensitive data is only accessed under approved, validated context.

To put it another way, a Zero Trust approach looks not just at the user's credentials, and the data that person is trying to access, but also the device (i.e., the endpoint) that person is using.

Migrating to Zero Trust

Most organizations don't get to start with a Zero Trust architecture (ZTA), they must migrate there over time. NIST Special Publication 800-207 provides a migration approach, and here's how Tanium can assist with several of the recommended steps:

1. Identify Actors on the Enterprise: **IMPACT** provides a visualization of the trusts and permissions granted to users and assets in an active directory environment. Taking control of these relationships is key to reducing lateral movement potential. It also provides a spring-board to ZT planning by identifying users, accounts and assets that should be required to meet more stringent requirements for privileged access.
2. Identify Assets Owned by the Enterprise: Per NIST, one of the key requirements of ZTA is the ability to identify and manage devices. **DISCOVER** provides visibility of managed and unmanaged assets connected to the enterprise. Gaining visibility of unmanaged assets is a challenge for many organizations - we routinely find 15-20% of an organization's assets are unknown, unmonitored and unmanaged. **ASSET** not only maintains an inventory of online and offline endpoints, it can also be used to associate data with "shadow IT," approved BYOD items and other endpoints that may connect to enterprise resources yet are managed differently than core enterprise assets. **ENFORCE** ensures security policies remain applied to domain-connected as well as non-domain-joined assets. Tanium's core strength is its ability to provide visibility and control of connected and mobile assets at the speed and scale required to meet the real-time evaluations required for an effective ZTA.
3. Formulating Policies for the ZTA Candidate: Understanding all the dependencies of any given workflow process is critical. Unfortunately, organizations are often surprised by unknown dependencies, even when undertaking planned maintenance actions. **MAP** provides an application service visualization from multiple points of view so that end-to-end service dependencies can be identified and included in ZT planning.

Zero Trust Imperatives

The NIST publication also highlights the absolute importance of continuous monitoring and general cyber hygiene for a successful ZTA. Tanium's proven ability to support multiple operating systems, geographically dispersed organizations and on-prem, in the cloud and as-a-service operating

©2021 Tanium. All rights reserved.

models at speeds and scales necessary to counter adversaries in today's contested cyber environment is the reason many of the world's most critical, demanding and targeted financial and government organizations rely on Tanium today. The flexibility of the platform and its cutting edge technology provide the foundation necessary to support the evolution of any organization's ZTA.

Most discussions of Zero Trust focus on user authentication - an important piece of the puzzle. But just as critical is the endpoint. After all, a user may be legitimate, but what about the device they're using? Has it been compromised without their knowledge?

Endpoint security is a growing concern in the context of mass remote employees working on personal devices. Organizations need to have confidence that these endpoints haven't been hijacked due to poor IT hygiene. This is the value that Tanium's Endpoint Identity brings to the ZTA for federal organizations.

Tanium's Endpoint Identity

With Endpoint Identity, you can integrate Tanium with Identity and Access Management (IAM) vendors to verify that devices connecting to your cloud applications and zero trust networks are managed and secure.

While employees typically access cloud applications from their company-provided computer, sometimes an employee might find a need to use another computer to log into cloud applications. For example, an employee has left their company-provided computer at home while visiting a relative, but an urgent work request comes up. They use their relative's unmanaged computer to try to log into the cloud application. When the employee attempts this login, the endpoint is checked against the known managed endpoints in Tanium. Because the employee is attempting to log in with an unmanaged computer, they are not allowed to access systems or applications with sensitive or proprietary company data. Tanium's approach to Zero Trust is context aware - meaning that all of the signals are combined and assessed against real-time data and threat intelligence - to create an accurate and comprehensive view and understanding of what's happening on the network at any particular moment.

Accelerating Your Journey

Thanks to Tanium and partners like Cloudflare and Google's BeyondCorp, the dream of an effective Zero Trust strategy is a reality. Tanium provides the real-time visibility and control necessary for managing Zero Trust on your endpoints. Cloudflare provides the platform for easily screening devices for threats before granting access and Google's BeyondCorp provides secure remote network access without VPNs. With all three of these capabilities in place, any organization can accelerate their adoption of the new era of Zero Trust security.

Key Take-Aways

Tanium is the ideal partner for your Zero Trust journey. It provides:

- Real-time visibility of your assets, both on-net and off-net
- Visibility of the dependencies between assets, applications and services
- Visibility of the trusts and permissions granted to users and assets in an active directory environment
- Assurance that enterprise security policies remain applied to endpoints, whether they are domain-joined or mobile
- Improved general cyber hygiene and visibility of network-connected devices

Above all, Tanium remains the most flexible platform in your inventory, supporting multiple operating systems (Windows, Linux, Mac and more), operator-developed content and on-prem, in the cloud or as-a-service delivery models.

About Us

Tanium offers an endpoint management and security platform that is built for the world's most demanding IT environments. Many of the world's largest and most sophisticated organizations — including nearly half of the Fortune 100, top retailers and financial institutions, and multiple branches of the U.S. Armed Forces — rely on Tanium to make confident decisions, operate efficiently, and remain resilient against disruption. Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

©2021 Tanium. All rights reserved.