TANIUM

WHITEPAPER

What is Zero Trust?

How securing the endpoint is a pivotal piece of the puzzle to a successful Zero-Trust strategy.

Contents

What is Zero Trust?

Zero Trust is a simple idea: Trust no user or device. And always verify.

Enterprises today are operating in a hostile environment. Study after study shows that the weakest link to an organization's cyber defenses is its people. It's easy to get fooled by phishing, and when all other defenses fail, it's the user and the device that need to be verified.

Zero-Trust security assumes no device or user can be trusted without verification. In a world where remote work is more common than it once was, the idea of a perimeter — the castle-and-moat approach to security — is long past its "use by" date. The endpoint is the new perimeter, and organizations should not automatically trust any device.

The practice of Zero Trust was made for this new reality, and the key to making Zero-Trust security work at scale is device visibility and posture.

Zero Trust is a solution, not a product

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?

An effective Zero-Trust approach will look not just at the user's credentials and the data that person is trying to access, but also at the device (i.e., the endpoint) that person is using.

In an era where 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 aren't vulnerable due to poor IT hygiene. A critical component of this is having accurate and real-time visibility into the endpoint, device, and user data.

NIST Special Publication 800-207 highlights the absolute importance of continuous monitoring and general cyber hygiene for a successful Zero-Trust approach.

Organizations need to be able to answer the following questions:

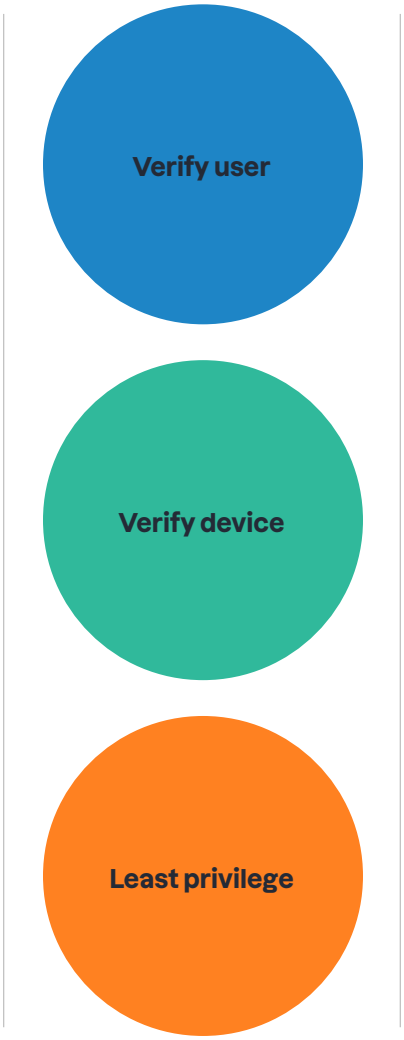
- How many unmanaged, under-managed, and managed assets do we have? Which operating systems are they?
- How many of those systems are out of compliance? Do we have a method to quickly bring those systems back into compliance?
- How many low, medium, and high vulnerabilities are present in our environment? How many of those vulnerabilities are exploitable?
- Do we have security controls in place to protect against these exploitable vulnerabilities? What about common security controls?
- Do we have standard operating procedures in place to handle security and operations workflows?

The endpoint is the new perimeter

A Zero-Trust practice requires users to validate their identity with multi-factor authentication (MFA). Once verified, users are then provided access only to the specific resources they need. A Zero-Trust model also applies micro-segmentation to break a network into smaller security zones, restricting lateral movement.

These safeguards are essential, but without endpoint visibility and proper hygiene, devices at the network edge can remain critically exposed to threats via unpatched vulnerabilities and insecure configuration settings.

Alongside user authentication, organizations must have the means to check endpoint "identity" by confirming the security status of remote machines. What if a user is accessing the organization's network from a personal computer at home that hasn't been patched in months or years? What if that endpoint has been compromised?



Tanium brings the perspective of the endpoint to Zero Trust

With the Tanium Converged Endpoint Management (XEM) platform, you can infuse device-posture checks with your Identity and Access Management (IAM) provider 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 enterprise-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 enterprise-provided computer at home while visiting a relative, but an urgent work request comes up. They log on to their cloud applications via their relative's unmanaged computer.

With Tanium, when the employee attempts this login, the endpoint is checked against the known managed endpoints. 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 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.

THE STEPS TO A ZERO TRUST STRATEGY

Identify attack opening and protect surface

Identify communication path

Design and implement Zero-Trust architecture

Monitor and maintain

Tanium solutions for a Zero-Trust strategy

In addition to – and working in conjunction with – your IAM, Tanium provides a variety of capabilities that aid in Zero Trust planning and execution.

Tanium Endpoint Management:

- 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 that 15–20% of an organization's assets are unknown, unmonitored, and unmanaged.
- Discover your "shadow IT", approved "bring your own devices". and other endpoints that may connect to enterprise resources yet are managed differently than core enterprise assets.
- Provides an application service visualization from multiple points of view so that end-to-end service dependencies can be identified and included in Zero Trust planning.

Tanium Incident Response:

- Enables security teams to detect, investigate, and remediate incidents. 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 Zero-Trust architecture.
- Provides a visualization of the trust and permissions granted to users and assets in an active directory environment. Taking control of these relationships is key to reducing lateral movement potential.
- Gives a springboard to Zero Trust planning by identifying users, accounts, and assets that should be required to meet more stringent requirements for privileged access.

Tanium Risk & Compliance:

- Conducts vulnerability and compliance assessments against operating systems, applications, and security configurations and policies.
- It provides the data necessary to help eliminate security exposures, improve overall IT hygiene, and simplify preparation for audits.
- Prevents security breaches by keeping endpoints up to date with the latest patches.

Tanium Digital Employee Experience (DEX):

The Tanium Digital Employee Experience (DEX) solution helps organizations diagnose performance issues on the endpoint, with options for employee self-help remediation.

A Zero-Trust practice weaves throughout these areas to create a robust security architecture because you cannot implement an effective security architecture if you do not fully understand your environment. Every component supports the functions of the other component and ultimately supports a Zero-Trust implementation.

Conclusion

Where once there was a clear model for network security — when you knew who you were physically letting in the building — today, things are more complex. To stay secure, distributed organizations need to easily monitor and control all activities across the network for both users and endpoints. Organizations need a seamless security model designed for the new reality of remote work, cloud services, and mobile communications. Zero Trust was made for this new reality, and the key to making Zero-Trust security work at scale is endpoint visibility and hygiene.

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

- Real-time visibility of your assets, both on-network and off-network.
- 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.

With Converged Endpoint Management, you'll have the information you need on a device posture, the ability to remediate any issues, and plug into your existing IAM solution to ensure your users and devices are verified before accessing important organizational systems. You can do this across multiple operating systems(Windows, Linux, Mac, and more).

Learn more about how Tanium can help you get visibility, control, and the ability to remediate issues with your endpoints at scale — all things that are pivotal for adopting a winning Zero-Trust strategy.

Reach out at www.tanium.com.