TANIUM | aws

EBOOK

What is Zero Trust?

How securing the endpoint is a pivotal piece of the puzzle to a successful unified Zero Trust strategy and approach with Tanium and AWS

CONTENTS

Introduction 3

What is Zero Trust? 4

The endpoint is the new perimeter 5

Tanium solutions for a Zero Trust strategy 6

A unified platform for Zero Trust provided by Tanium and AWS 8

The Tanium and AWS approach at work 9

Use the right partner on your Zero Trust journey 10

Introduction

Zero Trust is a simple idea: trust no user or device and always verify. To put it another way, don't trust anything. No individual. No endpoint. No application. No network.

Zero Trust is prompting enterprises to take into account identity, authentication, and visibility into other context indicators such as endpoint access and device state and health – to make real and meaningful security improvements over the status quo.

In this ebook, we define Zero Trust, what it is and what it is not, and explain it in the context of securing endpoints as part of a unified solution from Tanium and Amazon Web Services (AWS).

What is Zero Trust?

Zero Trust security assumes no device or user can be trusted without verification. Organizations should not automatically trust anything inside or outside their perimeters. In fact, 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. Zero Trust was made for this new reality. And the key to making Zero Trust security work at scale is a focus on endpoint visibility as part of an integrated, holistic approach to defending your cloud, assets, and workloads.

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 the device (i.e. the endpoint) that person is using. In an era where endpoint security is increasingly emphasized in the context of mass remote employees working on personal devices, organizations need to have confidence that these endpoints are protected. A critical component to 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 you have?
  What operating systems are they?
- How many of those systems are out of compliance?
  Do you have a method to quickly bring those systems back into compliance?
- Is there anything exploitable in your environment?
- Do you have security controls in place to eliminate unauthorized access?
  What about common security controls?
- Do you have policies or standard operating procedures in place to handle security and operations workflows?

The endpoint is the new perimeter

Zero Trust security requires users to prove who they say they are with multi-factor authentication (MFA). Once identified and 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. This is all great, but without endpoint visibility, you can miss areas where devices at the network edge are accessible by unauthorized users. 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 your organization's network from a personal computer at home that hasn't been patched in four years?

What if that endpoint has been compromised?

Tanium brings the perspective of the endpoint to Zero Trust

With Tanium 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 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 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. In addition to and working in conjunction with Endpoint Identity, Tanium provides a variety of capabilities that aid in Zero Trust planning and execution.

Tanium solutions for a Zero Trust strategy

Tanium Threat Hunting

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 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 springboard to Zero Trust planning by identifying users, accounts and assets that should be required to meet more stringent requirements for privileged access.

Tanium Asset Discovery & Inventory and Tanium Client Management solutions

Provides visibility of managed and unmanaged assets connected to the enterprise. Gaining visibility of unmanaged assets is a challenge for many organizations — often 15–20% of an organization's assets are unknown, unmonitored, and unmanaged.

Maintains an inventory of online and offline endpoints, and also can 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.

Visualizations of application service from multiple points of view so that end-to-end service dependencies can be identified and included in Zero Trust planning.

Tanium Risk & Compliance Management

- 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.

Zero Trust builds on these areas to create a robust security architecture because you cannot implement an effective security architecture if you do not fully understand your environment.

If you do not have an effective Compliance Management program it is difficult to determine what systems are allowed to communicate over certain ports and protocols. A unified platform approach to Zero Trust delivered by Tanium and AWS can help. In this approach, every component supports the functions of the other component and ultimately supports a Zero Trust implementation.

A unified platform for Zero Trust provided by Tanium and AWS

Zero Trust may be a simple term, but its implementation and management are a bit more complicated. The good news is that you can reduce the complexity of managing Zero Trust. Tanium and AWS provide a unified, managed approach to Zero Trust. Endpoints, identities, threat hunting, asset discovery, risk and compliance management, and security operations are managed with one platform, one agent, and zero infrastructure.

For example

AWS IAM authorization enables you to create identity controls. You can author standard IAM policies that define who can call your API and where they can call it from. Network-centric tools from AWS provide highly dynamic, software-defined network micro-perimeters. These make excellent guardrails for your identity controls. Add converged endpoint management from Tanium, and you can manage, inventory, monitor, contextualize, and remediate end-user and server, on-premises, cloud, remote, physical, and virtual endpoints with real-time visibility and control.

The Tanium and AWS unified platform approach is extensible and flexible, adapting easily to new incidents and issues. It provides a single view of all cloud, server, and user endpoints. One endpoint agent for integrated management and security fortifies endpoints against unauthorized access. You can discover managed and unmanaged assets as well as multi-tier application services to provide a complete inventory of what needs least-privileged access or changes to access configurations. If there are access events, you can respond quickly to prevent productivity disruptions.

Together, Tanium and AWS offer speed, scalability, reliability, and efficiency. You can deploy in hours—not weeks or months—with pre-configured capabilities that deliver value from day one. If the environments you are managing grow, the platform grows with them, folding in new endpoints as they are connected to the network. You gain confidence in the timeliness and completeness of your endpoint data by gathering it in real-time, even if it was previously unseen. You can also replace the hundreds of servers (or more) that legacy systems require with a single instance.

The Tanium and AWS approach at work

To create a unified platform for Zero Trust, Tanium's endpoint management and security platform is managed and delivered from AWS. Critical IT operations, risk, and security solutions are ready to go, all with zero infrastructure. Unlike legacy on-premises solutions, supporting a massively distributed workforce with Tanium on AWS has little effect on the processes of managing and provisioning servers. It eliminates the burden of updating, maintaining, and configuring these capabilities. More specifically, you can use the platform approach to address three of the common Zero Trust use cases identified by AWS.

Machine-to-machine

This use case requires the authorization of special flows between physical assets to eliminate unnecessary lateral network mobility. Tanium offers the communications framework that allows for real-time communication between a management server and any number of machine endpoints.

Human-to-application

For this use case, friction-free access to internal applications is enabled for your workforce. AWS services control application access, deliver strong user and device authentication, and apply modern identity standards. Tanium provides specific levels of access based on the endpoint a human is using for an application.

Software-to-software

When software deployments don't need to communicate, they should not be able to, even if they are in the same network segment. Similar to the machine-to-machine use case, Tanium can enable you to authorize specific flows between the software and eliminate unnecessary communication pathways.

With Tanium and AWS, you can create a flexible, identity-aware network that strengthens your security posture, eliminates unneeded pathways to data, and provides straightforward outer security guardrails. With the Tanium and AWS approach, you can apply Zero Trust concepts continuously to make meaningful security improvements over time.

The AWS Perspective on Zero Trust

AWS infrastructure aligns with the National Institute of Standards and Technology (NIST) 800-207 Zero Trust Architecture. These principles were built into the foundation of AWS infrastructure since its earliest days. AWS provides Zero Trust building blocks that work with solutions from AWS Partners like Tanium to help you achieve your unique Zero Trust goals. So regardless of the progress your organization has made toward Zero Trust, AWS can help you further your journey.

Use the right partner on your Zero Trust journey

The security landscape continues to change. Where once there was a clear model for network security — when you knew who you were letting in — today, things are more complex. To stay secure, today's 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.

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
- Improved general cyber hygiene and visibility of network connected devices

And when Tanium runs on AWS, you can simplify Zero Trust with:

- Unified endpoint management: In one platform, you can manage, inventory, monitor, contextualize, and remediate end-user and server, on-premises, cloud, remote, physical, and virtual endpoints with ultimate visibility and control.
- Unified endpoint security: No matter the size of your organization, with Tanium and AWS, you can identify and protect managed and unmanaged devices, and detect, respond to, and recover from threats and breaches.

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

Learn more about how Tanium can help you get visibility, control, and a single source of truth of your asset data at scale — all of which are pivotal for adopting a Zero Trust strategy in your organization.

Reach out

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 and follow us on LinkedIn and Twitter.

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 200 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

Learn more at aws.amazon.com.