Tanium Architecture

Tanium Architecture Overview

Tanium's patented endpoint communications architecture provides quick visibility and control across every endpoint on the network, and can easily scale to millions of endpoints without requiring additional infrastructure.

At a Glance

Patented communications architecture that is faster and more reliable than current approaches.

Leverages the speed of LAN and reduces the reliance on congested WAN.

Maintains performance without additional hardware investments.

Navigates around offline clients or network blockages to maintain high availability.

Zone servers enable all roaming clients to stay connected with Tanium.

You can't solve today's problems with yesterday's tools

The proliferation of cloud computing, virtualization, and mobility has reshaped how the endpoint is defined. Enterprise IT organizations are now expected to precisely manage, inventory, and distribute software and patches for hundreds of thousands of endpoints. Security teams are similarly tasked with the daunting challenge of combating increasingly elusive, efficient, and erratic cyber attacks across these expansive and complex environments.

Legacy security and systems management tools, designed with outdated notions and purposes, all share a common fatal flaw—they were simply not architected to perform well at scales beyond tens of thousands of endpoints. Using conventional hierarchical communications topologies (i.e. hub-and-spoke models), they are overly reliant on slow WAN traffic, suffer from bottlenecked databases and often require hundreds of supporting servers to scale. These tools inevitably become sluggish, unreliable, and costly to maintain as enterprise networks grow.

As a result, IT operations teams now need days or even weeks to fully deploy critical patches. Similarly, security teams are completely defenseless against advanced malware at scale, because primitive signature-based prevention or forensics approaches lack the sophistication and speed necessary to stop attacks already underway. These antiquated tools have become a liability to security and operational efficiency, and are incapable of solving today's most pervasive problems.

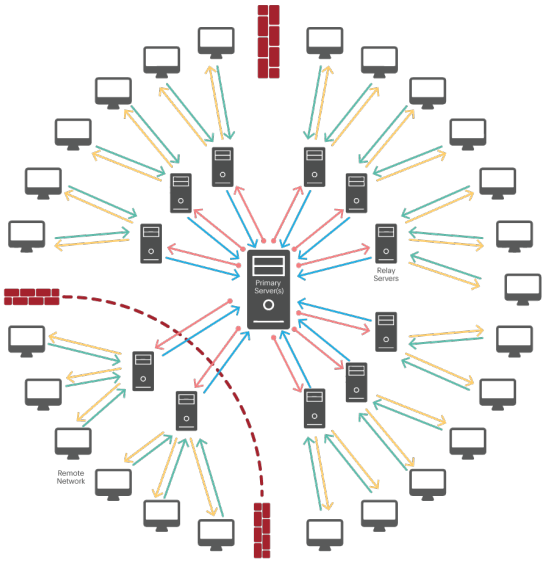
The Tanium architecture—our magic unveiled

Tanium is the first and only enterprise platform that empowers security and IT operations teams with quick visibility and control to secure and manage every endpoint, even across the largest global networks. At the heart of this platform is Tanium's patented linear-chain architecture.

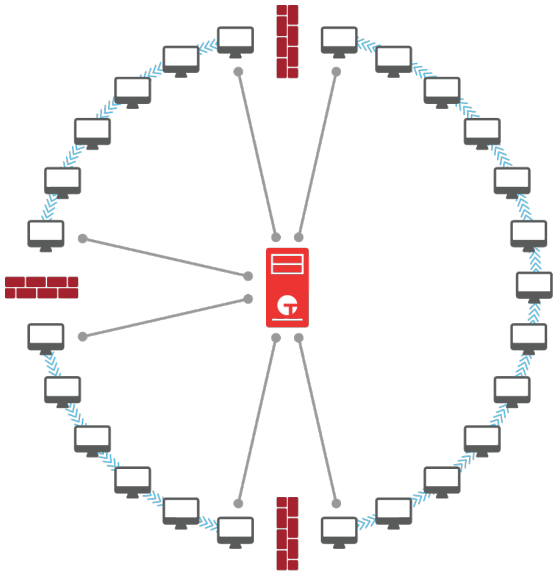
Tanium transcends the inherent limitations of hub-and-spoke architectures by decentralizing management intelligence directly onto individual endpoints through a single, lightweight agent. Each managed endpoint maintains an awareness of nearby machines on the network by contacting the Tanium Server periodically to get a concise update on the current state of its neighbors.

This simple interaction automatically pairs each endpoint with the optimal client to receive information from , while then passing this information to a different endpoint. Therefore, this process deliberately forms a series of efficiently chained endpoints.

Traditional Hub & Spoke Architecture



Tanium's Architecture



To propagate queries or actions to every endpoint throughout the entire network, the server simply sends information to a small set of endpoints along these linear chains, and collects aggregated results back from the endpoints at the end of these chains. This innovative approach fundamentally resolves the most egregious shortcomings of hub-and-spoke architectures, and is the foundation for the unparalleled speed and scalability.

Updated Website Assets

By decentralizing data collection, aggregation, and distribution down to the endpoint, the Tanium Architecture harnesses the intrinsic speed of low-latency LAN traffic. This dramatically reduces direct client-to-server communications, effectively eliminating the crippling inefficiencies caused by bloated databases, overloaded connections, and heavy traffic across WAN segments. With Tanium, security incident response teams can confidently hunt and remediate advanced threats across millions of endpoints, and IT operations teams can accurately manage and inventory every single global asset within seconds.

The impact of scale

Unlike traditional tools that require dozens to hundreds of secondary servers to scale their infrastructure, the Tanium Architecture's streamlined communications allows it to effortlessly support millions of endpoints and maintain optimal performance, without the need for ongoing investments in costly hardware even as the network grows over time. With this breakthrough architecture, secondary relay, database, or distribution servers are no longer necessary at different bank branches, retail locations, or geographically dispersed corporate offices.

99+ percent response rates from endpoints. Every time.

Aside from its superiority in speed and scale, the Tanium Architecture is also resilient by design making it well-suited to withstand the effects of today's dynamic environments, in which machines constantly move between wireless access points and virtual machines come in and out of existence by the hundreds or thousands. Unlike hub-andspoke architectures, where a failed or otherwise unavailable relay server can prevent timely access to thousands of machines, endpoints within the Tanium Architecture are capable of navigating around offline clients or network blockages to preserve high availability throughout the system. This self-healing nature of the Tanium Architecture ensures security and IT operations teams will always have the most complete and accurate view of their entire environment.

Enterprise ready

Zone Servers enable every roaming machine, as long as they are connected to the internet, to stay in contact with the Tanium Platform, allowing them to answer any questions or perform targeted actions as if they were on the enterprise network.

- Kerberos-based authentication leverages existing Active Directory infrastructure, credentialing, and security policies.
- Role-based access control (RBAC) regulates access available to different users based on their job responsibility or authority. Users can be limited from asking questions, executing existing actions, authoring new actions, authoring sensors, creating users, or assigning management rights. RBAC can even be flexibly set to apply for just a select group of machines.
- 512-bit Elliptic Curve Cryptography is used for queries and actions distributed across the network to prevent man-in-the-middle attacks or other malicious behavior initiated by compromised endpoints.

About Us

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control and manage millions of endpoints across the enterprise within seconds. With theunprecedented speed, scale and simplicity of Tanium, security and IT operations teams now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of cost efficiency in IT operations

TANIUM