SOLUTION BRIEF

Tanium for Threat Hunting

Intelligent threat hunting for today’s reality

Threat hunting is no longer a nice-to-have solution. It’s a must-have in today’s reality. You need to be confident that you can answer the question, “Are we good?” and know you can report back on any endpoint, anywhere in the world, in seconds, to fix incidents and prevent them from happening again.

90%

Reduction in mean time to investigation.

99%

Coverage of your security tooling.

90%

Reduction in mean time to remediation.

Confidently answer the question, “Are we good?”

Finding and stopping threats is more challenging — and more important — than ever. The average cost of an incident is nearly $9 million and threat actors are constantly evolving their attacks to evade detection. To keep their organization safe, Chief Information Security Officers (CISOs) need some way to find threats hiding in their environment.

Unfortunately, most CISOs lack the tools to hunt for complex new threats. They typically use point solutions that can detect only known threats, or that apply simplistic machine learning to limited data sets. These solutions often fail to catch previously unknown threats, and they can’t respond to the threats they do find. The result:

- CISOs must prevent damaging attacks against their organization without knowing if threats already dwell inside their environment.
- Security teams must shift between 10 different tools — each with a conflicting view — to identify and prioritize threats.
- Incident response is delayed by false positives, lag between tools and internal disagreement — all while threats advance to their goals.

> “With Tanium, our cybersecurity team can remotely check any endpoint and invoke a response procedure if necessary. They can also check every additional endpoint, globally, to help ensure the threat has not spread. This entire process takes less than four hours.
>
> Global Luxury Retail Group

The solution: Tanium gives you an extensible and unified approach to Threat Hunting.

Maintain a complete, real-time picture of your environment so threats have nowhere to hide.

If you can’t see the threats in your environment, then you can’t stop them. Yet today’s diverse, dynamic and distributed endpoints create a complex environment where threats can easily hide for days, weeks, or months. But with Tanium, you can:

- Find every endpoint in your environment and know if they are local, remote, on premises or cloud.
- Identify active users, network connections and other threat data for each of your endpoints.
- Visualize lateral movement paths that attackers can follow to access valuable targets like Active Directory.
- Verify if policies are set on each of your endpoints and identify gaps in key controls.

Proactively hunt for known or unknown threats across your environment in seconds.

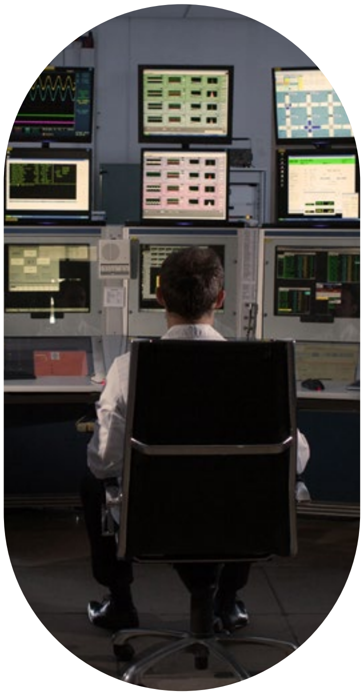
Once you can see your environment, it’s time to learn if there are threats already active in it. Attackers can dwell in your environment and evade detection by other endpoint tools for hundreds of days. But with Tanium, you can:

- Search for and discover new, unknown threats that signature-based endpoint tools miss.
- Hunt for threats directly on the endpoint, instead of through partial logs streamed to the cloud.
- Investigate either individual endpoints or your entire environment in minutes without creating large network strain.
- Determine the exact root cause of incidents you experience on any of your endpoints.

Respond to and eliminate any threats that you find within the same unified platform.

Finding a threat is not enough — you must eliminate it. Yet most endpoint tools separate threat hunting from remediation, which creates friction between teams, delays response and leaves threats active. But with Tanium, you can:

- Seamlessly pivot between threat hunting and response by giving teams a single dataset and platform.
- Rapidly apply defensive controls to any number of endpoints during an incident.
- Learn from incidents and harden your environment to prevent similar attacks.
- Simplify and streamline policy management to keep your endpoints in a “known good” state at all times.



Discover, investigate and eliminate threats across your entire environment.

Tanium provides a range of benefits that make threat hunting simple, flexible and accurate. With Tanium, you will:

Know everything now

Tanium tells you what assets you have, where they live, and what they are doing — giving your security teams a single source of real-time truth to rally around.
Tanium:

- Searches for arbitrary heuristics and indicators of compromise (IoCs) across your environment in seconds.
- Maps potential exploitation paths by endpoint name or user account.
- Visualizes access rights, registry settings, and asset dependencies and relationships.
- Shows you where your users have logged in and what they have done.
- Traces native artifacts back to the root cause of an incident.

Align teams

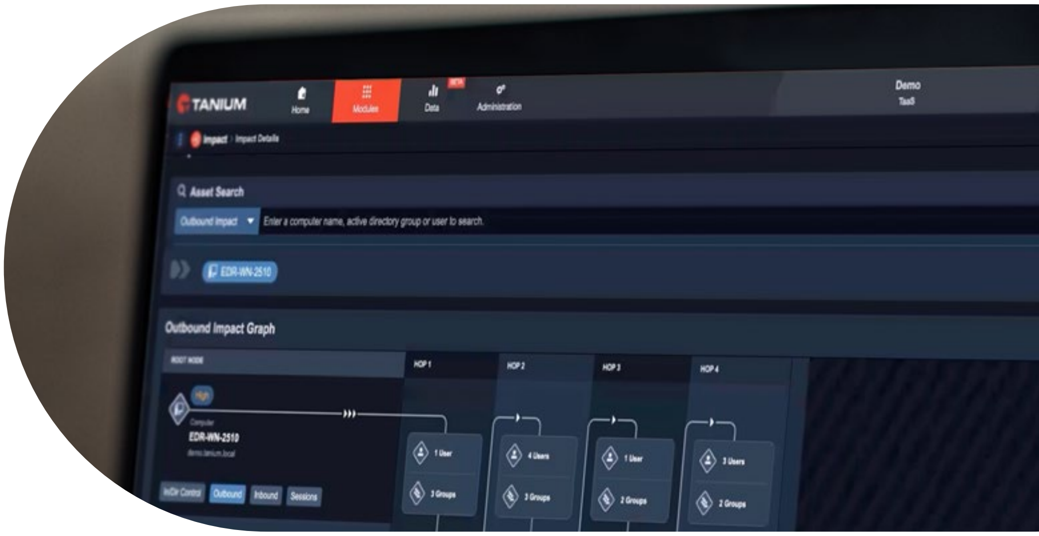
Tanium provides a single, unified platform that performs every task — from investigation to remediation — and replaces countless point tools and their costly infrastructure. Tanium:

- Unifies IT operations, security and risk teams under a single platform.
- Retrieves artifacts for your SOC & IR teams, and scopes lateral attack movement.
- Isolates and remediates compromised endpoints without losing operator context or depending on integrations.
- Validates the application of policy and controls and identifies gaps.
- Prevents the purchase of more tools and infrastructure.

Hunt threats anywhere

Tanium finds, scopes, traps, and eliminates threats anywhere in your environment, at any scale, within seconds — even threats that easily bypass traditional security tools. Tanium::

- Provides a flexible toolset to manage unknown attack patterns.
- Removes threats before they can attack without quarantining the endpoint.
- Specifies unique heuristics to set traps for attackers in your environment.
- Removes embedded threats instead of relying on rollbacks.
- Performs remote remediation actions like deleting files and managing native security controls like firewalls and antivirus.



How Tanium's Threat Hunting solution works

Threat Response

Proactively hunt for adversaries using arbitrary heuristics.

Impact

Quickly identify high-risk accounts and systems to reduce your attack surface.

Enforce

Push new policy rules and configurations to endpoints to stay ahead of vulnerabilities.

Schedule a demo of Tanium

Let us show you how Tanium's Threat Hunting solution provides a real-time view of your risk posture across your organization.

Request a demo

Tanium is the platform that organizations trust to gain visibility and control across all endpoints in on-premises, cloud and hybrid environments. Our approach addresses today's increasing IT challenges by delivering accurate, complete and up-to-date endpoint data — giving IT operations, security and risk teams confidence to quickly manage, secure and protect their networks at scale. Tanium's mission is to help see and control every endpoint, everywhere. That's the power of certainty.

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