DATA SHEET

# Tanium Threat Response

## End-to-end threat discovery, investigation,and resolution. In real time. At scale.

**You Can't Protect What You Can't See:**

94% of enterprises have endpoints they didn't know existed before implementing Tanium[1]

**Threats Still Bypass Modern Detection Tools:**

54% of incident victims were alerted by external sources[2]

**Disjointed Security Toolsets:**

On average, organizations have approximately 49 security tools within their environment[3]

Discover, investigate, and resolve security incidents with speed and certainty armed with access to comprehensive endpoint data, tailored threat intelligence, and complete control, all from a single platform.

### Stay prepared to respond with confidence when it matters most.

In high-impact incident and breach scenarios, time is of the essence. Lack of visibility into every endpoint and the inability to take control leaves teams scrambling, and delayed response times can keep organizations exposed to future events. Issues compound when multiple fragmented and disconnected point solutions are being used to piece together the necessary information to gain context to take the right actions. Security teams are left to operate with uncertainty, hindering their ability to swiftly lead response and recovery efforts.

With a comprehensive view of every endpoint in the environment, including immediate insights into the applications, users, files, processes, and more, security teams can make better decisions and confidently eliminate threats.

- Lack of real-time visibility into endpoints leaves blind spots
- Fragmented data from a collection of point solutions slows response times
- Lengthy recovery times leave organizations exposed

### Counter threats with unparalleled endpoint visibility and control, at scale, in real time

**Get complete data from every endpoint in real time**

Empower security teams with full visibility for improved threat context and accelerated response.

**Use insights to take actions that minimize impact**

Address threats head-on to safeguard endpoints and ensure operational resilience.

**Drive round-trip remediation platform for stronger resilience**

Enhance security posture by swiftly remediating threats that can cause crippling impacts.


**References:**

1. https://site.tanium.com/rs/790-QFJ-925/images/WP-Visibility-Gap-2020.pdf
2. https://services.google.com/fh/files/misc/m-trends-2024.pdf
3. https://www.idc.com/getdoc.jsp?containerId=US52023024

## Threat Response accelerates investigation and remediation – from hours or days – to minutes.

### Rapidly investigate threats across every endpoint

Instantly utilize current and historical endpoint data to assess the impact of an incident and activate response efforts.

- Monitor processes, file usage, IP addresses, and process hashes across all endpoints in both historical and real-time contexts. Visualize this data with a summary dashboard and access a searchable details grid for up-to-date information from each endpoint.
- Linear-Chain Architecture – fast visibility and control across every endpoint on the network.

### Proactively hunt for threats and indicators of compromise

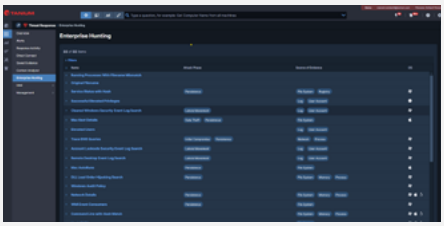
Proactively hunt for threats that have evaded existing security measures and other anomalies across all endpoints.

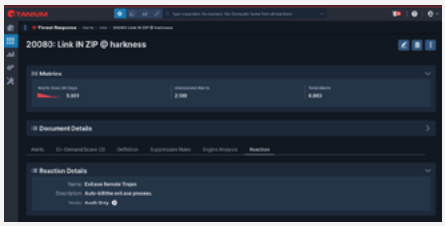
- Conduct proactive threat hunts across the entire environment to uncover threats that have eluded detection mechanisms. Promptly share detailed alerts with stakeholders upon detection of any unusual activity, facilitating swift response and mitigation efforts.
- Tailored Threat Intelligence – contextualized threat intelligence for current and emerging threats

### Completely mitigate and remediate incidents

Halt malicious activities to minimize impact and reinforce strong security hygiene.

- Mitigate the impact of threats by swiftly containing affected endpoints to prevent further propagation of compromise, data exfiltration, and lateral movement, then take full remediation actions to recover from the incident.
- Endpoint Reactions – immediate, automated responses to disrupt attacks and mitigate impact






**SEE TANIUM THREAT RESPONSE IN ACTION**

Schedule a live demo with a Tanium expert to see how you can streamline incident response and remediation.

**Schedule demo**

## Tanium Threat Response is a key component of Tanium's Converged Endpoint Management (XEM) platform

Tanium Converged Endpoint Management (XEM) platform offers round-trip endpoint security management with complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium XEM provides the visibility and control needed to help you continuously manage your organization's endpoint risk.

Tanium, the industry's only provider of Converge 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. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

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