




3 Steps to Accelerating Microsoft Defender for Endpoint with Tanium





Automated real-time visibility, control, and security for every endpoint, everywhere

The three main security challenges your organization likely faces today are poor visibility across your IT landscape, inadequate SecOps tooling, and lack of (or not enough) automation. Today's network environments are increasingly complex with millions of endpoints that now also include multiple cloud installations, containers, wearables, IoT devices – even drones — making it increasingly difficult to monitor and identify vulnerabilities.

And the number of those vulnerabilities has doubled, in some cases even tripled, in the last 12 months — stretching your security operations center (SOC) personnel and IT teams to their breaking point.¹ It's estimated that as many as 3,500 of your endpoints are unprotected — and that number increases as your organization scales.²

And even in the face of these growing demands, your teams are probably understaffed or have inexperienced members, and are dependent on threat detection solutions that can't deliver the insights you need for prompt action and correction. For robust threat management and resolution, your security team needs a modern AI-powered, cloud-based solution that delivers deep insights across your environment.

The solution: Tanium's real-time visibility and control over every endpoint – anywhere, paired with Microsoft Defender for Endpoint's (MDE) embedded behavioral sensors, cloud-based analytics, and real-time threat intelligence.

REFERENCES:

1. <https://www.nopsec.com/blog/state-of-vulnerability-management-6-key-takeaways/>
2. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us>



Tanium + Microsoft: Better together

Tanium and Microsoft empower more effective and resilient IT operations and security at scale by combining unprecedented analysis and automation with real-time visibility, control, and remediation.

What is Microsoft Defender for Endpoint?

Microsoft Defender for Endpoint (MDE) is a comprehensive enterprise endpoint security platform designed to help you prevent, detect, investigate, and respond to advanced threats across your enterprise network. Endpoint behavioral sensors, cloud security analytics, and threat intelligence are embedded in Windows 10 and Microsoft Cloud to deliver AI-powered security on millions of endpoints across Windows, macOS, Linux, Android, iOS, and IoT devices.

Key capabilities that go beyond traditional antivirus technologies include:

- Endpoint detection and response (EDR)
- Vulnerability management
- Attack surface reduction
- Next-generation protection
- Auto investigation and response
- Real-time detection of malware, polymorphic threats, and other malicious activity



100%

Endpoint visibility

99%

Vulnerability ID
and remediation

8x

Faster endpoint provision

What is Tanium?

Tanium is a modern, cloud-based endpoint management solution that provides visibility and control of every endpoint device — remote and on-premises. Tanium lets you perform rapid, scalable endpoint management across the entire lifecycle from a single, unified platform and console.

With Tanium, you can:

- Find every known and unknown endpoint connected to your network.
- Identify and remediate endpoint vulnerabilities at 99% efficacy.
- Provision new endpoints up to 8x faster.
- Patch and update hundreds of thousands of endpoints each day.

Tanium supports IT operations teams and SOC personnel efforts to deploy MDE quickly and effectively, ensuring it's deployed on every endpoint, running, and continuously updated and configured as desired. This out-of-the-box deployment provides monitoring and health reports for MDE agents, allowing you to change settings and configurations at scale.

With Tanium, you can:

- Monitor your Microsoft implementations across environments and seamlessly pivot from threat investigation to remediation — all from a single Tanium dashboard
- Detect and remediate vulnerabilities across millions of devices with speed and certainty
- Automate customizable remediation, including patching, compliance, app control, and quarantine (99% average compliance with Tanium³)
- Reduce tool sprawl and increase ROI with a single, integrated Microsoft and Tanium solution for IT operations and security
- Get end-to-end visibility across all endpoints — managed or unmanaged
- Investigate and remediate threats using real-time intelligence
- Keep MDE signatures and engine versions up to date
- Gain all the necessary context to investigate an incident without the extra cost of centrally storing every piece of data

REFERENCES:

3. <https://www.tanium.com/solutions/risk-and-compliance-management/>

How Tanium enhances Microsoft Defender for Endpoint

Tanium ensures your environment is ready for MDE deployment by providing comprehensive visibility to all endpoints – managed and unmanaged. Tanium's rich, real-time device data integrates with Microsoft Defender for Endpoint's logs and alerts, providing a powerful solution for end-to-end protection, detection, and investigation.

Tanium ensures MDE is deployed quickly and effectively managed across all environments – on-prem, hybrid, and multi-cloud – maximizing your Microsoft investment. Tanium enhances Microsoft's security offerings by providing comprehensive visibility and remediation capabilities in real time. It assures security and regulatory adherence throughout your entire network.

Four ways Tanium enhances MDE

1. Rapid deployment and management of MDE. Tanium can immediately discover assets across environments and operating systems so MDE can be deployed quickly and effectively on every endpoint and ensure it's running and up to date (even on non-domain or Azure AD joined/registered).

- Simplified and fast onboarding/agent deployment
- Manage agent configuration on Windows, macOS, and Linux
- MDE agent health monitoring and reporting

2. Manage MDE settings more effectively. Tanium provides a real-time control pane, allowing you to change and manage settings across the full scope of computers at speed and scale.

- Multi-platform configuration base evaluation
- Configuration quarantine options
- Virtually unlimited detection rule customizations

3. Accelerate identification of threats and endpoint vulnerabilities in real time. Leverage Tanium's rich, real-time data to identify and investigate vulnerabilities at scale. Integrations with MDE and Sentinel give you complete visibility across the entire environment to identify potential threats.

- Improve overall security with end-to-end visibility organization-wide
- Reduce mean time to respond (MTTR) and the risk of a breach
- Gain greater awareness to identify and respond to vulnerabilities

4. Consolidate point solutions. Tanium and Microsoft reduce complexity and manage risk with an integrated solution, reducing the load and number of agents required to manage all your endpoints. Consolidating your security vendors may help you reduce operational costs by up to 60 percent,⁴ making room in your budget for higher-priority needs.

REFERENCES:

4. <https://www.microsoft.com/en-us/security/business/security-101/what-is-soar>

Three steps to supercharging MDE with Tanium

Tanium supports the deployment and configuration of MDE by providing a comprehensive platform that simplifies the entire implementation process. It offers real-time data and controls, facilitating seamless integration and management of MDE across devices. With Tanium, organizations can streamline their endpoint security setup, effectively manage and automate workflows, and ensure consistent policy application during every stage of MDE deployment, from initial setup to ongoing management and response strategies. This integration ensures a fortified defense against threats and a more resilient IT environment.

Stage 1: Preparing for deployment

Tanium can immediately discover assets across environments and operating systems so MDE can be deployed quickly and effectively on every endpoint and ensure it's running and up to date (even on non-domain or Azure AD joined/registered).

Stage 2: Rapid deployment & management

Automatically deploy MDE quickly and effectively. With real-time visibility, Tanium can immediately discover assets across diverse environments and operating systems. Tanium's ability to find and take control of every endpoint in real-time allows MDE to be deployed quickly and effectively across all computers – even non-domain or Azure Active Directory joined/registered. Tanium ensures that MDE is deployed, running, and up to date on every endpoint.

Stage 3: Maintaining agent health

Tanium adds granular control over MDE settings. Tanium provides a real-time control pane, allowing you to change settings and manage configuration settings across the full scope of your environment – on-prem, hybrid, and multi-cloud – at speed and scale.

Conclusion

Leveraging Tanium alongside Microsoft Defender for Endpoint transforms cybersecurity practices. Tanium's real-time visibility and Microsoft's comprehensive security analytics ensure vulnerabilities are swiftly identified and addressed across all endpoints. This partnership provides a robust, scalable solution that automates the entire process, from deployment to continuous monitoring and management. Integrating these powerful tools fortifies your network's defense and streamlines your security operations, making the most of your IT investments and driving greater efficiency and protection throughout your organization.

Request a demo today

The Tanium platform offers comprehensive IT ops and security management from a single agent. It delivers complete, accurate, and real-time endpoint data – regardless of scale or complexity and with minimal infrastructure. Tanium XEM provides the visibility and control you need to continuously manage endpoint risk.

TRY TANIUM NOW

[See Tanium in Action →](#)

