SOLUTION BRIEF

Tanium Autonomous Endpoint Management (AEM)

Empowering organizations to efficiently mitigate risk while maintaining operational resiliency

Tanium AEM leverages real-time insights from Tanium cloud-managed endpoints to recommend and automate endpoint changes safely and at scale.

The increased frequency of OS and software updates from vendors, ongoing configuration drift on endpoints, and faster exploitation of vulnerabilities by attackers has made it difficult for IT and security teams to keep pace and maintain a secure, resilient, and compliant posture.

Tanium's patent-pending Autonomous Endpoint Management (AEM) is the next evolution of Tanium's converged endpoint management platform. Tanium AEM leverages AI/ML capabilities built into the platform to drive faster, better decision making and significant business outcomes for your organization.

By leveraging real-time data and analysis of cloud-managed endpoints, Tanium AEM recommends and automates routine tasks safely and reliably, ensuring operational health, reducing the business risk of negative IT outcomes, and enhancing the security of the IT environment.

Tanium AEM use cases

Improve IT availability by preventing disruptions when deploying endpoint changes

AEM provides confidence scores and automation rules that automatically deploy software packages, patches, and other changes. The Confidence Score gives you real-time context to how safe an update may be in your environment, based on data from millions of endpoints. The changes can then be managed through Tanium AEM deployment rings which phase changes to match your organization's change management process.

Proactively identify risks and operational items to improve operational health and security of the environment

Tanium Guide globally benchmarks and analyzes your dynamic IT environment in real-time to guide operators with recommendations that confidently lead your team towards the next best action and change to make to your endpoints.

For example, Tanium Guide may:

- Identify endpoints with out-of-date signatures for Microsoft Defender for Endpoint and provide a playbook to remediate it.
- Identify endpoints with increased risk scores beyond a specific threshold.

15 days

Industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery

3X

Vulnerability exploitation surged by nearly 3X (180%) in 2023

93%

93% of IT leaders indicate there is an overall skills gap in staff, which is inviting automation efforts

> "I highly recommend using Tanium Automate, especially for busy security teams that are trying to save time on manual, repetitive tasks like patching. Automate drastically simplifies security orchestration and gives you back countless hours to focus on deeper work."

David Anderson
Patch automation and vulnerability remediation lead, VFC

Scale IT and security operations in a cost-effective way

Tanium Automate provides built-in playbooks that your teams can use to capture operator expertise in reusable and repeatable with low and no-code custom playbooks that can combine both IT and security tasks from across the Tanium platform.

For example, Tanium Automate may:

- Scan all endpoints for software usage and use real-time data to determine least used licenses.
- Notify users that unused software has been scheduled for removal.
- Patch servers that are members of a cluster in a manner that ensures high availability is maintained during the end-to-end process.

Reduce time to remediate software vulnerabilities with lower business impact

Remediation Visibility, a new workflow in Tanium Comply, pivots directly from compliance findings to the remediation process to patch vulnerabilities to improve cross-team collaboration between security and IT Ops teams. Collaboration between these teams reduces risk when they have access to a unified data set, real-time reporting, and simplified workflows.

Proactively identify and remediate zero-day risks

Tanium Guardian publishes zero-day research which produces dynamic reports and guidance on where your IT environment is at risk from zero-day issues. Tanium Guardian works with Tanium AEM to provide proactive guidance on the implications of the remediation to endpoints so that your IT and security operations staff can intelligently evaluate the impact of the zero-day on business operations.

Instantly answer any question about endpoints

Tanium Ask uses the power of generative AI to enable everyone from the executive leadership to the operators to ask questions about endpoints that inform your operational and business decisions. Using Tanium's real-time visibility Tanium Ask provides you with rapid answers that reflect the current state of their environment.

For example, Tanium Ask may be used to ask questions such as:

- What is the average time to patch my machines?
- Are there any servers running into performance problems today?
- Which endpoints have unused Adobe Photoshop?
- What endpoints do I have that are missing critical patches that were released greater than 30 days ago?

Benefits of Tanium AEM

Tanium AEM revolutionizes decision-making and execution processes for IT and Security teams, ensuring safe and reliable changes across their environment, both at scale and in real-time.

Operational resilience: By deploying changes using insights from real-time analysis of changes to endpoints globally, combined with deployment rings and visibility to real-time impact of changes, IT teams can avoid costly disruptions that impact business and productivity.

Assured compliance: Continuous monitoring, industry benchmarking, and automated compliance checks support your organization in meeting regulatory requirements, reducing the risk of fines and legal issues.

Enhanced security posture: Proactive identification, prioritization, and remediation of cyber risks from vulnerabilities and configuration drifts help protect your organization from cyber threats – safeguarding sensitive data and maintaining customer trust.

Scaling IT and security: Automating routine tasks frees up staff to focus on strategic initiatives that drive business growth, optimizing the use of human resources.

Reduce IT support costs: Automatic resolution of several endpoint issues reduces IT and Security support overhead that can disrupt and impede employee productivity.

Increased IT agility: Automated processes and real-time data allow IT to quickly adapt and support evolving business needs.

REQUEST A DEMO TODAY

Connect with a member of our team to see Tanium in action.

Try Tanium AEM Now