TANIUM

Tanium Autonomous Endpoint Management (AEM)

Empowering organizations to efficiently mitigate risk while maintaining operational resiliency

SOLUTION BRIEF

Tanium AEM leverages real-time insights from all Tanium cloud-managed endpoints to recommend and automate changes on endpoints within a customer's environment in a safe, scalable way with its real-time platform. It empowers IT and Security teams to confidently and efficiently scale operations and improve the security posture of the environment.

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.

1. Increased cyberattacks demand faster patch deployment, better device configuration compliance and closer alignment with vendor life cycles to reduce vulnerabilities.
2. IT and security teams are stretched with constant upkeep of the environment, and have to undertake endpoint changes with limited visibility and understanding of the downstream impact, introducing operational risks.
3. Automation is inherently complex, requires highly skilled experts to build and without real-time data to inform it at runtime it can perform unreliably and cause disruption.

Tanium Autonomous Endpoint Management (AEM) is the next evolution of Tanium's converged endpoint management platform. Tanium AEM unlocks significant business value across Tanium's comprehensive suite of solutions, including asset discovery and inventory, vulnerability management, endpoint management, incident response, and digital employee experience. Tanium AEM leverages AI/ML capabilities built into the platform to drive faster, better decision making and significant business outcomes for customers.

Tanium AEM delivers significant increase in operational efficiency through automation of routine tasks that allow resources to be focused on growth initiatives, without compromising security, performance, or availability. In addition, through automation that's reliable and scalable, AEM improves customers' security posture and accelerates risk mitigation by proactively managing vulnerabilities and incidents.

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

90%

The probability of a vulnerability being exploited hits 90% between 40-60 days after discovery

Kenna Security

3x

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

Verizon

93%

93% if IT leaders indicate an overall skills gap in staff impacting automation efforts

CompTIA

Tanium AEM use cases

Improve IT availability by preventing disruptions when deploying endpoint changes

AEM provides confidence score and automation rules along with the software packages available via the Tanium Deploy gallery. The Confidence Score provides real-time context for how safe an update may be in the customer's environment, based on successes across the universe of Tanium cloud endpoints. The changes can then be managed through Tanium AEM deployment rings which phase changes to match the cadence of the business.

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

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

For example:

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

Scale IT and security operations in a cost-effective way

Tanium Automate can be used to capture operator expertise in reusable and repeatable with low and no code playbooks that can combine both IT and security tasks from across the Tanium platform.

For example:

1. 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
2. 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

The Remediation Visibility workflow pivots directly from compliance findings to the remediation process to patch vulnerabilities to improve cross team collaboration between security and IT Ops teams. Together they reduce risk based on a unified set of data, 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 a customer's 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 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 operational or business decisions. Using Tanium's real-time visibility Tanium Ask provides its users with instant answers that reflect the current state of their environment.

For example:

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

Tanium AEM platform foundations

Tanium AEM can analyze sensor trends, change impact and user usage patterns across millions of endpoints instantly to generate Real-time Cloud Intelligence that informs Tanium's autonomous functions.

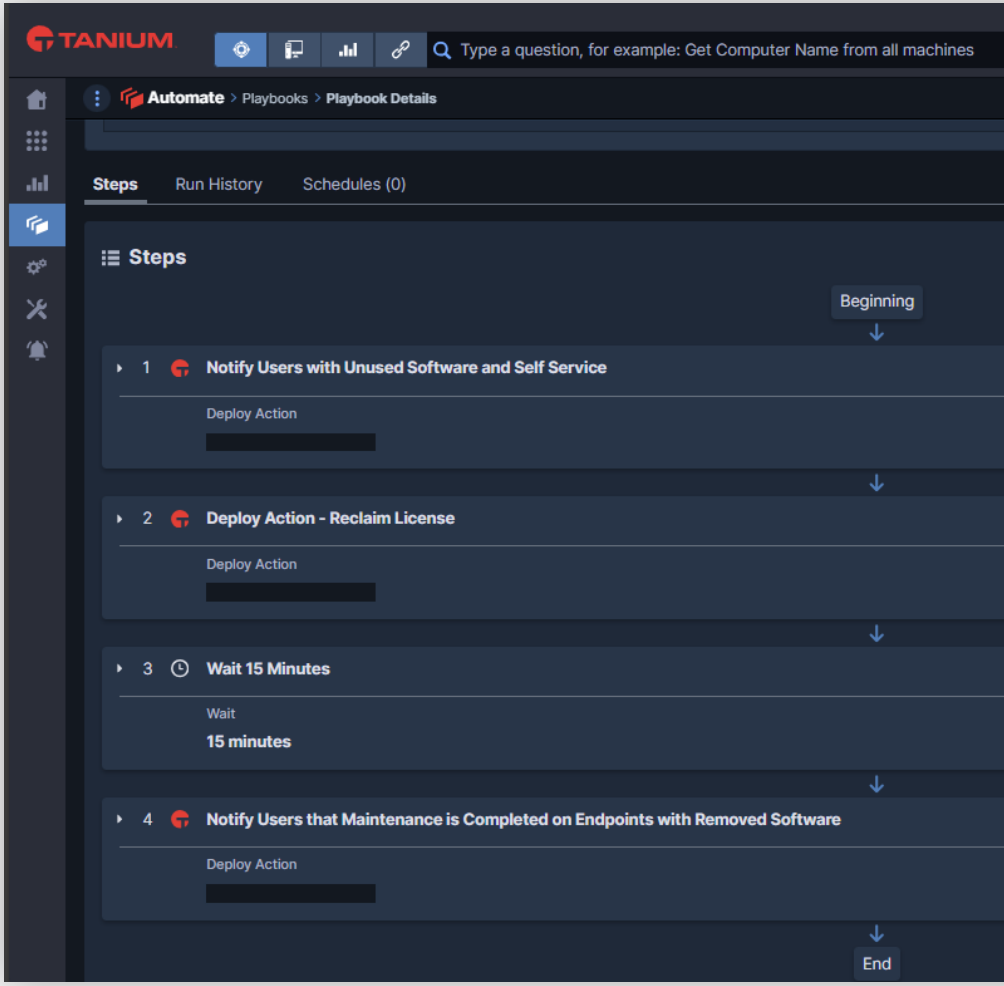
- Tanium uses a special cloud scale, multi-model stream processing architecture that can mix different analytical and AI models based on the insight needed
- Tanium AEM keeps improving and adjusting insights using its Using Real-time Cloud Intelligence which is informed by changing IT conditions and technologies

Real-time Cloud Intelligence doesn't have any user experience so we should use imagery that conveys this concept.

Tanium Automate simplifies IT and security task orchestration and automation, powered by real-time data and actionability.

Tanium Automate enables operators to automate complex tasks at speed and scale by replacing manual processes with easy-to-implement, no- to low-code orchestration and automation.

- Create playbooks with little to no code to automate common operations and security tasks
- Empower a broad range of authors with varying levels of technical skills to create powerful automation
- Define entrance, exit, and success criteria for each step before progressing to the next
- Maintain full visibility of actions, including historical audit logs, current playbook status, and future schedules
- Use Tanium APIs to run Automate playbooks via tools like ServiceNow or Microsoft security solutions

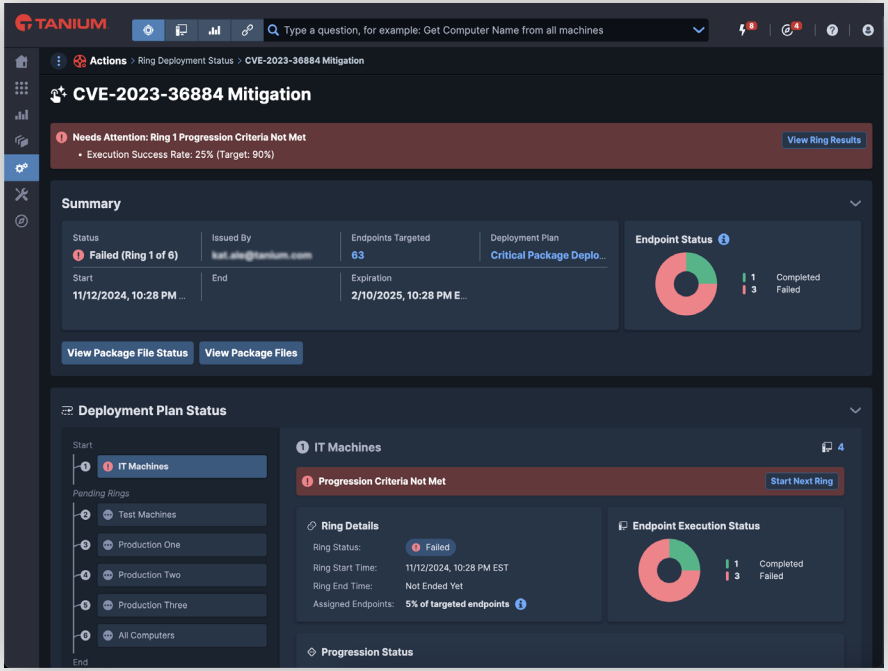


Tanium Automate

Deployment Templates and Rings minimize disruptions by rolling out changes to match the rhythm of the business.

When large scale changes to endpoints are needed Deployment Templates and Rings provide the ability to phase deployments out ensuring that they are well-managed and repeatable.

- Configure progression criteria leveraging real-time data to safely deploy changes across rings
- Take advantage of reusable deployment plans to consistently deliver changes
- Create custom deployment plans that are tailored to different levels of risk tolerance

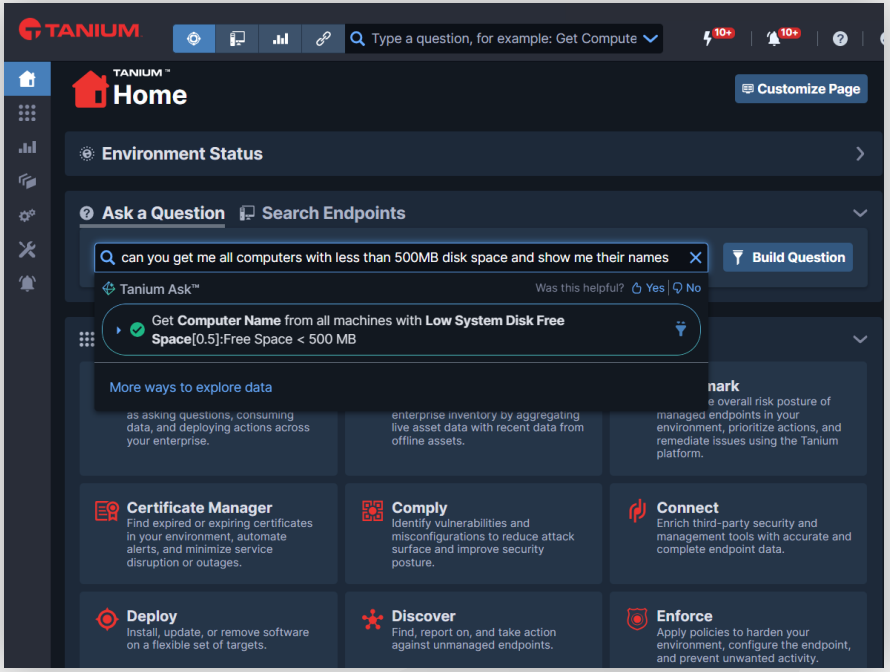


Deployment Templates and Rings

Tanium Ask empowers the entire team to get answers to even the most complex IT and Security questions.

Tanium Ask takes advantage of LLM AI to ensure that Tanium operators of any skill level can ask a question of their IT environment and get an answer back using real time data no matter the complexity of the question.

- Operators can easily ask questions using natural human language:
  "What is the average time to patch my machines? "
  "Are there any servers running into performance problems today? "
  "Which endpoints have unused Adobe Photoshop? "
- Further refine your Tanium Ask prompts with Tanium's Question Builder
- Get answers to questions in real-time no matter the scale of the environment
- Save your favorite Tanium Ask questions for use in the future



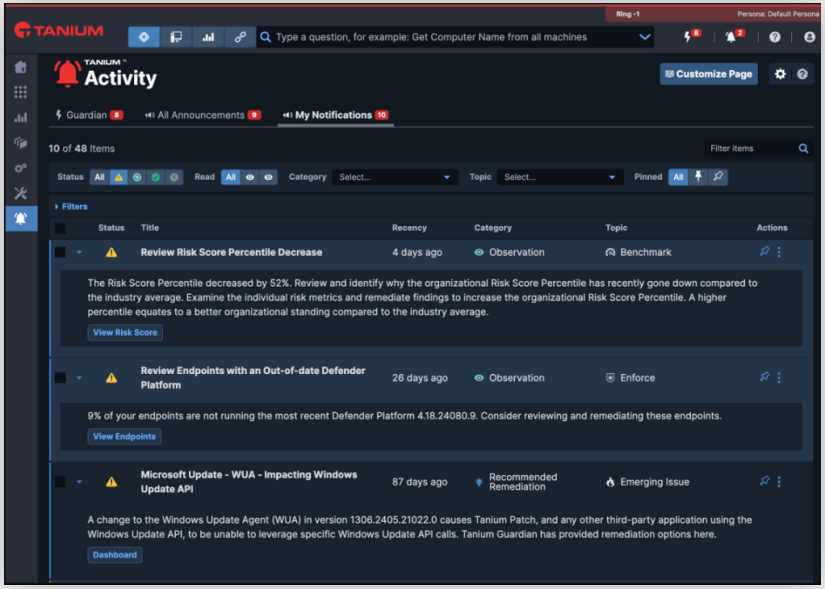
Tanium Ask

Tanium AEM autonomous controls

Tanium Guide prioritizes IT and Security Ops tasks enabling them to take the next best actions on endpoints.

Using Real-time Cloud Intelligence as a foundation Tanium Guide takes advantage of benchmarks and real-time analysis of dynamic global IT environments to provide timely and fully actionable recommendations to ensure operators are always focused on implementing the changes that can best improve the environment.

- Pivot from Tanium Guide recommendations to workflows to implement necessary changes
- Leverage environmental Observation notifications to link operators to investigation workflows
- Identify potential problems quickly without sifting through reports and endless data
- Greatly reduce the likelihood of overlooking critical or urgent issues

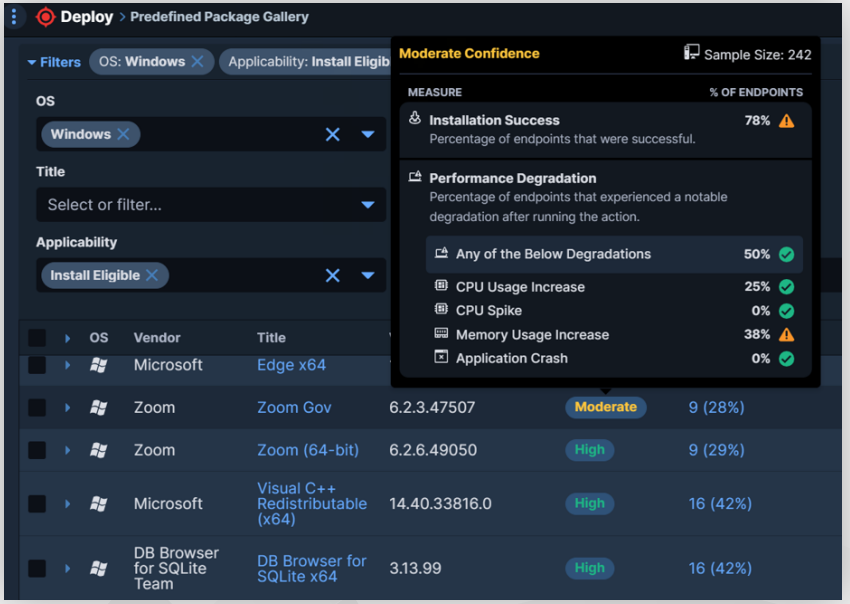


Tanium Guide

Tanium Adaptive Actions empower IT teams drastically decrease response and remediation times on critical endpoints.

Tanium Guide recommendations are linked to a Tanium Adaptive Action which is the automation playbook to implement the recommendation itself. Adaptive Actions can run without operator involvement but can be fully customized and controlled as needed.

- Confidence scores indicate how probable taking an action will succeed and produce the desired result
- Deploy changes into the environment using a phased approach (i.e., Rings) to contain issues and reduce risks
- Schedule Ring deployment progression based on preconfigured success criteria
- Keep humans in the loop as needed for visibility, governance and control

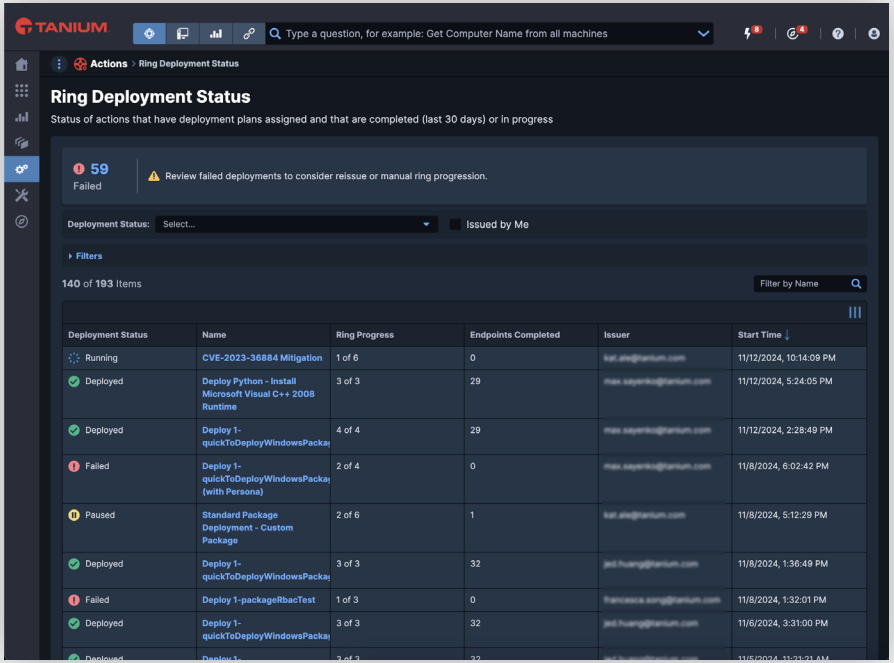


Tanium Adaptive Actions

Tanium Action Oversight puts operators in complete control with governance over all aspects of Tanium's autonomous functions.

Tanium AEM prioritizes safety above all else. Every system is tied into the centralized governance component, Tanium Action Oversight . It provides visibility, remediation and control at the right level of detail.

- Maintain a complete record of autonomous activity including the actions of the past, those currently in motion and tasks scheduled for the future
- Gain complete visibility and control over all autonomous activity while in flight (e.g.: halting or cancel progression)
- Operators can inspect autonomous activity at different levels of granularity helping both in diagnostic and planning activities
- When issues do arise, there is a full suite of functions available to swiftly and easily isolate and remediate as needed

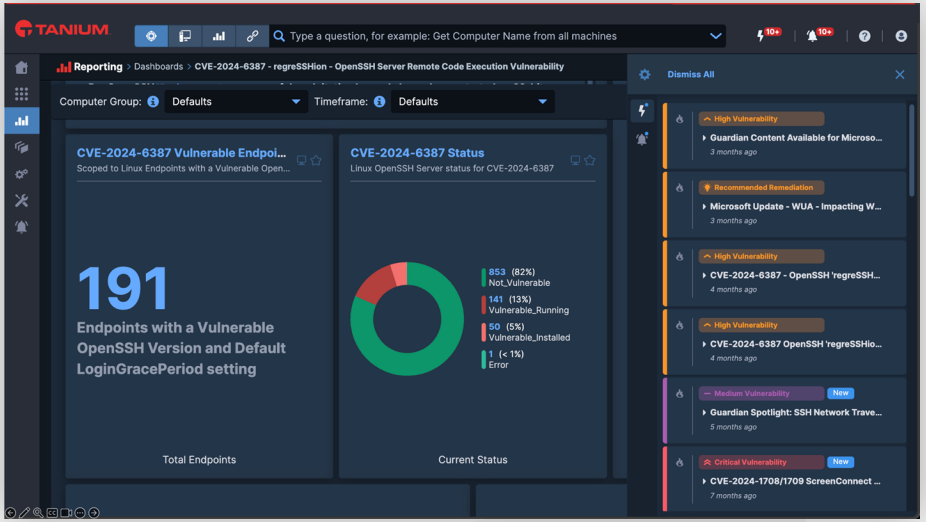


Tanium Action Oversight

Tanium Guardian provides alerts, insights, and remediation actions to respond quickly and effectively to critical zero-day vulnerabilities.

Combining real-time global endpoint analytics and human intelligence Tanium Guardian operates as a special express lane for zero-day or time critical issues. Guardian combines reports, dashboards, analysis and automation to enable operators to remediate issues before they cause disruption to business operations.

- Gain instant visibility into critical and high-severity issues on your endpoints that could expose your environment to attacks and exploits
- Take advantage of effective mitigations and automation, enabling you to take immediate control of emerging issues
- Remediate issues confidently just on impacted endpoints using Autonomous Control technologies like Confidence Scores, Adaptive Actions and Rings



Tanium Guardian

"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

Tanium AEM benefits

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.

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.

Assured compliance

Continuous monitoring, industry benchmarking and automated compliance checks ensure that the organization meets regulatory requirements, reducing the risk of fines and legal issues.

Reduce IT support costs

Automatic resolution of several endpoint issues reduce IT and Security support overhead that can disrupt and impede employee productivity.

Enhanced security posture

Proactive identification, prioritization, and remediation of cyber risks from vulnerabilities and configuration drifts help protect the organization from cyber threats, safeguarding sensitive data and maintaining customer trust.

Increased IT agility

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

Delivering on differentiation

Tanium AEM is a ground-breaking solution that establishes the standard for how a real-time converged platform should deliver safe and reliable automation for managing and securing the IT infrastructure. AEM empowers your IT operations and security teams with:

A converged platform providing visibility, control, and remediation for diverse IT operations and security needs

Prioritized, actionable observations from millions of data points

Real-time data analysis for instant insights

Detailed analysis on the probable success of an action

Confident execution of changes across large IT estates in real-time

Phased action execution for risk reduction

Governance and control during any autonomous activity

Improved operational efficiency through strategic focus

REQUEST A DEMO TODAY

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

Try Tanium AEM now →