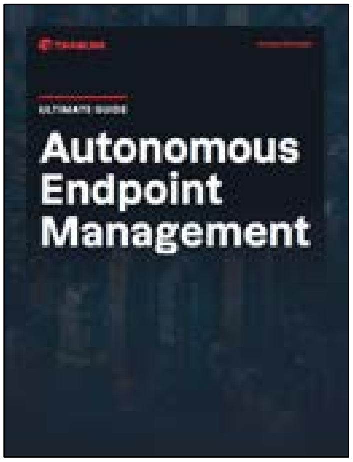
TANIUM

carahsoft.


ULTIMATE GUIDE

Autonomous Endpoint Management

Ultimate Guide: Autonomous Endpoint Management

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium’s solutions, please check out the following resources and information:

For additional resources:
carah.io/taniumresources

For upcoming events:
carah.io/taniumevents

For additional Tanium solutions:
carah.io/taniumsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
tanium@carahsoft.com

703-673-3560

To purchase, check out the contract vehicles available for procurement:
carah.io/taniumcontracts

For more information, contact Carahsoft or our reseller partners:
tanium@carahsoft.com | 703-673-3560

The Power Of Certainty™

ULTIMATE GUIDE

Autonomous Endpoint Management

The Ultimate Guide to Autonomous Endpoint Management

Contents

Introduction

Cybersecurity is at an inflection point. The speed, scale, and sophistication of modern threats are rendering traditional IT management models obsolete. Today's attacks are not only faster and more targeted, but increasingly automated, adaptable, and difficult to detect.

Organizations today face a surge in identity-based attacks, endpoint exploitation, and infrastructure compromise. At the same time, security and IT teams must contend with growing operational complexity, from protecting hybrid cloud environments and managing emerging technologies to controlling shadow AI.

Compounding these challenges are tight budgets, persistent staffing shortages, and rising pressure to do more with less. According to Fortinet's *2025 Cloud Security Report,* 76% of professionals said they are impacted by security skills shortages, while 63% are challenged by assuring data security and privacy.[1]

To improve outcomes, organizations are increasingly shifting from reactive to preemptive vulnerability management powered by predictive intelligence and real-time insights. This proactive approach aims to detect, eliminate, and prevent advanced threats. Gartner predicts that by 2030 up to 50% of IT security spend will focus on preemptive solutions, signaling a broad shift toward threat anticipation and risk mitigation.[2]

> **IDC reports that by 2026, 75% of CIOs will integrate cybersecurity measures directly into systems and processes to proactively detect and neutralize vulnerabilities.[3]**

Automation is the catalyst for this transformation. IT automation has the potential to power real-time threat detection and remediation, while converting manual tasks into intelligent, always-on workflows. Beyond security, automation may be harnessed to improve core IT operations, from patching and provisioning to compliance monitoring and reporting. In fact, PwC found that 82% of organizations are planning to invest more in at least one technology to automate and optimize compliance activities.[4]

In recent years, a variety of automation frameworks have been introduced into enterprise environments. Common examples include identity and access management (IAM) for controlling user privileges, security, orchestration, automation, and response (SOAR) for incident response, and security information and event management (SIEM) for event analysis. Taken together, these methodologies suggest the emergence of a unified security fabric providing unprecedented visibility, responsiveness, and operational efficiency.

Now, autonomous endpoint management (AEM) is emerging as a game-changing technology for security and IT operations to support this unified and automated approach. AEM technologies are poised to deliver real-time, automated discovery, patching, configuration, and threat remediation across an organization's endpoints.

The chapters ahead provide a primer on AEM and modern automation, exploring what autonomous endpoint management entails, how it helps security and IT teams, and how to choose the right automation tool. Finally, we'll look ahead to the future of AEM and how automation will continue to redefine workflows.

CHAPTER ONE

What is autonomous endpoint management?

For decades, organizations have struggled with manual patching cycles and fragmented security toolsets, resulting in delayed response times, data silos, and persistent security gaps. In many cases, it can take days or even weeks to identify and patch endpoints, giving threat actors ample time to exploit vulnerabilities.

Now, with AI becoming more accessible, threat actors can discover and exploit vulnerabilities faster than security teams can respond. To close this gap, organizations are turning to various forms of IT automation to deliver continuous and adaptive security and operational efficiency.

Among these is autonomous endpoint management, or AEM, an emerging IT and security strategy that combines automation, real-time data, and policy-driven workflows designed to deliver unified endpoint management at scale.

In its 2025 *Innovation Insight: Autonomous Endpoint Management,* Gartner explains:

> **"AEM is a next-generation approach that is enabled by new functionality within advanced endpoint management tools. AEM leverages configuration, compliance, risk, performance and experience data to intelligently perform common endpoint management and DEX tasks… AEM combines proven ring-based deployment with AI and ML, DEX, and intelligence-driven automation that can be tuned according to risk appetite."[5]**

Gartner predicts that by 2029, more than 50% of organizations will adopt AEM capabilities within advanced endpoint management and digital employee experience (DEX) tools—up from nearly zero in 2024.

The need for AEM is accelerating as AI threats rapidly evolve, and organizations begin to embrace fully automated agentic models that can potentially access sensitive data and systems.

With the right technology in place to support AEM, organizations can harness the transformative power of AI while also improving security, system resilience, and efficiency.

How organizations can use AEM to enhance IT and security

According to the Gartner report, the most well-established use case for AEM is autonomous patching, which ensures systems remain equipped with the latest features and security updates, along with consistent and repeatable configurations across all environments.

Some additional, future-facing use cases include:

- **Security monitoring:** Tracking endpoint activity to detect policy variations and anomalies in real time
- **Software deployment:** Automating application delivery and configuration across distributed endpoints
- **User provisioning:** Streamlining onboarding and offboarding by applying user roles, permissions, and access based on predefined policies
- **Compliance enforcement:** Ensuring endpoints continuously meet internal and regulatory standards like HIPAA and GDPR

> AEM represents the most significant advancement in endpoint management in over a decade.
>
> **Tom Cipolla & Dan Wilson**
> Gartner

While AEM is gaining momentum and generating interest, it's presently an emerging technology. This is partly due to its reliance on AI, which is still developing and maturing. As time goes on, new use cases will expand its value across both IT operations and employee experience.

Gartner also notes that AEM is likely to evolve into broader strategic functions, including:

- **Endpoint configuration adjustments:** Automatically adjusting settings based on user behavior and operational context
- **Employee engagement:** Using telemetry and digital experience metrics to improve user productivity and satisfaction
- **Hardware lifecycle planning:** Leveraging endpoint intelligence to anticipate hardware failures and reduce total cost of ownership

These forward-looking capabilities are deeply rooted in automation—an essential pillar of AEM. To fully understand how AEM works in practice, it's important to first define what automation means in the context of IT and cybersecurity.

Defining automation: General overview and how it relates to IT and cybersecurity

Automation is one of the most talked-about concepts in the workplace today, with organizations across all industries using it to streamline operations and reduce manual effort. Yet despite its popularity, there's still widespread confusion about what automation truly means—especially in the context of IT and cybersecurity.

At its core, automation uses various techniques to perform tasks with minimal human intervention. In IT, this often involves techniques like scripting, policy-based workflows, and AI-driven decision-making. IT automation helps manage workloads, streamline processes, and eliminate human error, enhancing overall operational efficiency.

Some of the top benefits include:

Increases precision and speed in performing repetitive tasks

Reduces manual intervention, leading to more reliable outcomes

Enhances security by automating tasks like monitoring and patch management

Reduces time spent on routine cyber hygiene tasks, freeing IT teams for higher-order work

Automation is now a top priority for resource-constrained technology leaders who must balance innovation with risk while delivering measurable ROI. According to IDC, 80% of CIOs plan to embrace automation and AI for agility and insights by 2028.[3]

Comparing automation, AI, and LLMs

Terms like automation, AI automation, and large language models (LLMs) are often used interchangeably. However, they represent distinct technologies with different capabilities and use cases. Understanding the distinctions between automation, AI, and LLMs is essential to navigating today's rapidly evolving IT and security landscape. But to fully appreciate how we arrived at this moment—and where we're headed—it helps to take a step back.

Traditional automation uses rules or scripts to perform repetitive tasks without human intervention. It's widely used to streamline workflows like data entry, password resets, and system maintenance.

AI automation builds on traditional automation by using either AI and/or machine learning (ML). AI-powered systems can learn, adapt, and make critical decisions. In IT and security, AI automation is often used for real-time threat detection, autonomous patching, and triaging.

Machine learning is a subset of AI that enables systems to learn from data and make predictions. ML algorithms help security teams identify anomalies, assess risk, and prioritize vulnerabilities. Common types of ML include supervised learning, which is used for predicting outcomes; unsupervised learning, which identifies patterns in data without human guidance; semi-supervised learning, which combines labeled and unlabeled data; and reinforcement learning, which relies on rewards and penalties to shape behavior.

Agentic AI is the latest evolution of artificial intelligence. As the name suggests, agentic AI uses reasoning to take actions and execute tasks in ways that resemble how a human would. Often described as the "third wave" of AI, agentic systems are now being used to manage complex workflows and boost operational efficiency. Adoption is expected to continue as more organizations learn how to deploy and optimize AI agents.

LLMs refer to AI models that are trained or developed on massive datasets. These advanced models enable AI programs to answer questions and engage in conversations with contextual awareness and reasoning abilities. Today, they are used for tasks like threat analysis, knowledge retrieval, and advanced helpdesk support.

How we got here: A brief history of automation

Automation has been evolving for centuries—steadily transforming the way people work, produce, and engage with technology.

We are currently in the middle of what many observers call the Fourth Industrial Revolution, a term first popularized by Klaus Schwab, founder and Executive Chairman of the World Economic Forum, in his 2016 book *The Fourth Industrial Revolution.*

This Fourth Industrial Revolution is driven by numerous advancements across the internet of things (IoT), high-speed connectivity, AI/ML, real-time data processing, and advanced robotics.

Here is a quick breakdown of previous eras of industrial progress, how automation has advanced over the years, and where it currently stands.

Industrial revolutions	**Role in automation**
First Industrial Revolution *Late 1700s*	Introduced mechanical tools for agriculture and textiles, allowing workers to be more productive
Second Industrial Revolution *Late 1800s*	Enabled early factory automation, such as mechanically powered machine tools, for greater speed and output
Third Industrial Revolution *1950s–2000s*	Replaced many manual tasks with digital systems, introducing programmable automation, computerized manufacturing, and digital communication networks
Fourth Industrial Revolution *2010s–present*	The future of automation is driven by rapid advancements in AI, ML, and real-time analytics, promising levels of productivity previously unimaginable

Unlike earlier forms of automation, today's AI-powered systems can analyze real-time data, adapt to changing conditions, and apply reasoning to make context-aware decisions. The next wave of agentic systems takes this even further by introducing the ability to continuously learn and respond to subtle changes in systems, identities, and endpoints.

Key takeaways from chapter 1

- AEM combines automation, real-time data, and policy-driven workflows to enable endpoint management at scale.
- Organizations can use AEM to keep pace with AI-driven threats, protect global endpoints, and ease the burden on overstretched IT and security teams.
- Today, AEM can help with patching, security monitoring, software deployment, and user provisioning.
- AI is taking automation to new heights and enabling IT and security teams to operate with greater speed and efficiency.

In this chapter, we explored how endpoint management is evolving from a manual, time-consuming process into a fully automated, intelligent, and unified system. With AEM in place, connected endpoints shift from operational liabilities to data-rich assets that deliver valuable insights and drive smarter decision-making.

Now that we have covered the basics of enterprise automation, let's take a closer look at the benefits that it offers—and why IT and security teams have little choice but to embrace it.

CHAPTER TWO

What are the benefits of automation?

IT and security teams have evolved from backend support roles to strategic enablers, powering everything from finance and accounting to sales and executive leadership.

As organizations become even more dependent on technology, they are painstakingly searching for ways to eliminate IT and security inefficiencies. This requires new levels of speed and precision, which is something that manual processes cannot deliver at scale. Incidents that once carried a response time of days or weeks to complete now require resolution within hours or, better yet, minutes.

While team sizes tend to vary, enterprises with 10,000 or more employees often maintain a ratio of just one IT professional for every 40 workers. This imbalance forces many teams into a reactive mode, leaving little time for innovation or growth initiatives.[6]

Automation—and increasingly, AI-driven automation—is no longer optional for IT and security operations. When implemented effectively, automation empowers teams to overcome resource limitations, reduce response times, and shift from reactive firefighting to proactive innovation.

Top three benefits of automation

1. Reducing burnout

IT and security workers must juggle complex issues, ranging from system outages to ransomware attacks. Service requests are often urgent, which can be challenging for teams that lack adequate manpower or expertise.

A Tanium study found that three-quarters of IT workers say automation could help reduce burnout, which is experienced by 69% of IT teams.[7]

2. Improving morale

There is a direct link between employee experience, morale, and IT efficiency. Frequent downtime, security incidents, and inefficient workflows can sap motivation and cause turnover.

Automation not only reduces downtime and security issues, but it also frees IT workers to take on more high-impact projects rather than constant firefighting.

3. Mitigating risk at scale

Even minor changes to an endpoint can expose organizations to breaches. Security teams must have eyes on every endpoint, and the ability to detect anomalies. However, this is exceedingly difficult for small teams managing global networks with hundreds or thousands of distributed endpoints.

In Tanium's study, over three-quarters of IT workers agreed that automation tools could improve overall security by shortening patch cycles, reducing vulnerability exposure timeframes, and accelerating incident response times.[7]

Key takeaways from chapter 2

- Organizations are now fully dependent on IT and security, making automation essential for success.
- Small IT and security teams can use automation to extend their resources and scale support globally.
- The top benefits of automation include reducing burnout, improving morale, and mitigating risk at scale.

In recent years, automation has become a cornerstone of modern IT and security operations—and we're only beginning to tap into its full potential. Looking ahead, AI-driven automation will fundamentally reshape how organizations design, manage, and secure their technology stacks.

As routine tasks integrate with intelligent systems, IT and security teams will shift from reactive triaging to delivering strategic, high-impact guidance. This will help CIOs, CISOs, and technology departments lead digital projects and deliver greater value.

In the next chapter, we'll explore common barriers that organizations experience with automation and some easy ways to accelerate adoption.

CHAPTER THREE

Accelerating automation adoption: Why data is key

Despite mounting pressure to automate IT and security operations, many organizations continue to face challenges that stall their modernization efforts. A growing divide now exists between organizations that are successfully implementing and scaling automation, and laggards who are behind the curve—stuck in pilot modes, and failing to generate strong results.

In many organizations, automation remains highly fragmented and siloed, delivering only limited value within individual teams and departments. Without a unified strategy, these isolated efforts struggle to drive meaningful impact at scale, often increasing operational risk and prolonging manual processes that strain resources and expose security gaps.

While infrastructure, organizational readiness, and resources all play a role, one factor that consistently separates those accelerating automation and those falling behind: data readiness.

Even the most advanced automation tools can't deliver meaningful results without reliable, accessible, and up-to-date data. According to Gartner, 89% of CEO and senior executives say effective data, along with analytics and AI governance, is essential for enabling business and technology innovation.[8]

Common data challenges that undermine automation

- **Data sprawl:** In many organizations today, data is scattered across cloud platforms, legacy systems, and disconnected tools, making it challenging to create unified automation workflows.

- **Lack of visibility:** IT and security teams often struggle to identify what data exists, where it lives, and how current or accurate it is. This hinders automation planning and implementation.
- **Stale data:** Almost all data comes with a shelf life. Outdated information can lead to automation decisions based on inaccurate inputs, reducing effectiveness and potentially creating new security risks.

Quick tips for automation data readiness

- **Establish quality metrics** for data accuracy, completeness, consistency, and timeliness.
- **Create ownership and governance frameworks** to maintain data integrity, privacy, and security.
- **Integrate validation steps** with automation workflows to catch and remediate errors early.
- **Map data dependencies** to discover how different datasets interact across your organization.
- **Invest in data pipelining** to ensure clean, real-time data flows between endpoints and teams.

IT data accuracy is as important as financial data accuracy

No organization would tolerate a CFO estimating revenue as "between $300-$500 million."

However, it's not uncommon to hear a CIO make an estimate like "300-500k endpoints" in their organization's environment.

IT data inaccuracy should not be an accepted norm.

The fact is that organizations have been grappling with data quality and availability issues for years. But with the shift toward fully automated, AI-driven IT and security operations, those challenges are becoming more urgent. High-quality, real-time data is critical for enabling AI to make accurate, context-aware decisions. And as more organizations begin relying on AI agents to handle critical IT and security workflows, having clean and reliable data will be imperative for success.

By focusing on data readiness now, organizations can set the stage for the next wave of AI and automation—and set the table for smarter workflows, real-time decision-making, and more resilient IT and security operations.

Data readiness + agentic AI: A force multiplier for automation

As we explained in the first chapter, agentic AI is the "next wave" of artificial intelligence. When paired with data readiness, agentic AI can make it possible to automate complex, multi-step processes—streamlining routine maintenance and manual interventions for IT and security teams and enabling them to focus on other pressing needs.

How agentic AI works

Agentic AI uses LLMs, NLP, ML, and reinforcement learning to quickly and independently make decisions. Agentic systems can identify relevant patterns, apply reasoning to interpret tasks and coordinate with models, and integrate with external software and tools using APIs. Most importantly, agentic models can learn over time using continuous feedback loops for enhanced effectiveness and adaptation.

How agentic AI supports IT and security operations

Up until recently, automation largely involved teaching computers to execute tasks using predefined steps. Agentic AI takes this to the next level by enabling agents to understand and act autonomously without requiring any user input.

According to UiPath, 93% of U.S. IT executives are extremely or very interested in agentic AI.[9] In the coming months and years, more teams will begin using agentic AI systems to automatically manage and update connected endpoints and mitigate cybersecurity threats. Agentic systems can instantly detect vulnerabilities and anomalies across connected endpoints through continuous monitoring and automatically execute proactive mitigation responses.

At this point in time, few IT and security teams are using agentic AI at scale. According to the 2025 Cyber Security Tribe annual report, no surveyed CISOs are currently using agentic AI for cybersecurity.[10] However, 59% are working on implementing it, making it a top emerging trend to know about.

Remember: To succeed with agentic AI, organizations must have all of the foundational elements listed above—including data readiness, high-quality supporting infrastructure, and automation-ready teams and processes.

Key takeaways from chapter 3

- Many organizations are currently behind the curve with automation. A gap is growing between automation leaders and laggards.
- Data readiness is a key factor for accelerating automation. Common challenges include scattered data, poor visibility, and stale data.
- By improving data readiness, organizations can achieve stronger and more accurate results with automation.
- When paired with strong data readiness, agentic AI can be a force multiplier—driving smarter decisions and enabling fully automated IT and security workflows.

To reach an advanced level of workflow automation, organizations must first lay the groundwork—just as they did during earlier shifts to digital transformation, cloud computing, and remote work. AI-driven automation holds tremendous potential, but it requires careful planning and coordination. Data readiness is one of the most important enablers.

Once your organization is ready for change, you can move on to the next phase: selecting a platform that aligns with your specific needs and goals.

CHAPTER FOUR

How to choose the right automation tool for endpoint management

The endpoint management market is highly saturated, with many platforms delivering comparable features like device management, policy enforcement, and remote monitoring—making it difficult to differentiate based on surface-level capabilities alone.

In this chapter, we'll break down some factors to consider when evaluating endpoint management and automation services to help you make an informed, strategic decision.

What is an endpoint management platform? Definition and features

First, it's important to understand what qualifies as an endpoint management solution. Gartner defines an endpoint management tool as one that provides configuration management and patching, as well as the deployment of operating systems and applications across both mobile devices and computers.[11]

At a minimum, qualifying platforms must:

- Support agent-based or agentless management
- Be offered as a single-license, generally available SKU
- Be delivered as a turnkey SaaS solution, hosted and operated by the vendor

Modern endpoint management platforms are evolving to meet the demands of hybrid work, security resilience, and digital experience optimization.

Below are key capabilities that Gartner defines as necessary for modern endpoint management tools:

AEM support

Gartner highlights that support for AEM is becoming increasingly important as organizations rely on digital employee experience metrics to assess patch success, endpoint performance, and overall IT effectiveness by enabling IT teams to prioritize remediation based on real-time user impact.

While Gartner frames AEM primarily through the lens of DEX, the concept is evolving. In practice, AEM is emerging as a broader operational model that integrates real-time telemetry, automation, and policy enforcement to reduce manual effort, eliminate silos, and deliver continuous compliance.

The shift reflects a growing need for platforms that not only respond to user experience signals but also proactively manage endpoint health, security posture, and configuration integrity at scale.

Agent-based or agentless management

Gartner states that a qualifying endpoint management platform must support either agent-based or agentless management—or both. This flexibility is essential for organizations managing a wide range of device types and deployment scenarios.

To meet this requirement, modern platforms should deliver integrated capabilities, such as device discovery, inventory, OS updates, patching, configuration, and encryption management, regardless of the underlying management method.

Gartner also notes that leading solutions are expanding support for diverse device ecosystems, including ChromeOS, IoT, and ruggedized endpoints. This development aligns with a wider industry movement toward enabling unified, flexible management across increasingly heterogeneous environments.

Third-party application patch automation

According to Gartner, modern endpoint management platforms are expected to automate patching not only for operating systems but also for third-party applications like browsers, collaboration tools, and productivity suites. This capability is critical for reducing risk exposure and maintaining consistent security hygiene across the enterprise.

To support this, some platforms now offer curated repositories of pre-approved application updates and installers. Gartner highlights that these features help streamline patch deployment, reduce manual effort, and ensure policy-driven remediation—especially in environments where speed and consistency are paramount.

Customizable reporting and dashboards

Gartner emphasizes that as endpoint environments grow more complex, IT and security teams require real-time visibility into device health, patch compliance, and security posture.

To address this, modern platforms are expected to provide customizable dashboards and reporting tools that consolidate these insights into a single, unified view. Gartner also points to the value of role-based dashboards and real-time analytics, which enable faster decision-making and more effective risk oversight—particularly in large-scale environments where centralized visibility is essential for operational continuity and governance.

Additional capabilities to consider

In its guidance on modern endpoint management, Gartner also identifies a set of extended capabilities that help organizations advance beyond basic device control toward more intelligent, resilient, and user-aware operations—capabilities that can support the evolution toward more autonomous endpoint management:

- Role-based access control (RBAC)
- Full mobile management
- Containerized mobile applications
- Remote data management
- Device imaging and reimaging
- Enterprise app store
- Agent-based management or prebuilt connector
- Customizable reporting and dashboarding capabilities
- Support for Windows Autopilot, etc.
- Flexible device configurations
- Extended features and integrations

These capabilities reflect Gartner's view that endpoint management is becoming a strategic discipline—one that underpins digital employee experience, operational agility, and enterprise-wide risk reduction.

For organizations building toward more autonomous operations, they represent not just "nice-to-haves," but essential components of a modern, scalable endpoint strategy.

Understanding the core and extended capabilities of modern endpoint management platforms—especially those outlined by Gartner—is essential. But capabilities alone don't tell the full story.

To make a strategic, future-ready investment, it's equally important to evaluate how those features support the day-to-day needs of your organization. Whether you're focused on improving patch velocity, reducing risk exposure, or enhancing DEX, the right platform should align with your operational priorities.

> **In the next section, we'll explore the most common—and most critical—use cases that endpoint management platforms are expected to support today, and how those use cases can guide your selection process.**

Primary supporting use cases for endpoint management

Modern endpoint management platforms can support a variety of use cases beyond basic device control—from securing sensitive data to ensuring policy compliance. It's important to find a platform that will meet your specific operational needs.

Use case	Description	Features
Security monitoring	Identify, classify, and secure sensitive data	● Agent-based scanning ● Multiple file-format and OS support ● Deep regulatory reporting
Software deployment	Enable phased software updates, with fewer disruptions and performance issues	● Application packaging ● Staged or ring-based deployment ● Version tracking
User provisioning	Rapidly configure devices with systems and apps	● OS imaging and deployment ● Policy-based provisioning ● Self-service
Compliance enforcement	Maintain alignment with internal and external policies	● Automated policy application ● Audit logging and reporting ● Encryption and access controls

In addition to the use cases outlined above, endpoint management platforms can also help with the following areas:

- **Integrated risk identification:** Continuously analyze and benchmark dynamic IT environments to proactively discover vulnerabilities, misconfigurations, and zero-day threats before they cause downtime and security incidents.
- **Efficiency:** Empower small teams to manage large, distributed environments using automation and centralized management.
- **Real-time visibility:** Consider choosing a platform that provides clear, real-time insight into device health, configuration, and performance, enabling faster troubleshooting and data-driven decisions.

Additional considerations

- **Scalability:** With endpoint management, there's a difference between monitoring at scale and managing at scale. While many platforms promise global scalability, it's essential to look under the hood and assess their ability to actively manage, update, and automate across large, distributed environments.

- **Ease of use:** At the end of the day, management and automation systems are supposed to save team members time and expedite system changes. Platforms that are overly complex and require a significant learning curve can be detrimental, especially to stretched-thin support teams.
- **Security and governance:** When deploying endpoint management and automation at scale, security is critical. It helps to have a platform with native governance features that provide reporting and visibility across all autonomous activity.

Key takeaways from chapter 4

- An endpoint management platform can be used for many different tasks, ranging from configuration management and patching to operating system deployment, compliance, and more.
- Common capabilities to look for include AEM, agent-based and agentless management, third-party patch automation, and customizable reporting, among others.
- Platforms tend to vary significantly in terms of scalability, usability, and automation maturity.

Sourcing an endpoint management tool for automation—and IT procurement in general—can be a long and challenging process, often requiring extensive research, cross-functional coordination, and vendor evaluation. In fact, 90% of IT executives in North America now view software sourcing and vendor selection as a pain point.[12]

To streamline the process, IT and security teams are encouraged to tap into their broader ecosystems—including internal stakeholders, trusted third-party consultants, and even managed service providers. These partners can provide valuable insights and help ensure the chosen platform aligns with the organization's environment and needs.

CHAPTER FIVE

How Tanium does autonomous endpoint management

Tanium officially began its AEM journey in 2023, when Chief Technology Officer Matt Quinn announced Autonomous Endpoint Management as the next evolution of the Tanium platform. Since then, Tanium has delivered a suite of cutting-edge platform capabilities and autonomous innovations to make this vision a reality.

Tanium Autonomous Endpoint Management

Today, Tanium AEM delivers measurable outcomes across a broad set of integrated solutions, including asset discovery and inventory, vulnerability management, endpoint management, incident response, risk and compliance, and digital employee experience.

Tanium AEM empowers IT and security teams to make faster, more informed decisions via AI-driven insights from real-time endpoint data. It significantly boosts operational efficiency by automating routine tasks, freeing teams to focus on strategic growth initiatives—without compromising security, performance, or availability.

Through intelligent, scalable automation, AEM also strengthens security posture and accelerates risk mitigation. It proactively manages vulnerabilities and incidents by analyzing real-time data from globally distributed, cloud-managed endpoints—safely recommending and executing actions to maintain operational health and reduce business risk.

Tanium AEM autonomous controls

With real-time data and analysis of changes across globally distributed, cloud-managed endpoints, Tanium AEM makes recommendations and automates changes safely and reliably—while keeping the user in control.

Gain real-time visibility into endpoint health, risk, and readiness.

Trigger intelligent, automated responses that adapt to your environment and policies.

Maintain control with built-in governance for safe, auditable execution at scale.

Tanium AEM innovations

Tanium AEM powers a growing arsenal of IT and security workflows with real-time data, massive scale, intelligence, and adaptive automation.

Tanium Automate

Tanium Automate is the orchestration and automation engine built into the Tanium platform. It enables IT and security teams to design and execute dynamic workflows that scale across the environment—powered by real-time data and actionable endpoint intelligence.

By replacing manual processes with low- and no-code playbooks, Automate empowers teams to streamline complex tasks with speed, precision, and confidence. These reusable workflows capture operator expertise and combine IT and security tasks from across the platform, helping teams scale operations efficiently and consistently.

For example, organizations can:

- Scan endpoints for software usage and use real-time data to identify underutilized licenses, then notify users that unused software is scheduled for removal.
- Patch servers that are part of a cluster in a way that maintains high availability throughout the process.
- Create reusable playbooks with little to no code to automate common IT and security operations.
- Empower a broad range of users—regardless of technical skill level—to author and manage powerful automation.
- Define entrance, exit, and success criteria for each step to ensure safe and reliable execution.
- Maintain full visibility into automation activity, including historical audit logs, current playbook status, and future schedules.
- Integrate with external systems using Tanium APIs to trigger playbooks from platforms like ServiceNow or Microsoft security solutions.

> “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, VF Corporation

Tanium Ask

Tanium Ask leverages advanced large language model (LLM)-powered AI and real-time endpoint data to help users of all skill levels get accurate, current-state answers to complex IT and security questions using natural language—no scripting or query language required.

Example questions include:

- What is the average time to patch my machines?
- Are there any servers experiencing performance problems today?
- Which endpoints have unused Adobe Photoshop installed?
- What endpoints are missing critical patches released more than 30 days ago?

By combining generative AI with Tanium’s real-time visibility, Ask enables faster, more informed decisions across the organization—from executive leadership to frontline operators.

To further streamline the experience, users can refine prompts using the Question Builder and save favorite queries for reuse—accelerating insight generation at any scale.

Tanium Guide

Tanium Guide provides crucial insights into endpoint environments. The platform globally benchmarks and analyzes a customer’s dynamic IT environment in real time to guide the next best action and change to take on their endpoints. These recommendations are designed to help operators confidently prioritize and execute changes that improve operational health and reduce risk.

For example, Guide can:

- Identify endpoints with out-of-date signatures for Microsoft Defender for Endpoint and recommend a remediation playbook.
- Surface endpoints with elevated risk scores that exceed defined thresholds and prompt targeted investigation or action.

Tanium Guardian

Integrated with Tanium AEM, Tanium Guardian delivers early insight and rapid response to critical and high-severity vulnerabilities. It provides real-time alerts and expert-verified guidance to help IT and security teams take swift, targeted action—while offering proactive visibility into the impact of remediation.

Backed by the Tanium Vulnerability Emergency Response Team (VERT), Guardian combines global endpoint analytics with zero-day research to surface emerging threats and publish dynamic reports identifying where environments may be at risk.

Adaptive Actions

With a focus on execution, Tanium Adaptive Actions are automation playbooks linked to Guide recommendations. They can run autonomously or with human oversight, using confidence scores.

When large-scale changes to endpoints are needed, ring-based deployments and preconfigured release plans provide the ability to phase deployments—ensuring changes are well-managed and repeatable.

Tanium Confidence Score

Tanium Confidence Score aggregates real-time global insights to provide context on the safety and reliability of the actions and changes you plan to implement in your environment.

Several key components contribute to this score, each evaluating distinct aspects of post-change performance across a vast network of managed endpoints:

- **Installation Success:** Measures the percentage of endpoints where installation was successful
- **Application Crash:** Tracks the frequency of application crashes
- **Performance metrics:** Includes critical indicators such as CPU and memory usage, and detects anomalies or spikes that could indicate underlying issues

These insights help determine how safe a proposed update may be in a given environment, drawing from observed outcomes across the Tanium Cloud community. They can be used to inform automation rules and guide phased rollouts using Tanium AEM deployment rings—ensuring changes are introduced safely and in alignment with the cadence of the organization.

This scoring system is tightly integrated with the software packages available through the Tanium Deploy gallery, enabling teams to evaluate, plan, and execute changes with greater confidence and control.

> **When Tanium's AEM Confidence Score was introduced to users at Tanium Converge 2024, you could hear the collective sigh of relief… [underscoring] how much decision-making fatigue cybersecurity admins wish to be relieved of.**

Grace Trinidad
IDC

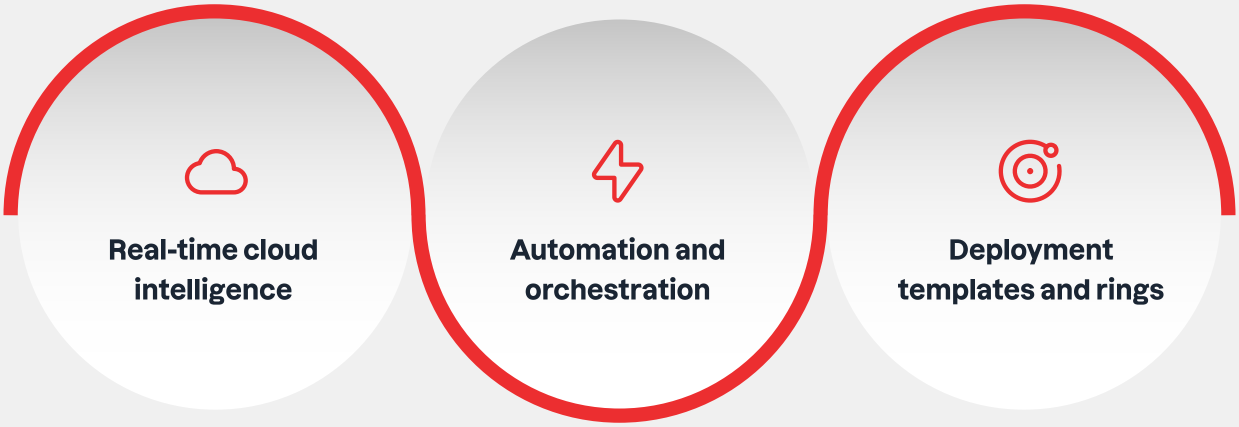
Remediation Visibility

Remediation Visibility bridges the gap between detection and action by helping teams prioritize and execute the most impactful remediation efforts. It highlights the top unscheduled patches that address critical vulnerabilities, enabling faster, risk-based decision-making.

With built-in patch impact analysis and integration across Tanium modules, teams can collaborate more effectively, reduce mean time to remediation, and strengthen their overall security posture.

Tanium AEM platform foundations

Tanium AEM is built on a cloud-native architecture that supports a growing number of IT security and operations use cases. This foundation enables continuous adaptation to dynamic environments, ensuring intelligent, real-time response across the endpoint landscape.



Real-time cloud intelligence

Measure and analyze even the smallest effects of change on endpoints to confidently predict the impact of endpoint changes in real time.

Automation and orchestration

Scale and extend the value of expert knowledge by capturing and designing dynamic, reusable automations that span IT and security operations use cases.

Deployment templates and rings

Minimize disruptions by rolling out endpoint changes in alignment with organizational cadence.

Tanium AEM use cases

Tanium AEM helps IT and security teams improve operational resilience, reduce risk, and scale their efforts through intelligent automation and real-time decision support.

Below are some key ways organizations can use AEM to drive impact:

Prevent disruptions during endpoint changes

Organizations can reduce the risk of outages or performance degradation by using real-time insights to assess the safety of changes before deployment. Phased rollout strategies help align changes with organizational cadence, ensuring minimal disruption and maximum reliability.

- **Tanium Confidence Score:** Evaluates the safety of changes using real-time global insights
- **Deployment rings:** Enable phased rollouts in alignment with organizational priorities

Proactively identify and address operational risks

By continuously analyzing endpoint health and configuration baselines, teams can surface issues—such as outdated security signatures or elevated risk scores—and take guided action to resolve them before they escalate.

- **Tanium Guide:** Benchmarks environments and recommends next best actions
- **Real-time cloud intelligence:** Continuously monitors endpoint health and risk indicators

Scale IT and security operations in a cost-effective way

Reusable workflows and automation frameworks allow teams to streamline repetitive tasks—such as software usage audits or patching processes—while maintaining oversight and control. This enables broader coverage without increasing headcount.

- **Tanium Automate:** Enables low- and no-code playbooks to automate IT and security workflows at scale

Accelerate vulnerability remediation while minimizing organizational disruption

Integrated workflows help bridge the gap between detection and remediation, enabling faster responses to compliance gaps or security findings. Teams can act on shared data and insights to coordinate efforts and reduce exposure time.

- **Remediation Visibility:** Prioritizes critical patches and remediation actions using real-time risk insights across the Tanium platform

Respond quickly to emerging threats

With early visibility into zero-day vulnerabilities and high-severity risks, teams can assess exposure and take informed action. Real-time guidance helps prioritize remediation efforts and minimize operational disruption.

- **Tanium Guardian:** Delivers early insight and expert-verified guidance to help teams assess exposure and respond rapidly to zero-day and high-severity threats

Gain instant answers to endpoint questions

Natural language querying makes it easy for anyone—from operators to executives—to ask questions about their environment and get real-time answers. Whether it's identifying underutilized software, spotting performance issues, or tracking patch status, teams can make faster, data-driven decisions.

- **Tanium Ask:** Enables natural language queries powered by generative AI and real-time endpoint data to deliver instant, actionable insights

Tanium AEM benefits

Tanium AEM transforms how IT and security teams make decisions and execute actions, enabling safe, reliable changes across their environments—at scale and in real time.

Operational resilience

By confidently deploying changes using insights from real-time analysis of global endpoint activity—combined with deployment rings and visibility into the real-time impact of those changes—IT teams can avoid costly disruptions that affect operations and productivity.

Assured compliance

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

Stronger security posture

Proactively identifying, prioritizing, and remediating cyber risks from vulnerabilities and configuration drifts helps protect the organization from threats, safeguard sensitive data, and uphold customer trust.

Scalable IT and security operations

Automate routine tasks to free up teams for strategic initiatives that drive organizational growth and optimize human resource utilization.

Lower support costs

Automatically resolve endpoint issues to reduce IT and security overhead and minimize productivity disruptions.

Increased agility

Real-time data and automation empower IT to respond quickly and adapt to evolving organizational needs.

Customer success story: VF Corporation

VF Corporation, also known as VFC, is a global apparel and footwear company specializing in outdoor, active, and work brands such as JanSport, Eastpak, Timberland, and The North Face. The company needed to evolve and automate its end-to-end patching and security orchestration strategy to boost productivity and protect its network.

VFC now uses **Tanium Automate,** which streamlines IT and security task orchestration through real-time endpoint visibility and data. The company also leverages other Tanium modules, including **Patch, Deploy,** and **Discover.** As a result, VFC benefits from stronger security, real-time visibility, and a faster, more efficient patching process. **Tanium Automate** also enables VFC's patching lead to focus on deep work rather than repetitive, labor-intensive security tasks.

> "My overall experience using Automate has been outstanding so far, the tool is delivering exactly what we expected. We are now able to quickly patch using runbooks and focus on other priorities, knowing that these critical updates are taking place in the background. Plus, runbooks only take about five minutes or so to create. The entire process gives us back countless hours in our schedule."

David Anderson
Patch automation and vulnerability remediation lead, VF Corporation

Tanium AEM for ServiceNow

Tanium AEM for ServiceNow enhances existing joint solutions across ITX, Security Operations, and Integrated Risk Management. These are trusted capabilities that customers already rely on—and now, with AEM, they're not just connected; they're continuous.

- **In IT:** CMDB data stays current and complete, empowering agents to resolve incidents with live data and AI-guided recommendations.
- **In security:** Threats are identified in real time, and remediation occurs at machine speed—before damage can spread.
- **In risk:** Compliance becomes continuous. Configuration drift is caught early. Audit prep is automated, not chaotic.

Additionally, recommended actions—like rebooting a device or uninstalling software—can be deployed directly from the chat interface, with full role-based access controls in place. This drives faster, safer outcomes while reducing reliance on manual troubleshooting.

Tanium AEM and Microsoft

Tanium integrates with several leading Microsoft products, including Microsoft Security Copilot, Defender for Endpoint, Sentinel, Entra ID, and Intune. Tanium's real-time insights complement Microsoft's advanced threat intelligence and analytics services, empowering effective and resilient IT operations at scale.

Tanium received a 2024 Microsoft Partner of the Year Award in the Independent Software Vendor (ISV) Innovation category and was named a finalist in the Microsoft Commercial Marketplace categories for the Global and Americas regions.

One company that's benefiting from Tanium's close integration with Microsoft is the innovative real estate firm Jones Lang LaSalle (JLL). JLL uses Tanium and Microsoft to simplify and enhance security for roughly 90,000 endpoints. The company also reduced cybersecurity spending by about 20%, which translates to $5 million in savings.

> **"By using a best-in-suite approach with Tanium and Microsoft, we have made orchestration and automation more seamless."**

Dane Thomas
Head of global security engineering, JLL

Key takeaways from chapter 5

- Tanium AEM leverages AI-driven automation and real-time data to streamline IT and security operations, enabling rapid, informed decisions and effective risk management across large enterprise environments.
- Tanium AEM includes an expanding set of autonomous controls (e.g., Guide, Adaptive Actions, Guardian) built on the platform's foundational capabilities.

Conclusion

The proliferation of identity-based attacks, endpoint exploitation, and infrastructure compromise continues to rise, demanding a proactive approach to IT security and operations. By identifying and addressing these issues head-on, organizations can mitigate risks and enhance their overall security posture.

The shift from reactive to preemptive vulnerability management—powered by predictive intelligence and real-time insights—is transforming how organizations approach security. Automation, particularly through autonomous endpoint management, is at the forefront of this transformation, enabling real-time threat detection and remediation while improving core IT operations.

Choosing the right IT tools and partners is essential to effectively addressing today's challenges. Tanium AEM stands out as a comprehensive solution that empowers IT and security teams to make faster, more informed decisions by embedding AI/ML into the platform. With its intelligent, scalable automation, Tanium AEM strengthens security posture, accelerates risk mitigation, and boosts operational efficiency.

To learn more about how Tanium AEM can revolutionize your IT and security operations, we invite you to request a personalized demonstration and experience the benefits firsthand.

See Tanium AEM live

SIGN UP FOR A PERSONALIZED DEMONSTRATION →

PRODUCTS FEATURED

- Tanium Autonomous Endpoint Management
- Tanium Ask
- Tanium Confidence Score
- Tanium Remediation Visibility
- Tanium Automate
- Tanium Guide
- Tanium Guardian

ENDNOTES

[1] https://www.fortinet.com/resources/reports/cloud-security

[2] https://www.gartner.com/en/articles/preemptive-cybersecurity-solutions

[3] https://my.idc.com/getdoc.jsp?containerId=prAP51917824

[4] https://www.pwc.com/gx/en/issues/risk-regulation/global-compliance-survey.html

[5] https://explore.tanium.com/resources/gartner-innovation-insight-aem

[6] https://www.talentmsh.com/insights/it-staffing-ratios

[7] https://explore.tanium.com/resources/rp-automation-report-anz

[8] https://www.gartner.com/en/articles/cio-challenges

[9] https://www.uipath.com/resources/automation-analyst-reports/agentic-ai-research-report

[10] https://www.cybersecuritytribe.com/articles/the-2025-reality-of-agentic-ai-in-cybersecurity

[11] https://explore.tanium.com/resources/gartner-market-guide-endpoint-management

[12] https://www.cio.com/article/3845869/how-tech-leaders-are-using-ai-to-solve-10-procurement-challenges.html

TANIUM.

The Power of Certainty.™

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