Ivanti's Cybersecurity Research Report Series

The Autonomous Endpoint Management Advantage

Listen to this report

00:00 **18:00**

Heavy workloads and burnout are eroding IT's ability to focus on strategic priorities. Despite this, many companies overlook time-saving automations.

IT professionals are stretched thin. Nearly two-thirds (62%) report feeling overwhelmed by day-to-day operations. And one in four (23%) say a colleague has resigned due to burnout.

What's behind these troubling numbers?

A significant share of IT professionals say they need better technology. For example, 25% say they don't have an effective tool to proactively remediate end-user issues — a seven-point increase in 12 months.

Autonomous endpoint management (AEM) offers organizations a forward-thinking approach. Autonomous endpoint management enables IT teams to resolve routine tickets and anticipate problems before end users are affected.

IT pros are on board:

- 67% say AI and automation will free up their time for more interesting, fulfilling work.
- 66% believe these tools will allow them to provide better service to end users.

IT teams say AI and automation will improve job satisfaction quality

Q: Which of these positive impacts do you believe AI and automation w organization?

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT professionals (n = 1,251).
Respondents could select multiple options.

The benefits of AEM extend beyond the IT team; AEM tools can also reduce friction in employees' digital interactions. For example, office workers experience an average of 6.3 tech interruptions per month — whether due to tech problems or scheduled updates.

If we assume each of these takes 15 minutes to resolve, tech interruptions cost companies 1.6 hours of productivity per employee monthly. As these micro-interruptions compound across the organization, they create measurable productivity drag.

By solving problems proactively — before end users are even aware — AEM can reduce friction in workflows and help employees reclaim lost productivity.

Despite the promise of automation, most organizations haven't capitalized on the opportunity. Only one in three (32%) say their organizations fully leverage automation within IT workflows.

Less than 1 in 3 organizations have fully leveraged automatic workflows

Q: How well does your organization remediate IT issues and automate p

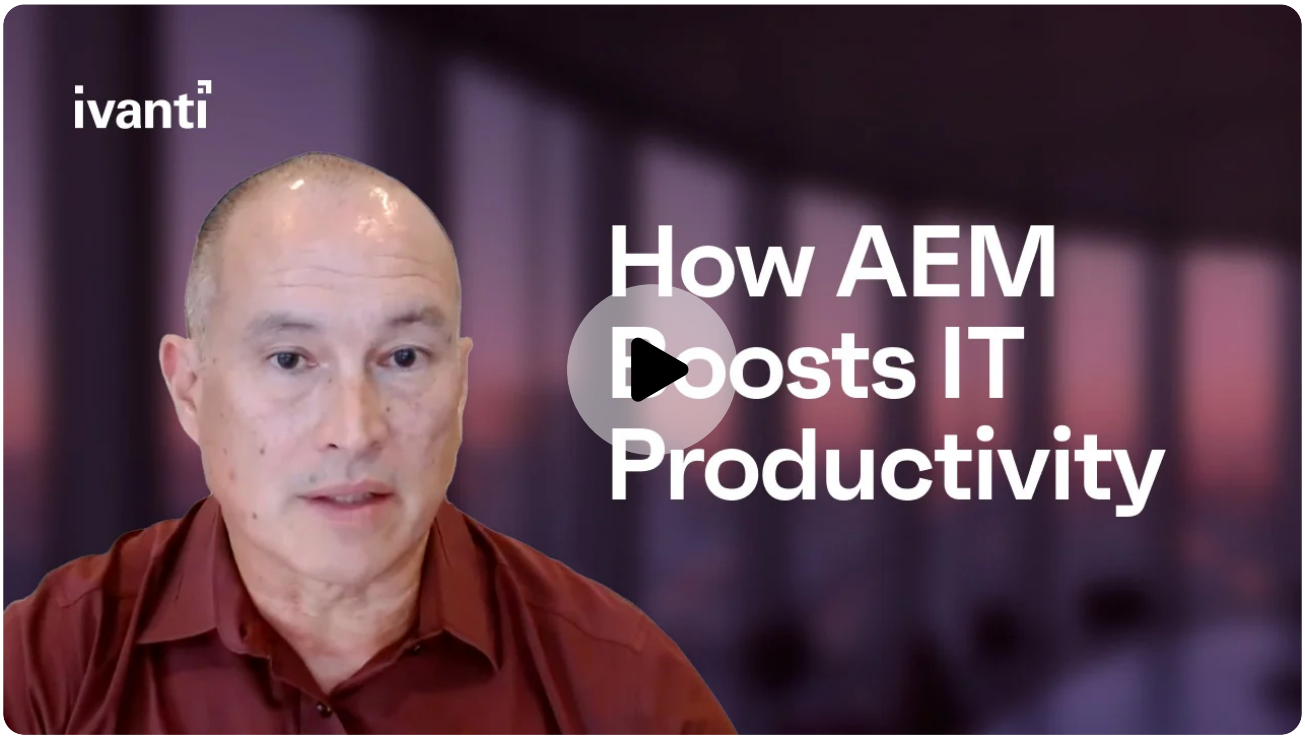
Maturity level	Description
Advanced	Fully automated remediation; proactive issue resolution is ir workflows
Intermediate	Automated for common issues; proactive problem solving i
Basic	Some automation exists; remediation remains largely manu
Poor	Remediation is manual, slow and inefficient; automation is a

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT professionals (n = 903).

Action steps

“Successful adoption of AI and automation hinges not just on deployment, but on robust change management and clear measurement of results — including faster resolution times and increased number of tickets handled via automation. These productivity savings can then be reinvested in upskilling IT teams so they can spend more time on initiatives that create real value for your organization.”

— Tony Miller, Vice President, Enterprise Services, Ivanti



The cyber hygiene gap

Adding to IT's challenges, companies often take a haphazard approach to cyber hygiene, the routine practices that keep systems compliant, secure and updated.

Maintaining cyber hygiene requires consistent, routine effort — but many IT teams are stretched thin, making this essential work challenging. Ivanti's research reveals why maintaining cyber hygiene has become such a difficult responsibility for IT teams:

> **Visibility gaps:** Just 52% of organizations are using endpoint management solutions — down 4 points in one year. Without the centralized visibility of an endpoint management solution, essential cyber hygiene tasks become exponentially harder. IT teams are left manually configuring devices, a time-consuming and error-prone process.
>
> IT pros also tell us they have insufficient data to make decisions across a wide range of dimensions. The biggest blind spots: shadow IT (45%), identifying vulnerabilities (41%), identifying devices accessing the network (38%).

Data blind spots are common and widespread

Q: In which of these areas do you feel you have insufficient data to mak security decisions?

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT and security professionals (n = 1,815).
Respondents could select multiple options.

Challenges with patch management: IT is responsible for executing patch management, yet due to visibility gaps, they struggle to do the job effectively. For example, 38% say they have difficulty tracking patch status and rollouts, and 35% struggle to stay compliant.

IT teams struggle to overcome major patch management cha

Q: What are the biggest challenges you face when it comes to patch ma

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT and security professionals (n = 1,815).
Respondents could select multiple options.

Gaps in security monitoring: Device monitoring helps identify cyber hygiene problems like configuration drift that might otherwise go unnoticed. Yet only 40% say they use fully integrated, automated security and compliance systems. Without this level of monitoring, cyber hygiene issues can silently accumulate.

Action steps

“AI and automation transform IT operations by unifying visibility, streamlining workflows and fostering real collaboration between IT and security teams. This enables organizations to move from reactive troubleshooting to proactive, data-driven management — reducing risk and improving outcomes across their entire endpoint environment.”

— Aruna Kureti, Director, Product Management

Accelerating IT-Ops with AI

IT teams face dual pressures to manage costs and improve service quality. Autonomous endpoint management can help them break down costly silos, boost visibility and streamline IT operations.

Tech sprawl and inefficient tech support are top causes of w spend

Q: In which of these areas does your organization spend its IT budget w

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT professionals (n = 703).
Respondents could select multiple options.

CIOs are under pressure to make their operations more efficient and productive. Among IT pros we surveyed:

- 56% say wasteful IT spend is a problem.
- 39% cite “inefficient tech support” as an area of wasteful spend.

The automation capabilities in AEM solutions can significantly reduce IT inefficiency while preserving service quality … and give IT teams a much-needed break.

AEM reduces wasteful IT spending by optimizing asset lifecycles — tracking devices from acquisition through retirement to maximize utilization, avoid overprovisioning and ensure timely refresh cycles. This lifecycle visibility helps IT leaders make data-driven decisions that reduce both unnecessary purchases and hidden maintenance costs.

AEM tools’ self-healing capabilities reduce the volume of routine service tickets by

automatically detecting and resolving endpoint issues before users submit them. By deflecting these low-level incidents, IT teams can lower support costs and redirect time toward higher-value, strategic work.

But AEM requires the right technology and connected data to work — and so far, these fundamentals are not in place. Among the biggest stumbling blocks:

1. Persistent silos: Nearly all (89%) of IT pros say siloed data negatively impacts their organization's IT operations in one form or another. For example:

- 39% say silos cause them to use resources inefficiently.
- 36% say silos reduce collaboration.
- 35% say silos drive up the risk of non-compliance.

AEM addresses this challenge by bringing together endpoint management, digital experience monitoring and endpoint security into a unified platform. This ensures organizations have the comprehensive visibility needed to automate intelligently — seeing not just device health, but also user experience and security posture in one place.

2. Lack of effective technology to manage and secure endpoints holistically: Just 32% use a unified endpoint management system. AEM's autonomous capabilities are most effective when organizations already have centralized endpoint management in place. Without unified visibility across endpoints, whether using a UEM system or other centralized management tools, adopting AEM becomes significantly more complex.

Ivanti's research shows that most IT teams are juggling multiple disconnected tools — or, in some cases, no centralized management at all. When these tools don't communicate with each other, the asset lifecycle optimization that drives efficiency becomes nearly impossible. IT can't easily track device utilization, identify overprovisioned resources or coordinate refresh cycles across the organization. And workflow inefficiencies can mount quickly. Think: redundant workflows, manual data reconciliation and increased risk of configuration errors.

Disconnected systems make it nearly impossible for IT and security teams to get the complete visibility they need to make informed decisions and take action across the entire endpoint ecosystem.

Action steps

“Key autonomous endpoint management use cases include: zero touch provisioning and eliminating the need for multiple authorization steps; compliance and policy governance via continuous monitoring of devices; and using AI and automation for threat detection and remediation. Automating these use cases allows organizations to optimize IT spending and prioritize more productive, higher-value activities.”

— Scott Hughes, Senior Vice President of Revenue Operations and Corporate IT, Ivanti

Operationalizing autonomous endpoint management

To eliminate inefficiency and waste, companies must integrate AEM into their IT workflows and processes and train IT teams to leverage these high-impact tools.

Autonomous Endpoint Management (AEM) works behind the scenes to continuously discover, monitor and address endpoint issues … before IT ever gets involved.

The benefits are evident:

Accelerated efficiency for IT teams: By using AI and automating core IT tasks — like device provisioning, patch management and performance monitoring — AEM helps organizations increase IT productivity and overall operational efficiency, reduce downtime and free up skilled staff for higher-value work. Ivanti's research finds that 86% of IT pros say AI can make their IT operations more efficient.

More robust compliance: AEM also supports compliance by constantly monitoring endpoints for adherence to security and regulatory policies, quickly remediating any deviations it detects. This approach streamlines the compliance process, simplifies audit preparation and helps organizations avoid potential penalties by ensuring endpoints always remain secure and policy compliant.

Improved business continuity: By identifying and resolving IT issues and security before they disrupt operations, AEM minimizes unplanned downtime and keeps critical business services running smoothly.

Enhanced end-user experience: An AEM approach proactively eliminates digital friction before employees ever encounter it — fixing performance issues and preventing application crashes. The result: Employees stay focused and productive rather than waiting for IT support.

Despite the clear benefits, organizations are still struggling to adopt the technology and embed it within internal workflows. Fewer than half use AI/automation for these high-value IT use cases: predictive IT maintenance (42%), optimizing resource allocation (35%) and compliance checks (32%).

Adoption of high-value AI/automation use cases in IT is mod

Q: In which of these areas does your organization use AI and/or automa

2026 Autonomous Endpoint Management Report | Ivanti
Responses from IT professionals (n = 1,251).
Respondents could select multiple options.

Organizations looking to adopt an AEM approach should focus on four foundational priorities:

1. **Establish comprehensive visibility across the IT and security infrastructure.** (You can't automate what you can't see.)
2. **Prepare your technical infrastructure and processes to integrate AI and automation capabilities into existing workflows.**
3. **Invest in training both IT teams and end users to work effectively with autonomous systems.** IT professionals need skills to interpret AI recommendations and manage escalated issues, while employees need guidance on interacting with AI tools.
4. **Collect employee experience data to continuously evaluate and improve how these human-AI relationships are functioning.**

Action steps

“The business value of autonomous endpoint management can be seen not only in improved IT productivity, but in the positive impact on the digital employee experience and end user productivity as well. Automation and AI can be used to proactively measure and eliminate friction points before employees are impacted — empowering employees to stay productive while freeing IT resources for strategic initiatives."

— Rex McMillan, Vice President, Product Management, Ivanti

Methodology

This report is based on Ivanti's 2025 State of Cybersecurity Report: Paradigm Shift, 2025 Technology at Work Report: Reshaping Flexible Work and 2025 Digital Employee Experiences Report. The three surveys were fielded in October 2024, February 2025 and May 2025, respectively. The studies surveyed a combined total of more than 600 executive leaders, 3,900 IT and cybersecurity professionals, and 8,400 office workers around the world.

The research was administered by Ravn Research, and panelists were recruited by MSI Advanced Customer Insights. The survey results are unweighted.

Products

Customers

Documentation

Partners

About Us

Careers

Events

Blog

Demo Videos

Resources

Glossary

Webinars

Contact Us

Email Opt-in