The High Cost of Manual. The Urgency of Autonomous.

2026 State of Endpoint Management



INFORMATION WEEK

Sponsored by

AUTOMOX

Executive Summary

Every hour spent on manually managing endpoints is an hour lost defending your enterprise. Despite rapid advances in more accessible and intuitive technology than ever, most IT teams are still stuck in manual routines. The cost of clinging to old-school methods is rising. Manual endpoint management drains operational budgets and burns through scarce IT resources.

Time isn't just money, it's a front-line security metric, with mean time to patch (MTTP) and mean time to remediate (MTTR) now defining your organization's potential to avoid fast-moving attacks. This year's State of Endpoint Management report explores the widening gap between awareness and action: Many teams still rely on human-driven processes that slow patch cycles, hinder compliance, and weaken overall security posture. The message is clear: Manual is unsustainable.

Autonomous endpoint management (AEM) represents the next stage of IT maturity where automation, visibility, and security work together to keep every endpoint secure and compliant. By combining policy-based automation with human insight, AEM gives IT teams the speed and control to act decisively and stay ahead of the next threat.

The survey results show:

Manual processes cost more than just time and therefore increase risk

- 43% of teams spent 10+ hours weekly on manual endpoint tasks, of which 6% spent more than 40 hours per week
- 51% of organizations took 5+ days to patch or were unsure of their MTTP
- Only 6% of organizations reported being fully automated

Scale is inhibited by only partial automation

- Teams commonly managed recurring tasks through scripts or custom workflows (57%) and manual procedures (37%) for managing recurring tasks
- 50% automated OS patching, showing that targeted automation reduces routine manual effort without demanding "full automation"

Routine IT challenges slow automation progress

- Top blockers to expanding automation: insufficient budget (35%), legacy systems or technical debt (35%), and skills gaps (34%)
- 27% of organizations allocate less than 10% of IT budget to endpoint management, constraining the time and tools needed to cut manual work

Guardrails promote the confidence needed to scale automation

- Top AEM impediments included data privacy and security implications (46%), followed by risk of incorrect or unauthorized changes
- Most-wanted safeguards before implementing automation: automatic rollback (43%), pause or override anytime (42%), RBAC, and audit logs (42%)

The Real Cost of Manual: Time

43% of teams spent **10 or more hours per week** on manual endpoint tasks, of which 6% spent more than 40 hours per week

51% of organizations either **took 5 or more days to patch** on average **or were unsure of their MTTP**

42% **of teams used spreadsheets** and dashboards to track and report patch and vulnerability statuses

33% spent **10 or more hours per week** building **custom reports**

Only 6% of organizations reported their organizations as **fully automated**

Only 36% were **very or extremely confident** in endpoint compliance visibility

Most organizations are still operating with a high manual tax in their endpoint management processes, and that drag shows up in real business risk. The impact isn't just operational inefficiency but also an increased breach likelihood, higher regulatory and cyber insurance costs, and reputational risk tied to security gaps.

Forty-three percent of teams are spending 10 or more hours each week on manual tasks (and some are spending more than 40 hours), time that should be used to reduce attack surface is instead consumed by process overhead.

Meanwhile, 42% rely on various dashboards or spreadsheets to track patch and vulnerability statuses, which means data becomes stale the longer it sits idle. Key decisions could be made without reliable visibility.

This all adds up to a lack of clarity, directly feeding into slower MTTR and MTTP: **More than half of organizations take five or more days to remediate, or can't quantify their MTTP at all.**

In an environment where exploit kits appear within hours of a CVE being published, a five-day patch cycle can be an open door for exploitation. And because only 36% of teams report high confidence in compliance visibility, leadership often learns about exposure after an audit failure or incident.



"Manual work is the new attack surface," Braunstein said. "Every manual task, whether it's managing tickets, tracking spreadsheets, or manually patching systems — provides extra time for an attacker to exploit something."

RYAN BRAUNSTEIN
Security Manager, Automox

Inaccurate Perception of Efficiency

The survey's data suggests there might be an inaccurate perception of efficiency while manual operations remain. IT teams may believe they're efficient because their current manual processes work. Those processes can even feel faster in the moment, though silently adding costs, such as slower response times or missed opportunities to scale.

It's a concern Automox Security Manager Ryan Braunstein has seen at play many times throughout his career in both large and small ITOps teams, particularly with companies undergoing acquisitions.

"When we were moving through acquisitions and picking up smaller companies, we'd come across IT teams of five and 10 that were doing literally everything manually. They viewed themselves as efficient, not realizing they could take a huge weight off their shoulders by using automated patching solutions," he said. "There's this viewpoint of, 'Well, we're doing a lot of work, we're getting it done, we must be efficient.' But they're not thinking about what their workflow could feel like with automation."

While inefficiency is expensive, the costliest effects of manual work are tied to a slow MTTP and MTTR, which can increase risk. Only about one in ten organizations report MTTP of less than a day.

50% of organizations said they took at least 5 days on average to patch endpoints or are not measuring their MTTP at all.

1 in 10 organizations report MTTP of less than a day.

Organizations need to fix vulnerabilities and respond to attacks on their endpoints in minutes or hours.

As attackers automate zero-day and n-day exploits, manual endpoint management creates dangerous delays, exposing organizations to breaches.

"Manual work is the new attack surface," Braunstein said. "Every manual task, whether it's managing tickets, tracking spreadsheets, or manually patching systems — provides extra time for an attacker to exploit something."

Visibility Gaps Waste Time

The visibility gap slows reporting and diminishes confidence in the data organizations use to make security decisions. Only 19% of teams say it is easy to produce reports for audits or executives, which means most reporting is likely manually collected and interpreted.

The reporting process alone creates drag. Sixty-six percent of respondents said they spent more than two hours per week building custom endpoint management reports. Of those, 33% spent 10 or more hours building reports. Twelve percent of respondents were unsure altogether.

Organizations should think of this as time taken away from improving overall security.

The lag in reporting could inaccurately capture a company's security posture and therefore risk. In short, spreadsheets age fast.

This is a broader fragmentation issue. Only 17% of organizations have a single unified dashboard that provides end-to-end visibility into patch status. This lack of streamlined visibility limits efficiency and increases operational risk. One respondent said:

> **"At present, we rely on a mix of tools, email, chat apps, shared drives and separate project trackers, which result in fragmented information, duplicated work, and delays when retrieving past work or aligning on priorities. Such a siloed setup makes it difficult to maintain a single source of truth, particularly for cross-functional projects."**

When asked who is ultimately responsible for endpoint management, 55% of respondents said IT operations. Second and third places were claimed by systems administration teams and the help desk, respectively.

But when asked who influenced decisions made about endpoint management, 66% of organizations cited security teams. This means security teams need more visibility.

Without maintaining a "single source of truth," as the respondent said, the likelihood of leaders acting on incomplete or outdated information increases.

Why Automation Matters (As a Tool, Not an End State)

Teams commonly relied on

57% scripts or custom workflows

37% manual procedures

for managing recurring tasks — helpful stopgaps but hard to scale and sustain

50% automated OS patching in some form, which is evidence that targeted automation reduces routine manual effort without demanding "full automation"

If one task were automated today, the biggest wins would be

39% patch installation

21% automated rollbacks

20% approval management

The following would improve the ability to report on IT operations:

58% visual dashboards

55% customization

51% AI-generated insights

When asked about recurring tasks, such as patching and software deployment, 23% of organizations said they fully automated these tasks. The most common response (57%) was "partially automated," using scripts or custom workflows.

Just like manual tasks carry the perception of efficiency, partial automation has a similar effect — it reduces steps, but teams are still dealing with disparate pieces of a puzzle.

Thirty-seven percent of organizations reported using manual processes with documented procedures, and 18% regularly relied on manual processes with limited documentation to back them up.

Sometimes these approaches can work in smaller contexts, but companies can't scale them.

As Jason Kikta, Chief Technical Officer at Automox, explained, "Automation doesn't fail because teams don't see the value, it fails because it's never complete. You automate one piece, but the exceptions, approvals, and edge cases all pull you right back into manual work."

That sentiment was echoed by Braunstein, who noted that while manual interventions often kept systems running in the short term, they introduced longer-term risk: "We've got great people doing heroic things manually, but heroics don't scale. Every undocumented script or one-off workflow becomes a liability when that person leaves."

Half of organizations automate OS patching in some form as targeted automation reduces the manual burden on IT teams without demanding full automation. Similarly, 46% of organizations automate endpoint inventorying and monitoring, and 45% automate software deployment and updates.

While partial automation does alleviate teams of some tasks, it won't solve visibility gaps found across workflows or platforms.

One respondent said that beyond automation, the biggest improvement would be a unified system that "consolidates timelines, dependencies, resource allocation, document storage, and real-time communication" to improve transparency and collaboration across the team. Another one said:

"Beyond reducing manual tasks, the single biggest improvement would be centralized, real-time visibility across all endpoints, regardless of location or OS. If we could instantly see patch status, configuration drift and threat indicators in one unified dashboard, it would radically streamline decision-making, reduce response time, and eliminate the guesswork. That kind of clarity would turn reactive firefighting into proactive control."

As organizations seek to gain the most out of automation and start to move toward AI-powered AEM tools, they have high expectations for visibility and reporting, including automating analysis or assembly of reporting.

Respondents said the top improvements for reporting on IT operations would be visual dashboards (58%), customization (55%), and AI-generated insights (51%).

As targeted automation reduces the manual burden on IT teams without demanding full automation:

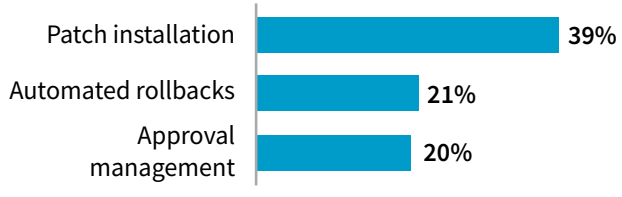
50% of organizations automate OS patching in some form

46% of organizations automate endpoint inventorying and monitoring

45% of organizations reported automating software deployment and updates

Figure 1

If one task were automated today, respondents said the biggest wins would be:



Trust: The Final Barrier to Autonomy

Top blockers to expanding automation:

35% insufficient budget

34% skills gaps

35% legacy systems ortechnical debt

27% of organizations allocate less than 10% of IT budget to endpoint management, constraining the time, and tools needed to cut manual work.

Day-to-day challenges mirror the blockers:

44% too many manual processes

37% insufficient staffing

18% outdated/poor-quality tools

There is an appetite for automation because manual is just not preferred. But the usual challenges, like budget, debt, skills, and staffing, have a hold on IT. These challenges cause a sustained reliance on manual tasks.

And it's a real Catch-22. When a company faces those challenges all at once, the leap to full automation can feel riskier.

IT professionals cited the following as the primary blockers to expanding automation (whether autonomous or not) in their IT environment:

- Legacy systems or technical debt (35%)
- Insufficient budget (35%)
- Skill gaps or lack of automation expertise (34%)
- Insufficient staff (31%)

Each of these barriers is essentially a different way to say: "failure to invest," Kikta said. "I always think of automation like mentoring and delegation. It takes longer to assign a task to someone that they've never done before, and then teach them how to do it rather than just do it myself … but in the long run, we're both better off having done it. Automation is the same way."

For most organizations, endpoint management accounts for a sizable portion of the IT budget, though it is rarely the dominant budgetary concern. More than one-quarter of respondents said they spent less than 10% of their budget on endpoint management.

Figure 2

What percentage of the IT budget is endpoint management?

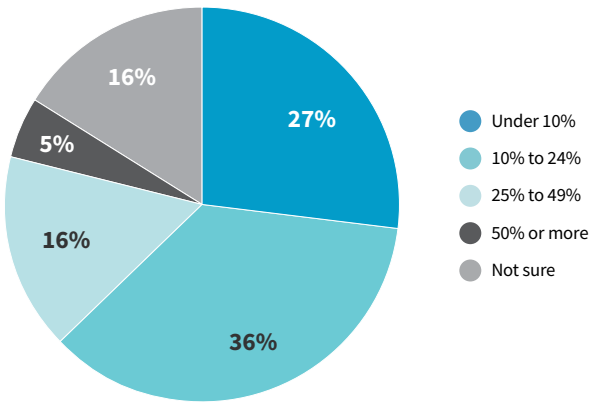
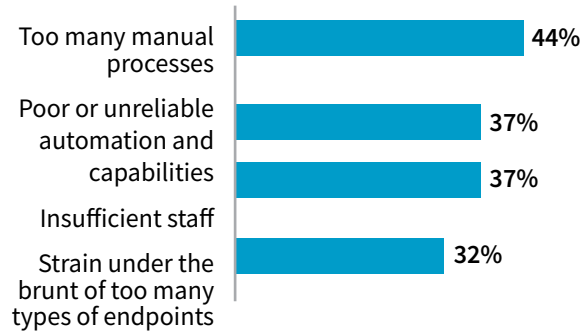


Figure 3

The most common daily challenges of IT mirror the blockers to expanding automation. The top challenges faced by ITOps are:



Note: Multiple responses allowed

Disjointed automation keeps organizations from getting the full ROI of AEM. But there could also be an issue of trust, particularly for IT and security professionals whose main experience of automation is through homegrown scripts and a patchwork of siloed automation tools.

Braunstein suggested starting small — pick one task, automate it, and let the team see the results. Then move on to the next. It's about building a standard and expanding automation, step by step, one win at a time.

When asked about the biggest barriers to autonomous automation, most respondents' issues revolved around trust, visibility, and control, naming the following as AEM impediments:

- Data privacy and security implications (46%)
- Risk of incorrect or unauthorized changes (44%)
- Limited trust in AI-driven recommendations (36%)
- Loss of visibility or control over actions taken (36%)
- Lack of transparency in decision-making (34%)

"These numbers encapsulate one of the biggest fears people have around automation: It's one thing to be wrong. It's a whole other thing to be wrong at scale. If I'm wrong on an individual computer, that's a problem. If I'm wrong on the entire network, I might get fired. If I'm wrong for a day on a backup, that's not good. If I'm wrong for three months, that might end the company. And so that's where people's fears take them."

JASON KIKTA
Chief Information Security Officer, Automox

Figure 4

When asked about the biggest barriers to autonomous automation, most respondents' issues revolved around trust, visibility, and control, naming the following as AEM impediments:



Guardrails Build Confidence

Gradual implementation that can showcase small wins along the way will incrementally diminish those fears. Mounting success will garner more confidence in what might feel like higher-stakes risk.

Even gradual progress, however, requires guardrails and updated policies. Define a desired device state with clear, policy-driven automation to clarify what an automation will enforce, when, and on which devices.

Guardrails push teams beyond their concerns and into autonomy. Guardrails include:

- Visibility into what becomes automatic
- Option to override or pause automation
- Options for rollbacks
- SOC/ITSM ticket generation
- Change-window awareness

A healthy combination of guardrails and automation provide oversight, which in turn builds more trust. IT pros say confidence in AEM comes from tools they can count on, verify, and control, with built-in guardrails that make automation feel safe to trust.

- Most-wanted safeguards before implementing automation: **automatic rollback (43%), pause or override anytime (42%), RBAC, and audit logs (42%)**
- Control over when agent updates are applied is very or extremely important to 74% of respondents, and at least somewhat important to 94%

Remember: **Trust, but verify.**

"Even when an automation is working well, you check in on it. … Humans and computers are good at different things," Kikta said. "We have experience, judgment, and intuition. Computers have speed, scale, repetition, precision, and accuracy," he said.

Effective IT operations depend on a partnership between humans and automation, where human expertise guides automation, and automation delivers consistency and scale.

Survey respondents said the most important safeguards for maintaining safe, reliable automation include:

- Automatic rollback (43%)
- The option to pause or override automation at any time (42%)
- Role-based access controls and audit logs (42%)
- Approval workflows for critical assets (41%)

Nearly three-quarters of respondents (74%) said having control over when agent updates are applied is very or extremely important when evaluating AEM. Almost half (46%) also expressed strong concern about potential agent tampering or unauthorized device actions in autonomous environments.

Figure 5

Survey respondents said the most important safeguards for maintaining safe, reliable automation include:



Conclusion

The 2026 State of Endpoint Management Report makes one thing clear: Manual endpoint management isn't sustainable.

Many organizations spend hours each week on repetitive, error-prone work. **More than half can't patch endpoints fast enough to keep up with today's attacks.** Every hour lost to manual work heightens the risk of breaches, adds burden to IT operations staff, and widens the visibility gap that attackers exploit.

Autonomous technology isn't just an efficiency play for IT operations, it's an urgent imperative for resilience.

Strategic Priorities for Achieving Autonomous Endpoint Management

- **Treat time as the new security metric**

  Insist on MTTR and MTTP as core operational KPIs. Let them guide investment and process decisions the way uptime or SLA targets do.

- **Make a financial case for automation investment**

  Work with chief information security officers and chief financial officers and enterprise risk executives to articulate the soft costs associated with manual work, along with the financial risks associated with leaving endpoints unremediated. Get agreement on these financial metrics to make the case for endpoint automation investments.

- **Evolve from partial to purposeful automation**

  Move beyond scripts and ad hoc workflows toward integrated, policy-driven automation to lay the groundwork for autonomous endpoint management.

- **Make MTTR reduction a shared business objective**

  Position MTTR reduction as a companywide objective, not just an IT metric. Framing it as a business-resilience target builds alignment and urgency across teams.

- **Establish informal metrics to promote baby steps**

  Track short-term KPIs that support IT cleanup, such as reducing the number of endpoint configurations. Fewer variations make automation more resilient and lower MTTP and MTTR.

- **Unify operations and visibility across environments**

  Adopt a single platform that covers all OS types, locations, and teams. Centralization breaks down silos, speeds response, and reduces friction.

- **Build trust before autonomy**

  Implement the right guardrails and visibility tools so teams can confidently adopt processes without fear of losing control.

- **Trust but verify automation performance**

  Use those same tools to audit automation performance monthly. Regular human oversight keeps automation reliable, secure, and trusted.

Demographics/Methodology

The findings of this research are based on an online survey conducted by TechTarget from Aug. 11 to Sept. 16, 2025. A total of 103 IT professionals participated in the research. The sample was generated from TechTarget databases.

Approximately 60% of respondents had titles of IT manager or above and 63% worked for organizations with 1,000 or more employees.

About Automox

Automox is the Autonomous Endpoint Management platform built for autonomous from day one.

Policy-driven, human-controlled automation gives IT and security teams the speed, clarity, and control to reduce risk and move faster with confidence.

Automox unifies automation, visibility, protection, adaptability, and speed in a single, cloud-native platform – enabling teams to automate up to 96% more patches, shorten remediation time, and operate securely at scale across Windows, macOS, and Linux devices.

Learn more at www.automox.com, connect with the Automox Community, or connect with us on X, Threads, LinkedIn, Facebook, Reddit, or Instagram.