Why Endpoint Automation Needs More Than Tools

The Tools Are There. The Outcomes Aren't.

2027 State of Endpoint Management

AUTOMOX | CYBERSECURITY DIVE

Custom content for Automox from Studio by Informa TechTarget

Executive Summary

Endpoint automation is now commonplace, but the operating models around it haven't kept pace with the demands of endpoint management. This has resulted in a persistent gap between technical capability and operational outcomes. Faster patch release cycles, a growing volume of CVEs, and AI-driven vulnerability discovery and exploitation have compressed the window between exposure and incident.

Organizations that rely on manual and reactive intervention to keep up aren't just falling behind; they're more exposed, operating with a disconnect between their tools and processes that attackers exploit.

But teams aren't starting from zero. Most have tools, dashboards, and automation, and many described their operations as mature. However, reality tells a more complicated story.

- **Patching still took days** — 70% of teams reported a mean time to patch (MTTP) of five to 14 days; 24% reported 15 or more
- **Emergency response was rarely immediate** — no organization surveyed could deploy an emergency patch within hours
- **Manual reactive work remained common** — 63% spent 10 to 19 hours per week on manual or reactive endpoint work
- **Knowledge left with employees during turnover** — only 13% said their endpoint operations are very distributed
- **New capabilities typically took months to become predictable production workflows** — 92% needed at least three months; 41% needed more than six

To better understand the operational gap, Automox partnered with Cybersecurity Dive to survey 150 IT leaders and gauge where they were in their journeys between implementation and measurable business outcomes.

The results found that while simple automations were now universal, the future of endpoint management depended on operating models that made automation repeatable, governed, measurable, and resilient, especially as endpoints become more distributed and attackers move faster.

The survey results show:

Nobody can deploy emergency patches within hours

71% take 3-7 days

25% take more than a week

92% need at least three months to turn a new capability into a repeatable workflow

41% say it takes more than six months

84% say endpoint operations are only "somewhat distributed"

One key person leaving puts the whole system at risk

100% say guardrails significantly or moderately eased resistance to autonomous action

Zero respondents reported minimal or no impact

93% use more than five endpoint management tools

57% use more than ten

Yet **40%** still can't measure whether any of it is driving the right outcomes

Finding No. 1: The Operational Debt Is Due

The gap between perceived maturity and operational reality was getting hard to ignore:

81% described endpoint management as mostly or highly automated

92% needed at least **three months** to turn a new capability into a repeatable workflow

99% spent at least **10 hours** per week on manual or reactive endpoint work

Most IT teams use more than five separate tools to manage endpoints, including patching, remote access, configuration, and compliance.

93%
used six or more endpoint management tools

63%
spent 10 to 19 hours per week on manual or reactive endpoint work

while almost everyone else spends
20 to 39 hours

Many teams looked mature on paper, but outcomes told a more complicated story. Sixty-nine percent of organizations described their endpoint operations as "very mature," while 81% said they were either mostly or highly automated. Despite that, 92% said it took at least three months to turn a newly deployed capability into a repeatable workflow. Patching still took eight or more days on average for almost two-thirds of teams, according to the 2026 State of Endpoint Management Report.

The crux of the problem is the operational debt, which is the gap between perceived operational maturity and measurable business outcomes. **In other words, automation might exist, but it often hasn't been embedded into repeatable, governed workflows that produce results reliably.**

Justin Talerico, CEO at Automox, put the problem down to tracking activity over outcomes. "Too many programs are activity-focused, but you can be doing tons of activities and working incredibly hard and still not achieve the outcomes."

He argued that, while teams might work hard and automate extensively, they can still miss the real business objective, such as reducing risk or maintaining performance. After all, conditions drift all the time, and simply too many variables are at play for people to manage directly. Instead, people should be free to define and govern the rules, while allowing machines to handle the fast-moving execution needed to sustain consistent outcomes.

Given the scale of endpoint management, automation is clearly necessary: 72% of the organizations surveyed had over 3,000 traditional computer endpoints, including 41% that managed over 5,000. Third-party software patching, software deployments and updates, and OS patching had been automated across the board. However, without operational discipline and process automation, it was insufficient on its own.

Talerico said he believed the answer wasn't simply to automate more.

> **"Many automated tasks don't become true operational workflows. You have to define the outcome at the policy level up-front, and then prove you're hitting it. Do those two things, and you have a workflow. Skip them, and all you have is a set of automations."**
>
> **JUSTIN TALERICO**
> CEO, Automox

Finding No. 2: More Tools Don't Fix More Problems

Endpoint complexity compounded as tools and environments multiplied:

93% used more than **five** endpoint management tools

57% used more than **10**

40% struggled to determine whether endpoint operations were producing the right outcomes

Endpoints have ballooned in recent years, while management teams accumulate tools faster than they simplify operations. Fifty-seven percent now use more than 10 tools for endpoint management alone, and each added to the maintenance burden. Generally, the more endpoints an organization manages, the higher its tool count.

But complexity isn't just the number of tools or even the number of endpoints. For many, the bigger challenge was often the diversity and connectivity of those endpoints: laptops, desktops, servers, and virtual machines, to name a few. Just over half of respondents cited managing too many endpoint types as one of their top three challenges, while nearly as many cited inconsistent endpoint connectivity with VPNs or too many endpoint management tools as major challenges.

According to Talerico, managing all those endpoints and tools becomes a project unto itself. "We have to purchase tools to help us do our jobs more effectively, more efficiently, at a scale and level of accuracy that we can't achieve on our own. And because those tools are there to serve us, we need to minimize the toil we have to put into them. **No tool is maintenance-free."**

Clearly, there's more to the problem than either a lack or an abundance of tools. More importantly, it's a lack of a standardized operating model that spans that tooling in its entirety. Forty percent of respondents cited difficulty measuring whether their endpoint management operations were driving the right business outcomes, for example.

Measuring return on investment (ROI) was another leading barrier to expanding automation, according to 68% of organizations. But **ROI concerns are themselves another symptom of fragmentation**, where endpoint activity is distributed across such a large stack that leaders struggle to verify whether their tools reduce more operational burden and risk than they create.

Talerico emphasized the importance of enforcing standards for outcomes rather than activities. "You start with a few critical questions. Are my endpoints secure and performant? Are my tools consistently demonstrating those business outcomes? That's verified action from my point of view, and so 'secure and performant' are the strategic business imperatives. Maturity comes with consistently maintaining low risk and high performance in a volatile and higher-velocity world."

> **"Maturity comes with consistently maintaining low risk and high performance in a volatile and higher-velocity world."**
>
> **JUSTIN TALERICO**
> CEO, Automox

Finding No. 3: Most Teams Have Automations, but Few Have an Operating Model

Most organizations still applied automation tactically rather than strategically:

91% treated automation as a tool used where appropriate

9% treated it as a foundation for systems and processes

95% **to 100%** had automated core patching and software-deployment tasks

Automation adoption is now universal, but the clear majority of leaders still treated it tactically, with 91% describing automation as a tool they used where it made sense. Only 9% described it as a foundation upon which to build systems and processes, suggesting that automation tended to be bolt-on rather than an integral part of an endpoint management strategy.

Talerico described what an automation-first operating model would look like, rather than simply adopting another tool. "It's **working backward from the outcomes** to the operational requirements needed to achieve, for instance, reduced risk or higher-performing endpoint fleets."

The perception among many that automation was just a tool aligned with the widespread misconception that automating tasks created autonomous workflows. It doesn't. Most organizations automated core tasks such as third-party software patching and software deployment, but there was still a lot of manual, reactive work, such as identifying which endpoints were exposed or prioritizing which ones to patch.

"That's automation at the system level and not at the organization level," Talerico said. "Instead, you need a sustainable system and process design that's independent of individuals and gives you a risk profile from a C-level perspective. That's what creates a durable foundation."

While teams had automated most of the more obvious tasks, challenges often emerged beyond task-execution problems. This automation plateau happened when teams still lacked automation and consistency for more complex operations, such as enforcing guardrails for exceptions and maintaining visibility into changes. Only once they'd overcome that plateau could organizations build the confidence necessary to believe that automation would behave as intended across different endpoint groups.

Talerico said that once they'd created something, leaders needed to own its entire life cycle. **"You need to have a plan to own the life cycle, because the greater the complexity and the number of things you have to do to achieve your operational goals, the more likely you are to have management drift."**

Cautionary Tale

Highlighting the importance of owning the entire life cycle, Talerico shared an example from a large entity that set up an entire network, with automated maintenance via a contractor. However, after a series of consolidations and reorganizations, the organization lost track of its network for 12 years. It was still being maintained, albeit only at the rate required 12 years earlier. Given the rapid pace of cyberattacks and the emergence of new vulnerabilities, that's a perfect example of an operating model that can't keep up with today's needs.

Finding No. 4: Patching Timelines Are Falling Behind the Threat

Urgency was clearest when current patching timelines were set against today's risk environment:

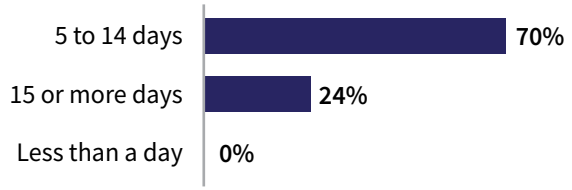
94% reported an average MTTP of **five days** or more

96% needed at least **three days** to deploy an emergency patch

None of the organizations surveyed could deploy emergency patches within hours

Operational debt has serious consequences, largely because it prevents organizations from keeping up with increasingly high-velocity cyberattacks. Patching speed offered the clearest evidence of these consequences.

The average mean time to patch (MTTP) is typically five to 14 days.



Across the board, patching simply wasn't fast enough to keep up with the current threat landscape, especially as attackers use AI to accelerate and scale their attacks. For 71% of respondents, even emergency patching took an average of three to seven days, while one-quarter said it took over a week. It should take a matter of hours.

Talerico said he believed that speed had now become a leadership-level endpoint management issue, and not just a metric for IT operations teams. **"You now have frontier AI models identifying vulnerabilities at a scale that's far beyond human capacity. When risk increases exponentially like that, it becomes an organizational issue.** That compression of time, combined with the increase in volume and velocity, means that the number of things you have to fix and the speed at which you have to fix them is much greater than it's ever been before."

According to Talerico, the underlying technology isn't usually the issue, since it can support much faster patching. The real constraint is whether teams have the governance and operational safeguards to use that technology in a way that balances the risk of a security incident with the risk of business disruption. That requires careful preparation, scoping, and creation of endpoint management policies that align with your business needs and are easy to track.

Talerico said he believed it was about asking the right questions when scoping your policy. "The technology can already patch this fast. The real question is whether you did the preparation. Do you have a rollback mechanism and clear criteria for triggering it? Have you decided who owns exceptions and how those tickets get triaged? **Speed is a governance problem before it's a technical one."**

Industry standards and regulations are steadily catching up with today's requirements. For instance, CISA's recent Binding Operational Directive 26-04 requires federal civilian agencies to prioritize vulnerability remediation based on risk, with the highest-risk vulnerabilities to be remediated within three calendar days. While not a private-sector mandate, it does show where expectations are heading, and private enterprises are likely to be judged on the same operational standards.

Finding No. 5: Proof and Governance Make Automation Safer at Scale

Adoption grew where autonomy was visible, controlled, and reversible:

81% were concerned about data privacy and security

80% were concerned about transparency in automated decision-making

100% said guardrails had eased resistance to self-healing

Business leaders were, for the most part, receptive to automation, but concerns persisted around poorly governed autonomy.

IT executives' top personal concerns about using AI-assisted or autonomous systems in endpoint management are data privacy and security implications, and lack of transparency in decision-making.

81%
Data privacy and security implications

80%
Lack of transparency in decision making

Clearly, the governance gap is the bigger issue, rather than a lack of trust in the technology.

Talerico said he believed leaders should treat trust and governance as inseparable, with trust earned through sustainable, repeatable processes that yield verifiable results. "Autonomous endpoint management needs to keep humans in the middle of the rules of engagement. Humans set the standards and make the rules, and they leave computers to do the heavy lifting of applying those rules quickly and at scale."

Guardrails have emerged as the biggest enabler of the wider adoption of autonomous endpoint management. Fifty-two percent of respondents said guardrails had "significantly eased resistance" to self-healing, while the remainder said they had "moderately eased resistance." On the other hand, **41% also cited a loss of visibility or control over actions** taken as a key concern about using AI-assisted or autonomous systems for endpoint management. That evidence suggests governance hasn't yet matured enough in many enterprises to support broader autonomy.

Talerico shared some examples of technical guardrails that made autonomous behavior more predictable and understandable. "You should never let an autonomous agent directly control patching. That's just wildly dangerous. But an agent can also be fantastic in interpreting human intent and natural language and turning that into a deterministic artifact: 'Here is the patching policy I think you wanted.' If it's not right, you tweak it until the artifact matches your intent, and then that artifact governs execution repeatedly and at scale."

Wider autonomy requires proof, control, accountability, and explainability. With top concerns including data privacy and security, lack of transparency, regulatory restrictions, loss of visibility and control, and the risk of incorrect or unauthorized changes, it's essential to keep humans in command of the rules of engagement, not in the path of every action. After all, **automation without human ownership becomes risk at scale.**

"AI is an assistive technology. It's not a replacement. And I think that's what's lost on so many people and what prevents organizations from guardrailing their AI sufficiently," Talerico said. In other words, **AI is an assistive layer around reliable code, and not a substitute for controlled execution.**

> **"You should never let an autonomous agent directly control patching. That's just wildly dangerous. But an agent can also be fantastic in interpreting human intent and natural language and turning that into a deterministic artifact: 'Here is the patching policy I think you wanted.' If it's not right, you tweak it until the artifact matches your intent, and then that artifact governs execution repeatedly and at scale."**
>
> **JUSTIN TALERICO**
> CEO at Automox

Conclusion: Paying Down the Debt

The debt is payable. Teams that close the gap between perceived maturity and measurable outcomes don't do it by adding more tools or layering on governance for its own sake. They do it by building operating models in which automation is repeatable, accountable, and provably effective.

Respondents were clear about what would help them get more value from endpoint management over the next 12 months:

40% cited ongoing validation that configurations stayed aligned over time

53% cited better reporting on results and impact

39% cited alignment with regulatory compliance standards

Together, those priorities suggest a more durable approach to automation, one built around measurable business outcomes, sustained alignment, and accountability.

Talerico gave endpoint management teams a clear starting point: "Focus on risk and performance as outcomes rather than activities. Remember that even the most rigorous patching practices overlook the majority of risk, which is likely in mitigation rather than remediation, and that means you need rigorous mitigation automation in addition to rigorous remediation automation."

Meanwhile, Talerico advised leaders to begin with a comprehensive inventory and identification. "Humans are good at applying judgment and experience, and taking accountability for their actions. Computers, on the other hand, are good at scale, speed, repetition, and precision. You want to have an audit leveraging the computer for what it's really good at to help you understand the environment you're in. Then you can apply your judgment and experience to go after the things that are most meaningful to do first."

The organizations that get there first will spend less time reacting and more time staying ahead of risk. That's not a distant goal. The report found that most teams had the automation. What comes next is making it count.

Demographics/Methodology

The findings of this research were based on an online survey conducted in partnership with Cybersecurity Dive from May 8 through 12, 2026. A total of 150 IT professionals participated in the research. The sample was generated from Informa TechTarget databases.

All 150 participants worked in IT, held manager or higher titles, and worked for companies with 600 to 9,999 employees. Participants worked in a wide array of industries: Half worked in education, financial services, retail/e-commerce, healthcare/medical, and construction/engineering.

About Automox

Automox is the cloud-native autonomous endpoint management platform trusted by 4,875+ organizations to automate OS and third-party patching, device configuration and policy enforcement across Windows, macOS and Linux. Automox customers automate up to 96% more patches and achieve 362% ROI over three years (IDC, 2025). Getting there is as much an operational challenge as a technical one. Automox Turnkey Results addresses this using data from 1.6 billion policy runs to build a personalized blueprint for each team, mapping their current state to their desired state and continuously validating against drift.

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

© 2027 Automox Inc. All rights reserved. Automox, Automox WorkletTM, and the Automox logo are registered or unregistered trademarks of Automox Inc.



Expert led.
Impact driven.

Studio is Informa TechTarget's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more