

# NinjaOne Predicts 2026

---

The death of Patch Tuesday, AI at the edge, and MSPs lean into co-managed services to fuel growth



ninjaOne®

# 2025 redefined IT and security

AI models and updates emerged weekly, with new global regulations to decipher. The digital landscape grew increasingly complex, paving the way for new threat vectors. And emerging trends like “vibe coding” shifted how we work.

On the other hand, there are constants. The call for tool consolidation has grown louder, and IT organizations are increasingly being asked to do more with less. Meanwhile, the pursuit of AI-driven growth and differentiation shows no signs of slowing down even as murmurs of an “AI bubble” persist.

So, what can we expect in 2026? Here are our predictions for IT teams and MSPs as they gear up for the year ahead.

# Table of contents

AI and autonomous patching will move us beyond Patch Tuesday.	4
AI at the edge will unveil a new era of enterprise IT challenges and opportunities.	5
Fully autonomous AI won't be realized anytime soon.	6
The Digital Operations Center will rise, as the rivalry between IT and security shrinks.	8
2026 is the year the public sector starts looking more like the private sector.	9
Digital employee experiences will become the new employer brand.	10
Co-managed IT and verticalization will be the new MSP growth engines.	12
MSPs will double down on education and enablement for differentiation.	13
Navigating changing frontiers.	14
Citations	15

# AI and autonomous patching will move us beyond Patch Tuesday.

2026 will finally bid adieu to “Patch Tuesday.” Instead of waiting for scheduled drops, we’ll see more organizations move toward [continuous patching models](#) powered by automation, AI, and real-time telemetry from endpoints. Vulnerabilities will be assessed, prioritized, and remediated autonomously, shrinking the time between discovery and fix from weeks to hours. This shift won’t just be about speed — it will reshape how IT and security teams operate.

**“Using automation and AI to improve patch processes is a perfect example of where AI can positively and more efficiently drive business outcomes while closing the gap between historic IT and security siloes,”**

**Mike Arrowsmith**

NinjaOne’s Chief Trust Officer.

AI will also give rise to new threats and [increase](#) the number of anticipated new Common Vulnerabilities and Exposures (CVEs). Having a resilient and adaptive security foundation in place will

become more critical. Rather than building workflows around a predictable monthly cycle, teams that oversee an “always on” patching environment will see greater cyber resilience, compliance, and better efficiencies across IT operations as a result.

“A shift away from monthly patching cycles may face some initial resistance in the enterprise,” adds Tom Molden, NinjaOne CIO of Global Executive Engagement. “Well established processes have evolved over the years, in response to the high level of effort required and fear of business disruption. What’s new is that pragmatic and meaningful use of AI is enabling companies to move towards more autonomous, and always-on patch analysis, prioritization, and deployment. Organizations that lean into automated patch processes will significantly reduce effort and business impact, while at the same time achieving a higher level of patch efficacy. By keeping humans at the center of the AI, companies are able to maintain a “trust-but-verify” stance, without the manual overhead.”

# AI at the edge will unveil a new era of enterprise IT challenges and opportunities.

[According to Gartner®](#), “analysts forecast AI PC shipments will total 143 million units and are projected to represent 55% of total PC Markets in 2026” (1). Additionally, Gartner also predicts that “[40% of enterprise apps](#) will feature task-specific AI Agents by 2026, up from less than 5% in 2025” (2). As new devices roll out and more AI agents are deployed across the enterprise, individuals will have the opportunity to do more faster, but it also means that IT and security teams will face new challenges with access, visibility, and control.

**“As technology improves and organizations refine models for specific use cases, handheld and telemetry devices now have enough computing power to run far more AI workloads locally, rather than relying solely on large cloud data centers,”**

**Joel Carusone**  
NinjaOne SVP of Data and AI.

Better compute presents more opportunities for business, including faster response times, and quicker on-device remediation when outages occur. Though if not properly managed, AI at the edge can lead to a host of new security risks — not to mention the introduction of significant concerns around data leakage and privacy.

The silver lining? If organizations account for growing swaths of smarter endpoints proactively — with the right IT management tools to help scale and manage operations across distributed environments — they’ll enjoy benefits like faster decision-making and quicker technical resolution at the individual endpoint level.

# Fully autonomous AI won't be realized anytime soon.

Despite rapid improvements in models, fully autonomous AI won't materialize in 2026. Barriers like security, compliance, and data privacy will keep organizations cautious when it comes to adopting and implementing fully autonomous AI systems.

“There are a lot of expectations around how close you can get to fully autonomous,” says Carusone. “The ability to achieve fully autonomous isn't hard, but the ability to get there without completely breaking critical systems is difficult. Even if you're at 99% autonomous and that stands to boost your business significantly, but that 1% of risk presents some catastrophic impact to your business or your customers, the cost still outweighs the benefit.”

Not only are autonomous systems still depending on human oversight, but models also aren't sophisticated enough to operate autonomously at a price point that makes sense for the average organization. While computational capacity grows every year, there is still a long way to go before we get to a place where people can trust AI tools to make the most crucial decisions for individuals or for the business completely on their own.

As organizations and enterprises look to gain more value from their AI investments in 2026, we'll see two things happen: more organizations will turn to smaller, domain-specific AI models to automate use cases, solve targeted problems, improve ROI, and reduce exposure to systemic risks. And the pendulum will swing back towards more thoughtfully incorporating AI into organizational systems and processes [in a way that augments](#), and doesn't replace, human expertise.

**“When we talk about AI, it's about really prioritizing safe and thoughtful adoption. (...) How do I let a computer do a thing that a computer should be doing, and a human shouldn't? How can I free up my team for more high-value tasks and objectives? It's questions like these that should guide where and how organizations are leaning into AI. Let AI do things like data normalization — things that computers are historically quite good at, and humans aren't. But don't use AI just for the sake of using AI.”**

**Egon Rinderer**

NinjaOne SVP of Federal and Enterprise Growth

Digital **shifts**,  
renewed momentum,  
and **redefined**  
experiences.

# The Digital Operations Center will rise, as the rivalry between IT and security shrinks.

As team siloes collapse towards a unified digital operations function, the long-standing IT and security divide will close fast.

IT and security teams will continue to blend into a single unit that owns both protection and resilience. Enter the Digital Operations Center (DOC): a consolidated hub where infrastructure, security, compliance, and user experience are managed as an integrated whole, with Chief Trust Officers at the helm.

“More and more, we’re seeing IT and security’s main purview being resilience,” says Arrowsmith. “How can you respond quickly to address and remediate issues when they inevitably occur? Modern organizations tend to reach resolution more quickly when there are strong communications channels established across IT and security.”

Additionally, a rising “shift left” mentality across IT lends credence to the DOC model.

**“Vulnerability management, compliance, and browser management in the AI era are all areas where stronger collaboration between IT and security teams represent significantly better security and business opportunities for organizations,”**

**Rahul Hirani**

NinjaOne’s Chief Product Officer

“Incorporating IT into traditionally long-held security processes earlier on in the planning process leads to less toil and reactive work for IT teams.”

For instance, as shadow AI becomes a larger factor in enterprise security and operations, IT teams charged with provisioning and monitoring (of not just apps, but AI tools too) are now essential counterparts to traditional security functions. “We’ll continue to see this gap close as core IT competencies increasingly overlap with and play an outsized role in driving organizational security and compliance,” Hirani adds.

---

# 2026 is the year the public sector starts looking more like the private sector.

For years, the public sector has been known to move cautiously, bound by outdated infrastructure, limited resources, and as a result, resistant to modernization. But in 2026, that story flips. With new procurement processes, a relentless drive towards efficiency, and compliance mandates coming into effect, public sector organizations are being forced — and empowered — to modernize quickly.

“What will help the federal government close the gap with the private sector are streamlined programs and procurement processes like FedRAMP,” says Rinderer. “Initiatives like [FedRAMP 20x](#) are game changers because they lower the cost and barrier to entry for more next-gen, modern SaaS companies to start directly working with the federal government in ways that weren’t previously possible. That access will strengthen the technical capabilities and tooling at the government’s disposal.”

For State, Local and Education (SLED) organizations, ongoing modernization efforts will continue, with tool consolidation and cost efficiency top of mind. “Having things like AI and enhanced capabilities at the edge will democratize work being done by smaller teams,” says Aaron Kinworthy, NinjaOne VP, Public Sector.

**“Both small and large organizations have limited resources, but with modern technology, they’re better enabled to focus on executing bigger projects and initiatives. That results in much better and more efficient experiences for both SLED organizations and the constituents they serve.”**

**Aaron Kinworthy**  
NinjaOne VP, Public Sector

---

# Digital employee experiences will become the new employer brand.

In 2026, digital employee experience (DEX) will sit alongside salary, benefits, and culture as a core part of an employer's value proposition. Tomorrow's candidates will increasingly evaluate prospective employers based on the seamlessness of their digital workplace — how easy it is to access tools, how frictionless security feels, and how well technology enables collaboration rather than hinders it.

[Gartner notes that](#), “greater focus on DEX improves the relationship between IT and the workforce and can improve talent retention” (4). On the flipside, enterprises that neglect DEX will see it show up in offer declines, retention struggles, and Glassdoor reviews that cite “tech frustrations” just as often as bad managers. Conversely, organizations that invest in intuitive, integrated, AI-enabled digital experiences will turn their tech stack into a recruiting superpower.

**“IT responsibilities are evolving. It’s not enough to ensure that infrastructure or devices are online and operational. IT’s responsibilities are increasingly extending to making sure that the overall experience is positive for all end users,”**

**Rahul Hirani**

NinjaOne’s Chief Product Officer

By the end of the decade, “digital employee experience” won’t be an IT metric — it will be a top-line differentiator in both the battle for top talent and the business bottom line.

MSP accelerants:  
**Powering**  
**next-year growth**

# Co-managed IT and verticalization will be the new MSP growth engines.

MSPs working closely with internal IT teams will lead to more furious growth opportunities in the new year. Those that can tailor service offerings to augment existing internal IT functions, operations, and business objectives, while demonstrating an ability to improve organizational outcomes while driving down operational costs, will unlock new levels of differentiation and demand.

**“The data shows that tech buyers prefer a hybrid approach that involves a mix of in-house and managed services provider (MSP). Tech buyers recognize the importance of having a skilled in-house IT team... however, they also value the skills and expertise that MSPs bring to the table.”**

**IDC**


Pairing internal IT context and control with MSPs’ specialized talent will be the winning strategy. Additionally, MSPs as service providers can no longer control what technology clients use,

and as a result, what technologies they can support. “Today, the client and the market trends define the technologies you have to support,” says Paul Redding, NinjaOne’s Head of MSP Partnerships. As a result, more MSPs will also double down on verticalization — positioning themselves as digital experience experts in healthcare, retail, finance, or other industries — to boost their competitive advantage and grow more efficiently. “Find the clients that you have, and lean into their markets,” Redding advises. Learning what you can about their unique needs and standards, and finding ways to monetize those services, will be what best position MSPs for growth.

In the end, MSPs that can move past being service providers and become trusted educators and strategic growth partners, for both internal IT teams and customers within specific industries, will be the ones best positioned for success and scale.

---

# MSPs will double down on education and enablement for differentiation.



The break/fix era has long been dead — and so is the mindset that MSPs are simply outsourced IT. In 2026, winning MSPs won't just sell tools or uptime; they'll sell knowledge and enablement, which will drive a greater competitive advantage for their clients and themselves.

“MSPs moved past break/fix a long time ago,” says Redding. “What’s happening now is a new, forced evolution from selling subscription IT services to delivering business outcomes.

**“Customers are no longer satisfied if their MSP ‘just makes things work.’ They expect you to help them learn how to leverage advanced technology like AI to grow their business or streamline their operations—and that will ultimately create more growth for MSPs.”**

**Paul Redding**

NinjaOne's Head of MSP Partnerships

MSPs that hone in on business differentiation for customers, like selling compliance as a service or adding marketing services, are the MSPs that stand to grow their business most significantly in the new year.

# Navigating changing frontiers.

There's no way to predict exactly what 2026 will hold. But it's evident that organizations will continue to lean into more modern, highly scalable endpoint and IT management operations to drive differentiated business outcomes, employee experiences, and more competitive offerings.

At its core, IT success in 2026 will hinge on the success of the end user. Organizations that can keep humans at the center of their technology, implementation, and enablement strategies will be the ones that win out in the new year.

To learn more about where NinjaOne can help your organization simplify digital work, and reduce IT cost, risk, and complexity in 2026, visit: [www.ninjaone.com/endpoint-management/](https://www.ninjaone.com/endpoint-management/)



# Citations

1. Gartner Press Release, “Gartner Says AI PCs Will Represent 31% of Worldwide PC Market by the End of 2025,” August 28, 2025. [www.gartner.com/en/newsroom/press-releases/2025-08-28-gartner-says-artificial-intelligence-pcs-will-represent-31-percent-of-worldwide-pc-market-by-the-end-of-2025](https://www.gartner.com/en/newsroom/press-releases/2025-08-28-gartner-says-artificial-intelligence-pcs-will-represent-31-percent-of-worldwide-pc-market-by-the-end-of-2025)
2. Gartner Press Release, “Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025,” August 26, 2025. [www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025](https://www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025)
3. IDC Tech Supplier, Worldwide Services Survey Spotlight: Do Organizations Prefer to Use In-House IT Resources Over External Managed Services Providers for IT Requirements?, #US53147325, Feb 2025
4. Gartner Research, “Predicts 2025: Transform End-User Services Into a Predictive and Resilient Digital Workplace,” Lina Al Dana, Dan Wilson, Erin Pierre, Tom Cipolla, Stuart Downes, Sunil Kumar, February 19, 2025. [www.gartner.com/en/documents/6187855](https://www.gartner.com/en/documents/6187855) (Accessible to Gartner clients only)