Solution Brief

Ivanti Autonomous Endpoint Management: Scale IT, Reduce Risk, Drive Productivity

Ivanti Autonomous Endpoint Management (AEM) brings endpoint security, risk-based patching and governed AI together through a trusted system of record that helps teams reduce risk, automate confidently and stay ahead of disruption.

The challenges IT and security teams face today

Security risks from unpatched endpoints

Every unpatched endpoint is a potential breach waiting to happen. IT and security teams are caught in an impossible race: AI has accelerated the speed at which threat actors can discover potential exposures, and IT teams are expected to prioritize, test and deploy patches constantly despite ever-expanding attack surfaces and limited resources. 2026 research from Ivanti revealed that IT's biggest hurdles to overcome in patch management are prioritizing risk remediation, deploying patches efficiently and balancing security urgency without disrupting business operations.[1] To keep pace in the AI-accelerated threat era, traditional patch management approaches no longer cut it.

Limited IT resources and flat budgets

IT professionals are stretched thin, constantly asked to do more with less as the gap between demands and resources widens. Budgets remain frozen while device counts grow, user expectations rise, and technology complexity multiplies. In fact, according to Ivanti's Digital Employee Experience Report, nearly two-thirds (62%) of IT professionals report feeling overwhelmed by day-to-day operations, and one in four (23%) say a colleague has resigned due to burnout.[2] Scaling your operations requires a smarter, autonomous approach— not additional hours, more headcount or more disconnected tools.

Visibility gaps and fragmented tools

IT leaders are managing increasingly complex environments with incomplete, contradictory data scattered across disconnected systems. In 2026, just 52% of organizations use endpoint management solutions — a decrease of 4 points in just a single year.[3] Without centralized visibility, essential cyber hygiene tasks become exponentially harder, leaving teams to manually configure devices with time-consuming and error-prone processes. Trusted visibility is the foundation of effective endpoint management, security and automation. Without it, every remediation decision carries unnecessary risk.

Negative impact on employee productivity and experience

When endpoints are poorly managed, your digital employee experience (DEX) suffers, which directly impacts retention rates and hurts the company's bottom line. On the positive side, the business impact of effectively managed DEX is substantial. IT professionals overwhelmingly agree that a strong DEX positively affects employee productivity (87%), satisfaction (85%), and retention (77%).[4] Our goal is to help you eliminate friction and turn endpoint management into a powerful driver of employee success.

Manual patching leaves exposure windows open	**Periodic assurance is not continuous compliance**	**Visibility gaps weaken governance**

38% Difficulty tracking patch status widens vulnerability windows during critical threat periods.	**35%** Manual tracking creates gaps between scheduled checks and real-time regulatory requirements.	**45%** Organizations still lack trusted context across shadow IT, devices, and vulnerabilities.

The solution: What Ivanti Autonomous Endpoint Management delivers

Ivanti Autonomous Endpoint Management helps organizations establish trusted data authority, automate within defined guardrails, and move from reactive operations to proactive IT.

Trusted visibility and data authority

Ivanti establishes a trusted, continuously updated view of devices, software, configurations and exposures to ensure every decision, workflow and remediation is built on trusted, accurate context. By bringing managed, unmanaged, and shadow IT assets into one trusted system of record, the platform lets teams make faster decisions, automate with confidence and eliminate blind spots across their entire environment.

Governed AI and IT efficiency

Built on trusted endpoint data, Ivanti helps teams assess, assist and automate through governed AI workflows. Organizations can reduce ticket volume and scale operations while maintaining human-in-the-loop oversight, accountability and appropriate decision controls.

Autonomous remediation

Ivanti helps organizations to move from reactive support to proactive, autonomous remediation. With self-healing capabilities and automated resolution, the solution prevents common endpoint issues before they escalate, deflecting tickets and freeing IT and security teams to focus on higher-value, strategic work.

Productive, frictionless digital experiences

Technology should enable teams to work better, not hinder their efforts. Ivanti detects experience issues early and remediates them automatically, significantly reducing downtime. The platform ensures employees stay productive while helping IT deliver a seamless, highly reliable digital workplace.

Autonomous patching and continuous compliance

Ivanti takes the guesswork out of vulnerability management. Our autonomous endpoint management solution prioritizes and automates patching based on real-world risk, active exposure and your organization's specific risk appetite. It then verifies the results and maintains continuous compliance through governed, automated workflows.

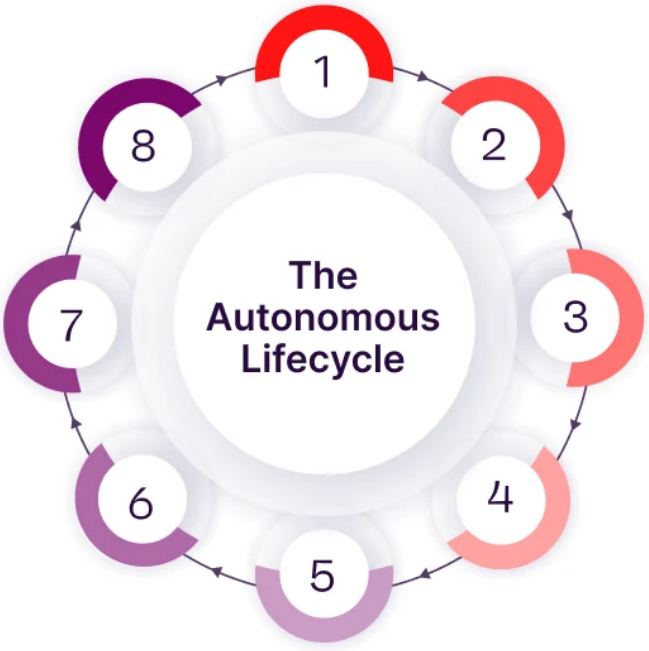
Security by design, built into operations

Security is integrated into endpoint operations from the outset. Through continuous discovery, strict policy enforcement, exposure reduction and coordinated workflows, Autonomous endpoint Management bridges the gap between IT and security operations, ensuring organizations remain secure by design from the ground up.

The autonomous lifecycle

While basic automation executes individual tasks, Autonomous Endpoint Management continually discovers, prioritizes, remediates, and optimizes across your entire IT ecosystem. Ivanti ensures that every action delivers a measurable result. This intelligent, self-healing approach doesn't just save time—it actively hardens security, enforces compliance, and guarantees a frictionless digital experience for every user.

1. **Establish trusted visibility** with a continuously updated view of devices, software, configurations and exposures.
2. **Manage every endpoint** throughout its entire lifecycle across enrollment, policy, configuration, app delivery, security and retirement.
3. **Deploy at scale** by streamlining device enrollment, OS provisioning and application delivery.
4. **Protect and secure** access and connectivity across the entire environment.
5. **Patch autonomously** by prioritizing devices based on risks and active exposure.
6. **Support remotely** to resolve issues faster and keep employees productive.
7. **Automate routine tasks** and troubleshooting at scale to dramatically improve IT efficiency.
8. **Optimize IT** operations through proactive, autonomous remediation.



Ivanti Autonomous Endpoint Management in action

South Star Bank transformed its endpoint management by moving from traditional reactive patching to continuous, autonomous remediation using Ivanti Autonomous Endpoint Management. This shift addressed visibility gaps and compliance challenges in a highly regulated financial environment, enhancing security and operational confidence.

- **Confidence gaps in traditional patching:** Traditional patch management relies on assumptions about device reachability and patch success, often leading to silent failures and delayed validation, which creates uncertainty during high-risk vulnerability events.
- **Establishing data authority:** With Ivanti's solution, South Star Bank unified endpoint discovery, asset inventory, configuration and patch status into a single system of record built on a trusted data foundation that enabled accurate visibility and safe automation of remediation.
- **Implementing autonomous management:** Continuous monitoring and automatic remediation informed by organizational policies allowed vulnerabilities to be addressed promptly with verification and escalation of failures, reducing manual workload and stress for their IT teams.
- **Business and security outcomes:** Continuous patch compliance minimized exposure windows, improved frontline productivity by reducing disruptions and freed IT staff to focus on strategic initiatives. Overall, South Star enhanced their overall security posture and operational resilience.

As Jesse Miller, Director of Desktop Engineering at South Star Bank, described:

"I was able to reach out and touch everything and really get information, and see the power of viewing, analyzing, solving problems quickly… to where we could basically see what was happening and solve problems before our customers knew they had them."
— Jesse Miller, South Star Bank

This clarity did not exist before autonomy. Leadership recognized that without continuous visibility and verification, patching cycles created anxiety rather than confidence.

Ivanti Autonomous Endpoint Management delivers a seamless, end-to-end journey. By establishing trusted endpoint data and unified management and executing risk-based patching and autonomous remediation, Ivanti integrates provisioning, app delivery, troubleshooting and advanced analytics into one powerful platform.

Establish trusted visibility

Comprehensive visibility enables continuous discovery of managed and unmanaged IT assets (including shadow IT). This allows IT and security to reduce potential risk blind spots and establish a trusted foundation for secure, automated workflows. This enables organizations to maintain a continuously updated inventory of devices, configurations, ownership details and endpoint context so their teams can act with confidence.

Examples:

- **Asset discovery:** Discover unmanaged laptops and unknown devices connecting to the network.
- **Device inventory:** View device ownership, OS version and encryption status in one place.
- **Software estate management:** Identify outdated software versions, unused apps and unapproved tools across the estate.

Manage and deploy at scale

Manage Windows, macOS, iOS, Android, Linux, and ChromeOS devices across enrollment, policy, configuration, app delivery, security and retirement from one platform. Provision new devices faster with modern enrollment workflows and enable employees to install approved apps from a self-service catalog without opening a ticket.

Examples:

- **Multi-OS endpoint management:** Apply a new policy across corporate Windows and macOS devices at once.
- **Device enrollment and OS provisioning:** Provision a laptop for a new hire with apps, settings, and access preconfigured
- **App deployment and self-service:** Enable employees to install approved apps from a self-service catalog without opening a ticket.

Protect, patch and support

Deliver risk-aware, autonomous patch management across macOS and Windows, continuously reducing exposure and keeping devices protected. Apply conditional access, secure connectivity and governance policies across device types to strengthen compliance and reduce risk.

Examples:

- **Risk-based patch management:** Prioritize and deploy a critical patch to vulnerable devices before the next maintenance window.
- **Secure access, app access, and governance:** Block access to sensitive apps from noncompliant or unmanaged devices.
- **Remote support, control and device actions:** Restore access during a help desk session by remotely connecting to a device and restarting a service.

Automate and optimize operations

Take one-to-many action across device groups to resolve issues, enforce changes and reduce manual effort at scale. Use bot actions and autonomous remediation to diagnose, fix and automate routine work with governance and control so teams can scale without added complexity.

Examples:

- **Fleet remediation and bulk actions:** Remove a risky application or update a configuration across thousands of endpoints in one action.
- **Autonomous actions and bots:** Detect low disk space and clear temporary files before users notice a problem.
- **Experience and endpoint analytics:** Spot recurring boot performance issues and target remediation before they drive new tickets.

Ivanti Autonomous Endpoint Management value

Customer Zero: Autonomy at Scale - Proven Results. Measurable Impact.

- **Financial results:**
  - **483%** documented ROI 8-month payback period
  - **$11.2 million** in total financial benefits over three years.
- **Productivity gains:**
  - **55,600 hours** of employee productivity gained annually.
  - **66,000** manual tasks automated annually.

Ivanti deployed our Autonomous Endpoint Management solution to demonstrate real, impactful results that validate the Autonomous Endpoint Management narrative with undeniable operational evidence. By operating as Customer Zero, Ivanti documented a staggering 483% ROI and an 8-month payback period. This serves as clear proof that autonomous models scale economically, leaving manual, legacy approaches behind. Learn more.

Transitioning to Autonomous Endpoint Management isn't just an IT upgrade; it’s a catalyst for business transformation. When organizations establish trusted data authority and deploy governed autonomy, they fundamentally shift the economics of endpoint management and drive stronger security, continuous compliance and unmatched resilience. Ivanti has experienced the results of these benefits firsthand. The technology is ready. How quickly will your organization seize the advantage?

References:

1. The Autonomous Endpoint Management Advantage | Ivanti
2. 2025 Digital Employee Experience (DEX) Report and Trends | Ivanti
3. Ivanti as Customer Zero: Transforming IT & Security Operations with AEM | Ivanti
4. 2025 Digital Employee Experience (DEX) Report and Trends | Ivanti