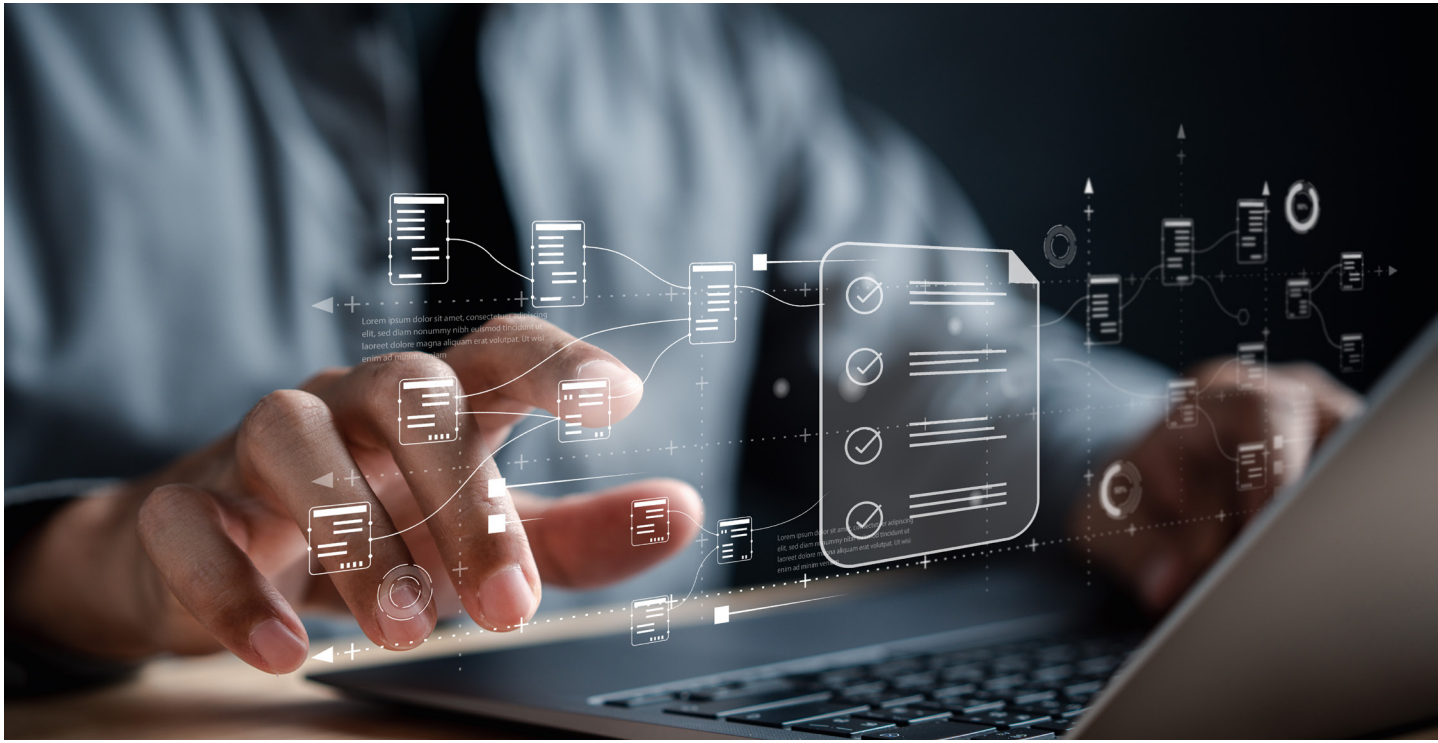
ivanti

SOLUTION BRIEF

Ivanti Autonomous Endpoint Management

Autonomous. Predictive. Protective. The Future of Endpoint Management Starts Here.

Organizations today face unprecedented endpoint complexity—spanning desktops, mobile devices, rugged hardware, and IoT—while battling rising security risks and flat IT budgets. Manual processes and fragmented tools leave endpoints vulnerable, impacting compliance and employee productivity. Ivanti Autonomous Endpoint Management (AEM) transforms endpoint operations with AI-powered automation, risk-based patching, and self-healing capabilities. By unifying management across all devices and OS platforms, AEM helps IT and security teams reduce risk, scale efficiency, and deliver frictionless digital experiences.



Customer Challenges

- 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: vulnerabilities are discovered daily, patches are released constantly, and critical-severity exploits are weaponized within hours—sometimes before patches are even available.
- Limited IT resources and flat budgets: IT teams are being asked to do more with less—and the gap keeps widening. Budgets are frozen or shrinking while device counts grow, user expectations rise, and technology complexity multiplies. The math simply doesn't work.
- Poor visibility and fragmented tools: IT leaders are flying blind, managing an increasingly complex environment with incomplete, contradictory data scattered across disconnected systems. It's like trying to complete a jigsaw puzzle when half the pieces are missing and the other half are from different boxes.
- Negative impact on employee productivity and experience: Your employees chose to work for your company—but their technology experience is making them reconsider. Every friction point, every delay, every IT roadblock chips away at productivity, morale, and ultimately retention.

Ivanti Autonomous Endpoint Management (AEM) Solution Overview

Ivanti AEM delivers a next-generation approach to endpoint management:

- AI-Powered Automation: Automates patching, compliance enforcement, and onboarding.
- Unified Management: Supports all devices—Windows, macOS, iOS, Android, ChromeOS, rugged, and VR/XR—from a single platform.
- Self-Healing & DEX Optimization: Proactively resolves issues and enhances employee experience through intelligent workflows.

Core Use Cases

- Risk-based patch management: Automatically prioritizes and applies patches based on vulnerability severity and exploit likelihood
- Zero-touch device onboarding: Fully automated provisioning of new endpoint devices without IT intervention
- Self-healing capabilities: Detects and resolves performance or security issues autonomously
- Digital Employee Experience optimization: Uses telemetry and AI to proactively address user-impacting issues
- Automated Software Lifecycle Management: Handles deployment, updates and retirement of applications
- Continuous compliance enforcement: Real-time monitoring and remediation of configuration drift

Key Capabilities

- Comprehensive Visibility: Real-time asset discovery and endpoint visibility across all devices and environments. Eliminates blind spots and ensures accurate inventory for compliance and optimization.
- AI-Driven Automation: Self-healing endpoints that remediate issues automatically, humans in the loop, autonomously patching across OS and apps to reduce risk proactively.
- Proactive Risk Reduction: AI-powered threat prevention before issues arise. Continuous compliance monitoring and vulnerability remediation. Integrated risk-based patching and vulnerability management.
- Broad OS and device support: Unified management for Windows, macOS, Linux, iOS and Android including rugged and VR/XR.
- Zero-Touch Provisioning & Self-Service: Automated device onboarding and configuration. Self-service capabilities for end-users to reduce IT workload and improve experience.
- Connected ecosystem: Unified platform combining UEM, DEX, and security capabilities.
- Integrated ITSM and Security: Native integration with ITSM and security workflows. End-to-end without silos aligning IT & Security operations.

What Makes Ivanti AEM Different

See everything, miss nothing

Your IT environment is constantly evolving—new devices, shadow IT, remote workers. Ivanti AEM delivers real-time visibility across every endpoint, every OS, and every location. No more blind spots that leave you vulnerable or non-compliant. You get a complete, accurate picture of your entire estate, so you can make informed decisions with confidence.

IT that fixes itself

Why wait for tickets when problems can solve themselves? Ivanti AEM's AI-driven automation detects and remediates issues before users even notice—patching vulnerabilities across operating systems and applications autonomously. Your team shifts from firefighting to innovation, while your security posture strengthens continuously.

Stop threats before they start

Security teams can't afford to be reactive anymore. Ivanti AEM uses AI to predict and prevent threats before they materialize. With continuous compliance monitoring, intelligent vulnerability remediation, and risk-based patching working in concert, you're always one step ahead of attackers—not one step behind.

One platform, every device

Windows laptops, MacBooks, Linux servers, mobile devices, even rugged handhelds and VR headsets—your users work on everything. Ivanti AEM manages it all from a single pane of glass. Finally, unified control without the complexity of juggling multiple tools or platforms.

Empower users, free up IT

Nobody wants to wait for IT to set up their device or fix basic issues. With zero-touch provisioning and intelligent self-service, new employees are productive from day one, and experienced users solve their own problems instantly. Your IT team reclaims hours every week to focus on strategic initiatives instead of routine requests.

Break down the silos

When UEM, digital experience monitoring, and security operate in isolation, problems slip through the cracks. Ivanti AEM connects it all—native integration with your ITSM workflows means IT and Security finally speak the same language. One ecosystem, one source of truth, one streamlined operation.

IT and security, aligned at last

The days of IT and Security working at cross-purposes are over. Ivanti AEM integrates seamlessly with your existing security and service management tools, creating end-to-end workflows where visibility, action, and governance flow naturally. Operations become faster, smarter, and dramatically more secure.

About Ivanti

Ivanti breaks down barriers between IT and security so that Everywhere Work can thrive. Ivanti has created the first purpose-built technology platform for CIOs and CISOs – giving IT and security teams comprehensive software solutions that scale with their organizations' needs to enable, secure and elevate employees' experiences. The Ivanti platform is powered by Ivanti Neurons - a cloud-scale, intelligent hyper automation layer that enables proactive healing, user-friendly security across the organization, and provides an employee experience that delights users. Over 40,000 customers, including 85 of the Fortune 100, have chosen Ivanti to meet challenges head-on with its end-to-end solutions. At Ivanti, we strive to create an environment where all perspectives are heard, respected and valued and are committed to a more sustainable future for our customers, partners, employees and the planet. For more information, visit ivanti.com and follow @GoIvanti.

ivanti

Learn more at Autonomous Endpoint Management Solutions or contact your Ivanti representative today.