

AUTONOMOUS ENDPOINT MANAGEMENT

Trusted Data. Governed AI. Proactive Remediation.

The Future of SLED Endpoint Management Starts Here.

State & local governments and educational (SLED) organizations face unprecedented endpoint complexity. This complexity spans desktops, mobile devices, hardware and IoT, while battling rising security risks and constrained IT budgets. Manual processes and fragmented tools leave endpoints vulnerable, impacting compliance and workforce productivity. Ivanti Autonomous Endpoint Management brings endpoint security, risk-based patching and governed AI together through a trusted system of record.

By establishing trusted data authority and unifying management across all devices and OS platforms, Autonomous Endpoint Management helps IT and security teams reduce risk, scale efficiency and deliver frictionless digital experiences across every agency, department and campus.



SLED 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. AI has accelerated the pace at which threat actors can discover and exploit potential exposures, and teams are expected to constantly prioritize, test and deploy patches despite ever-expanding attack surfaces and limited resources. For state and local governments and schools, the stakes are even higher — ransomware gangs and other bad actors have made municipalities, counties, school districts and universities some of their most frequent targets.

Limited IT resources and constrained budgets:

State, local and education IT teams are being asked to do more with less, and the gap keeps widening. Budgets are frozen or shrinking while device counts grow, staffing levels are frozen 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.

Negative impact on workforce productivity and service delivery:

Your employees chose to serve the public. But their technology tools are undermining their ability to do so. Every friction point, every delay, every IT roadblock chips away at productivity, morale and ultimately their ability to serve their communities.





Ivanti Autonomous Endpoint Management Solution Overview

Ivanti Autonomous Endpoint Management helps agencies and educational institutions establish trusted data authority, automate within defined guardrails and move from reactive operations to proactive, resilient IT:

- **Trusted Visibility and Data Authority:** Establishes a continuously updated, trusted system of record across managed, unmanaged and shadow IT assets so every decision and workflow is built on accurate context.
- **Governed AI and IT Efficiency:** Assesses, assists and automates through governed AI workflows, reducing ticket volume while maintaining human-in-the-loop oversight and accountability.
- **Autonomous Remediation:** Moves from reactive support to proactive, self-healing resolution that prevents common endpoint issues before they escalate.
- **Autonomous Patching and Continuous Compliance:** Prioritizes and automates patching based on real-world risk, active exposure and agency risk tolerance, aligned with zero-trust principles and state and local cybersecurity mandates such as CJIS and GovRAMP.
- **Productive, Frictionless Digital Experiences:** Detects and resolves experience issues automatically, keeping employees productive and reducing downtime.
- **Security by Design:** Bridges IT and security operations through continuous discovery, policy enforcement and exposure reduction, supporting CJIS and state compliance mandates.

Ivanti Autonomous Endpoint Management in Action

Establish Trusted Visibility

Continuous discovery of managed, unmanaged and shadow IT assets gives SLED organizations a trusted foundation for automated workflows and audit-ready compliance.

- Asset discovery: Identify unmanaged and unknown devices connecting to the network.
- Device inventory: View ownership, OS version and encryption status in one place.

Manage and Deploy at Scale

Manage every OS and device type — Windows, macOS, iOS, Android, Linux, ChromeOS, VR/XR — across enrollment, policy, app delivery and retirement from one platform.

- Multi-OS management: Apply a policy across Windows and macOS devices at once.
- Zero-touch provisioning: New devices arrive with apps, settings and access preconfigured.

Protect, Patch and Support

Risk-aware, autonomous patch management continuously reduces exposure, while conditional access and governance policies enforce compliance.

- Risk-based patch management: Prioritize and deploy critical patches ahead of vulnerability windows, supporting CJIS Security Policy and GovRAMP requirements.
- Continuous compliance monitoring: Detect and remediate configuration drift in real time.

Automate and Optimize Operations

One-to-many bot actions and autonomous remediation resolve issues and enforce changes across device groups at scale.

- Fleet remediation: Remove risky applications or update configurations across thousands of endpoints in one action.
- Experience analytics: Spot recurring performance issues and remediate before they generate tickets.



Key Capabilities

Comprehensive Visibility: Real-time asset discovery and endpoint visibility across all devices and environments, unified into a trusted system of record. Eliminates blind spots and ensures accurate inventory for compliance and audit readiness.

Governed AI-Driven Automation: Self-healing endpoints that remediate issues automatically, with 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 aligned with agency risk tolerance and zero-trust principles.

Broad OS and Device Support:

Unified management for Windows, macOS, Linux, ChromeOS, iOS and Android, including rugged and VR/XR devices.

Zero-Touch Provisioning and

Self-Service: Automated device onboarding and configuration. Self-service capabilities for employees to reduce IT workload and improve experience.

Connected ecosystem: One platform combining unified endpoint management (UEM), digital experience monitoring, and security capabilities.

Integrated IT Service Management (ITSM) and Security: Native integration with ITSM and security workflows. End-to-end without silos, aligning IT and Security operations.

What Makes Ivanti Autonomous Endpoint Management Different

See everything, miss nothing

Your IT environment is constantly evolving with new devices, new apps and remote employees. Ivanti Autonomous Endpoint Management delivers real-time visibility across every endpoint, every OS and every location. No more blind spots that leave you vulnerable to shadow IT or out of compliance. You get a complete, accurate picture of your entire estate so that you can make informed decisions with confidence, demonstrating that posture to oversight bodies.

Automation you can trust, oversight you keep

Built on trusted endpoint data, Ivanti helps agency teams assess, assist and automate through governed AI workflows. Reduce ticket volume and scale operations while maintaining human-in-the-loop oversight, accountability, and the decision controls SLED organization, like yours, demands.

IT that fixes itself

Why wait for tickets when problems can solve themselves? Ivanti Autonomous Endpoint Management moves your team from reactive support to proactive, autonomous remediation. This detects and resolves issues before employees even notice, patching vulnerabilities across operating systems and applications autonomously. Your team shifts from firefighting to higher-value work, while your security posture continues to strengthen.

Stop threats before they start

SLED security teams can't afford to be reactive anymore. Ivanti Autonomous Endpoint Management prioritizes and automates patching based on real-world risk, active exposure and your agency's risk tolerance – then verifies the results. With continuous compliance monitoring, intelligent vulnerability remediation, and risk-based patching that directly support your CJIS and GovRAMP obligations. So you're always one step ahead of adversaries, not one step behind.

One platform, every device

Your workforce needs it all — Windows laptops, MacBooks, Linux servers, mobile devices, rugged handhelds and even VR headsets. Ivanti Autonomous Endpoint Management manages it all from a single pane of glass. Finally, unified control without the complexity of juggling multiple tools or platforms.

Empower employees, free up IT

Nobody wants to wait for IT to set up their device or fix basic issues. Ivanti detects experience issues early and automatically remediates them, significantly reducing downtime. 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 recovers hours each week to focus on strategic initiatives rather than routine requests.

IT and security, aligned at last

The days of IT and security working at cross-purposes are over. Secure by Design means it's built into operations from the outset. Ivanti Autonomous Endpoint Management integrates seamlessly with your existing security and service management tools, creating end-to-end workflows where visibility, action and governance flow naturally, supporting CJIS compliance and zero-trust architecture requirements. Operations become faster, smarter and dramatically more secure.

The Ivanti logo, featuring the word "ivanti" in a lowercase, sans-serif font. The "i" is a light blue color, while the rest of the letters are white. The logo is set against a dark blue background.

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 workforce 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 a workforce 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](https://www.ivanti.com) and follow @Golvanti.

Learn more about Ivanti Autonomous Endpoint Management [here](#) or contact your Ivanti state and local government representative today.