AUTONOMOUS ENDPOINT MANAGEMENT

Trusted Data. Autonomous Remediation. Proactive Protection.

The Future of Federal Endpoint Management Starts Here.

Federal civilian and Department of War agencies manage endpoint environments of staggering complexity. These endpoints span desktops, mobile devices, rugged field hardware, and IoT and face rising security risks while budgets have not kept pace with expanding mission requirements. Nation-state adversaries and ransomware operators target government infrastructure with increasing precision, and the consequences of an unpatched endpoint are no longer theoretical. At the same time, agencies are being asked to carry out the same or an expanded mission with reduced IT staff and budget, a growing infrastructure footprint and an expanding list of compliance mandates to satisfy.

Ivanti Autonomous Endpoint Management gives federal IT and security teams a unified foundation for trusted data authority, unified management, reduced risk and frictionless workforce experiences. With AI-powered automation, self-healing capabilities and continuous compliance enforcement, autonomous endpoint management helps agencies maintain a defensible security posture and reclaim the IT capacity they need to deliver on their mission — across every agency, bureau and field office.

Agency Challenges

Security risks from unpatched endpoints

The window between vulnerability disclosure and active exploitation has collapsed. Recent research has found that only 16% of patches are completed within the 48-hour industry best-practice window, and CISA's Binding Operational Directive (BOD) 26-04 now sets remediation timelines as short as three calendar days for the highest-risk vulnerabilities in its Known Exploited Vulnerabilities (KEV) catalog. Meanwhile, enterprise mean time to remediate (MTTR) critical vulnerabilities exceeds five months for complex applications. For federal agencies, that gap is a mission and national security risk.

Limited IT resources and constrained budgets

Federal IT teams are being asked to manage more devices, satisfy more compliance requirements and respond to more threats, all while staffing levels have not grown proportionally. Budgets are shrinking while device counts rise and infrastructure complexity multiplies. Manual patching, siloed tools and reactive workflows consume the capacity that agencies need for strategic security work.

Poor visibility and fragmented tools

Legacy and siloed agency systems leave IT leaders without a reliable, real-time picture of their endpoint environment. Incomplete asset inventories, contradictory data from disconnected tools and gaps in coverage across remote and field-deployed devices make it difficult to answer the questions that auditors, inspectors general and oversight bodies demand: What is on the network, what is its current state and what risk does it carry?

Mission and service delivery impact

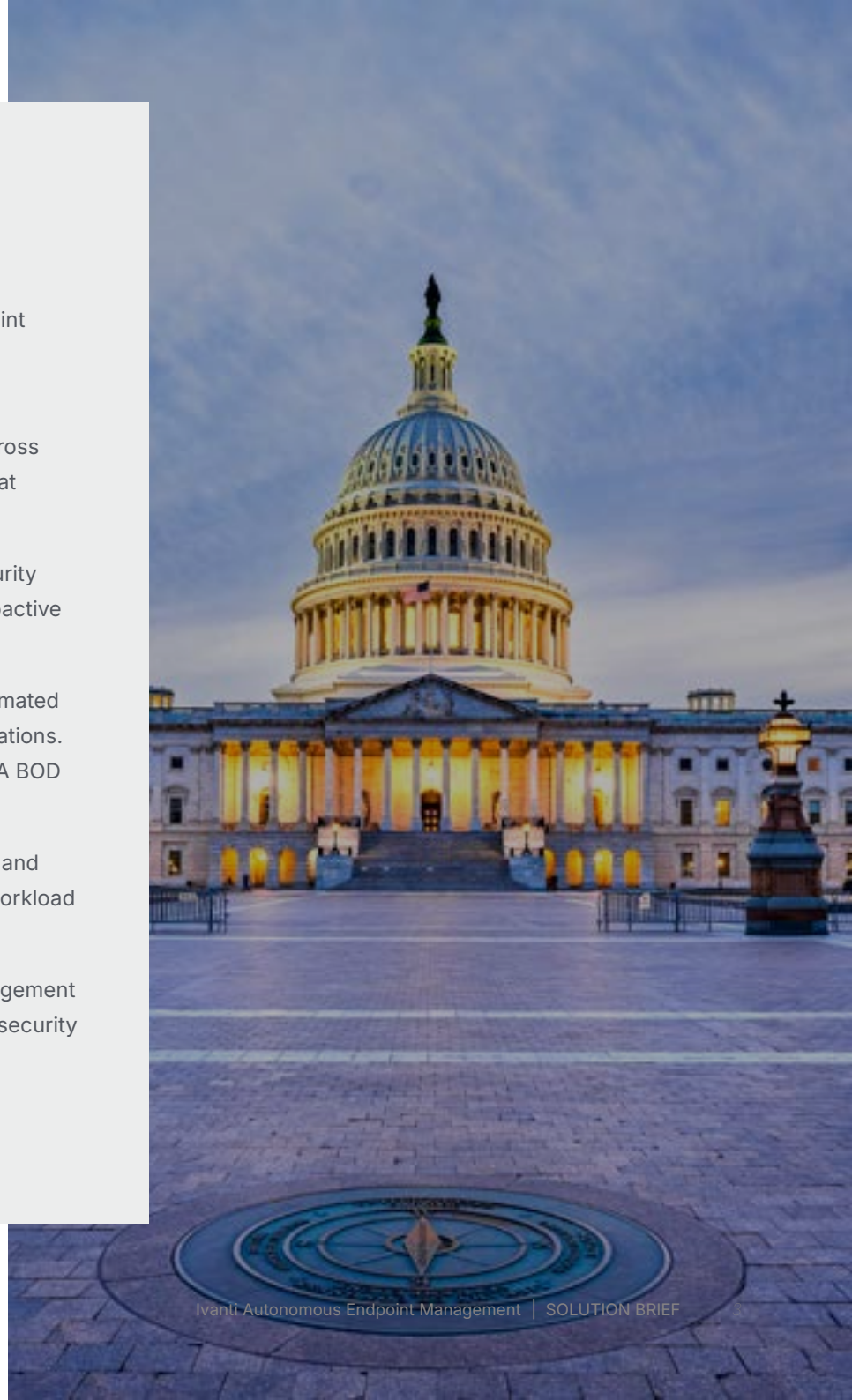
Every IT friction point has a downstream cost. When devices take too long to provision, patches disrupt operations, or support tickets go unresolved, agency personnel lose time they cannot recover. The workforce expects technology that works. When it does not, mission delivery suffers, for the agency and the mission.



Ivanti Autonomous Endpoint Management: Solution Overview

Ivanti Autonomous Endpoint Management delivers a next-generation approach to federal endpoint management, purpose-built to address the compliance, security and operational demands of unclassified and classified environments:

- Trusted visibility and data authority: Real-time asset discovery and continuous inventory across every device, OS and location — giving agencies the accurate, auditable data foundation that compliance and oversight require.
- Autonomous remediation: AI-driven automation detects and resolves performance and security issues without waiting for a help desk ticket, shifting IT teams from reactive response to proactive operations.
- Autonomous patching and continuous compliance: Risk-based patch prioritization and automated deployment across Windows, macOS, Linux, iOS, Android and 1,000-plus third-party applications. Continuous configuration monitoring supports alignment with NIST 800-171, NIST RMF, CISA BOD requirements and Zero Trust mandates under OMB M-22-09.
- Productive, frictionless digital experiences: Zero-touch provisioning, intelligent self-service and proactive issue resolution keep agency personnel productive from day one and reduce IT workload across the board.
- Secure by Design: Security is built into every layer of the Ivanti Autonomous Endpoint Management solution, not added after the fact. Role-based access, audit-ready reporting and integrated security workflows support accountability and governance at every level.



Autonomous Endpoint Management in Action

Establish trusted visibility

You cannot protect what you cannot see. Ivanti Autonomous Endpoint Management delivers real-time asset discovery and endpoint visibility across every device and environment in your agency, on-premise, cloud-managed, remote and field-deployed. Blind spots that leave you vulnerable or out of compliance are eliminated. The result is a complete, accurate and continuously updated inventory that supports audit readiness for inspector general reviews, Government Accountability Office (GAO) inquiries and FISMA reporting.

Manage and deploy at scale

Ivanti Autonomous Endpoint Management supports every device your workforce relies on — Windows laptops, Macs, Linux servers, iOS and Android mobile devices, rugged handhelds and VR/XR hardware — from a single management platform. Zero-touch provisioning brings new devices and new personnel online without IT intervention. Integration with Android zero-touch enrollment and Apple Business Manager enables fast, consistent device setup at scale, whether onboarding happens at headquarters or in the field.

Protect, patch and support

Enterprise MTTR critical vulnerabilities currently average more than five months. Against a threat landscape in which exploits are weaponized within days, that exposure is indefensible. Ivanti Autonomous Endpoint Management's risk-based patch management automatically prioritizes and applies patches based on vulnerability severity and real-world exploit likelihood, across operating systems and 1,000-plus third-party applications without manual intervention. Ring-based phased rollout and scheduling that accounts for digital employee experience ensure patches deploy safely and predictably, without disrupting operations. Continuous compliance monitoring and automated remediation support agency obligations under NIST RMF, CISA BOD 26-04, and the Zero Trust requirements of OMB M-22-09.

Automate and optimize operations

Manual processes consume IT capacity that federal agencies cannot afford to waste. Ivanti Autonomous Endpoint Management's self-healing capabilities detect and resolve performance and configuration issues autonomously, before personnel open a support ticket. Intelligent automation handles routine tasks including software lifecycle management, configuration drift remediation and device health monitoring, freeing IT teams to focus on mission-critical priorities rather than day-to-day triage.

Key Capabilities

- Comprehensive visibility: Real-time asset discovery and endpoint visibility across all devices and environments. Eliminates blind spots and ensures accurate, auditable inventory for compliance reporting and optimization.
- AI-driven automation: Self-healing endpoints remediate issues autonomously, with humans in the loop. Automated patching across operating systems and applications reduces risk proactively without adding IT workload.
- Predictive remediation: AI-powered threat prevention delivered before issues arise. Continuous compliance monitoring, vulnerability remediation and risk-based patching aligned with Zero Trust and NIST RMF requirements.
- Broad OS and device support: Unified management for Windows, macOS, Linux, iOS and Android including rugged devices and VR/XR hardware, from a single platform.
- Zero-touch provisioning and self-service: Automated device onboarding and configuration via Android zero-touch enrollment and Apple Business Manager for instant device setup. Self-service capabilities reduce IT workload and accelerate time-to-productivity for agency personnel.
- Connected ecosystem: A unified platform combining unified endpoint management (UEM), digital experience monitoring, and security capabilities. Native integration with IT service management (ITSM) workflows aligns IT and security operations without creating new silos.
- Integrated IT asset management and security: Centralized asset and service management with built-in security controls, role-based access, and activity tracking to support accountability, oversight, and audit readiness.

What Makes Ivanti Autonomous Endpoint Management Different

See everything, miss nothing

Federal IT environments never stop changing. New devices come online, personnel rotate and field deployments extend the asset inventory in ways that legacy tools cannot track. Ivanti Autonomous Endpoint Management delivers real-time visibility across every endpoint, every OS and every location. No blind spots. No stale data. You get a complete, current picture of your entire environment that holds up to inspector general and GAO scrutiny and gives your team the confidence to make informed decisions.

Automation you can trust, oversight you keep

Federal agencies require automation that operates within defined boundaries, with humans maintaining control over critical decisions. Ivanti Autonomous Endpoint Management's AI-driven workflows automate repetitive, high-volume tasks such as patching, remediation and onboarding, while keeping your team in the loop for actions that require human judgment. Automation accelerates the work; your personnel retain the authority.

IT that fixes itself

Why generate a help desk ticket for a problem that can resolve itself? Ivanti Autonomous Endpoint Management detects and remediates performance and security issues before personnel notice them, patching vulnerabilities across operating systems and applications without waiting for manual intervention. Your team transitions from firefighting to mission support, while your security posture continues to improve.

Stop threats before they start

Federal security teams cannot operate reactively in an environment where critical vulnerabilities are actively exploited within days of disclosure. Ivanti Autonomous Endpoint Management uses AI to prioritize and address threats before they materialize, with continuous compliance monitoring and risk-based patching working in concert. This directly supports federal agency obligations under NIST RMF, CISA BOD 26-04 and the Zero Trust requirements of OMB M-22-09 — keeping you ahead of adversaries rather than responding to them.

One platform, every device

Your workforce operates on everything — laptops, tablets, mobile devices, rugged handhelds and specialized hardware. Managing all of it from a single platform eliminates the cost and complexity of juggling multiple tools, reduces the risk of coverage gaps and gives agency leadership a consolidated view of the entire endpoint estate. Tool consolidation is also a direct path to cost reduction in constrained budget environments.

Empower employees, free up IT

With zero-touch provisioning and intelligent self-service, new personnel are productive from day one without placing additional demand on IT. Experienced users resolve common issues on their own. Your IT team reclaims hours every week, time that goes toward strategic security initiatives and mission support rather than routine requests. Federal agencies get more from their existing workforce without the risk of burnout.

IT and security, aligned at last

When endpoint management, security operations, and ITSM operate as separate functions with separate tools, risk accumulates in the gaps between them. Ivanti Autonomous Endpoint Management integrates natively with ITSM workflows, creating end-to-end visibility and governance across IT and security teams. One ecosystem, one source of truth, supporting Zero Trust architecture and providing leadership with the unified operational picture that effective federal cybersecurity governance requires.

About Ivanti

Ivanti is a global enterprise IT and security software company that provides the trusted data authority for AI-driven, autonomous endpoint management. Ivanti connects IT and security operations data in a unified system of record — giving teams clear visibility of every device in their environment, and the ability to intelligently manage risk. With automated remediation and self-healing capabilities, IT and security teams can agree on governance, proactively and autonomously resolve issues and operate at scale. At the heart of Ivanti's offerings is the AI-powered Ivanti Neurons platform, where authoritative data drives decisions across endpoints, services and exposure — so AI acts on what is known, within pre-defined guardrails. Ivanti fosters an inclusive environment where diverse perspectives are honored and valued, reflecting a commitment to a sustainable future for customers, partners, employees and the planet. Learn more at www.ivanti.com and follow us on social media @GoIvanti.

Copyright © 2025, Ivanti. All rights reserved. IVI-2965 NB/DM

ivanti

Learn more about Ivanti Autonomous Endpoint Management here or contact your Ivanti federal government representative today.