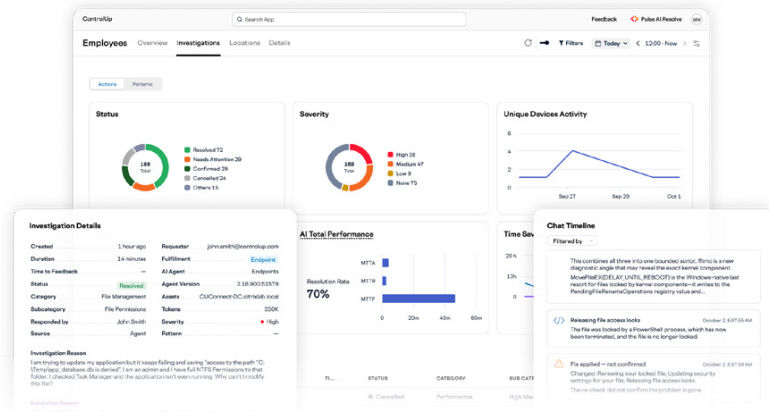


SOLUTION BRIEF

Pulse AI Resolve

AI-Native Self-Service and Remediation for the Employee Endpoint

ControlUp Pulse Resolve goes beyond the native self-service and ticketing capabilities of a help desk portal by giving IT a purpose-built agent that detects, diagnoses, and fixes issues directly on the employee's device.



Instead of employees waiting for a slowdown to get bad enough to report, or IT connecting five tickets to one root cause after the fact, Pulse Resolve consolidates detection, diagnosis, and remediation into one continuous process running on the endpoint itself.

With ControlUp Pulse Resolve, teams don't just respond to tickets, they eliminate the ones that never needed to exist. Continuous, policy-governed detection catches anomalies before employees notice them, a self-service chat resolves issues in plain language without a ticket, and layered guardrails, RBAC, and change control keep every autonomous action inside the approval rules IT defines. When a fix does need a human, ServiceNow handoff arrives pre-populated with full technical context.

ControlUp Pulse Resolve transforms IT support from a reactive, ticket-driven operation into a proactive, self-healing one.

BENEFITS OF PULSE RESOLVE

Pulse Resolve reduces ticket volume from day one by resolving issues on the device before an employee has to notice, call, or wait.

Eliminate alert fatigue with continuous detection that flags only sustained breaches, not momentary blips, so IT sees what matters without the noise.

Act with confidence through a layered guardrail architecture, built-in platform checks, an execution gate, and organization defined policy, that governs every proposed action before it touches a device.

Delegate safely with six additively combinable RBAC roles that let teams investigate, approve, or govern remediation without granting blanket agent authority.

Continuous, Governed Detection	Pulse Resolve monitors CPU, memory, event logs, and other endpoint signals on a continuous cycle, alerting only on sustained breaches so alert fatigue stops being the tradeoff for catching issues early.	Startup shield suppresses alerts during boot and security-agent initialization
		Hourly and daily caps prevent alert overload during sustained strain
		Admin-configurable thresholds, with ControlUp defaults recommended
Self-Service Chat & Guided Remediation	Employees describe an issue in plain language and Pulse Resolve investigates, diagnoses, and, within policy, resolves it in real time, keeping the employee informed and asking for consent throughout.	Four-level resolution model from pre-approved scripts to agentic reasoning
		Consent and transparency built into every diagnostic and fix
		Continuous learning sharpens pattern recognition over time
Layered Guardrails & Governed Autonomy	Every proposed action passes through built-in platform guardrails, an NVIDIA NeMo Guardrails execution gate, and organization-defined policy before it ever touches a device, so autonomy and governance travel together.	Curated policy library or fully custom rules for regulated environments
		Same guardrail chain applies to chat, plan, and execution steps
		Vetted-patterns-only mode available for stricter environments
RBAC & Change Control	Remediation workflows execute under six additively combinable roles, so what Resolve is allowed to do, and to whom, is controlled by role rather than left to agent judgment alone.	Separate approval gates for diagnostics versus mitigations
		Separate approval gates for user-context versus system-context actions
		Auto-expiring approvals and required decline notes prevent limbo
Verified Outcomes & ITSM Handoff	Pulse Resolve confirms a fix worked against real device evidence rather than a clean exit code and rolls back automatically if a multi-step remediation fails partway through.	Automatic ServiceNow ticket creation prepopulated with technical context
		Device re-examined after every fix before marking an issue resolved
		Undo restrictions and confirmation required for irreversible actions

ControlUp combines leading digital employee experience capabilities with agentic AI to detect, diagnose, and resolve IT issues before they affect employees. This enables Autonomous Endpoint Management (AEM), helping IT lead, employees thrive, and work flows smoothly.

[Get a Demo](#)
[Start a Free Trial](#)