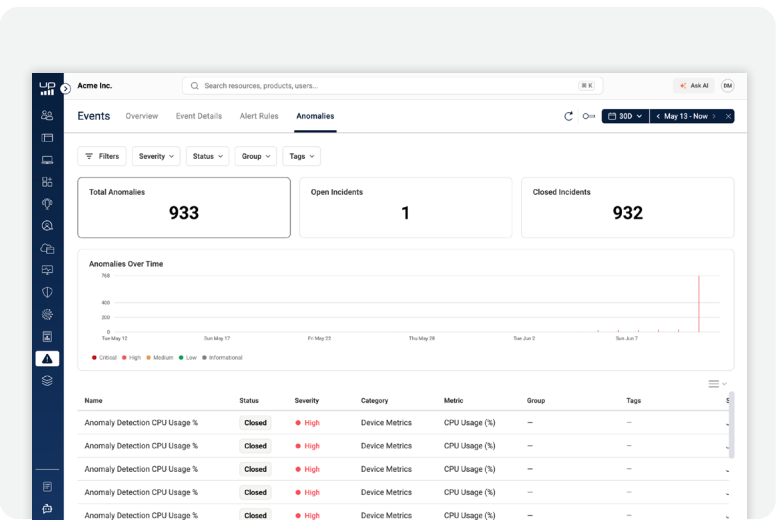
SOLUTION BRIEF

# Pulse AI Detect

Redefine IT Alerting with Behavior-Based Intelligence That Learns Your Environment

ControlUp Pulse AI Detect go beyond the limitations of static threshold alerting by giving IT teams a smarter, self-adjusting signal that reflects how their environment actually behaves.




Instead of relying on fixed rules that generate noise during expected activity or miss gradual degradation entirely, Pulse AI Detect uses machine learning to establish a normal operating range for each device or group and alerts only when behavior truly deviates from it.

With ControlUp Pulse AI Detect, teams don't just receive more alerts, they receive the right ones. Historical baselines automatically account for daily and weekly usage patterns, patching windows, and business growth, so IT can stop spending time tuning thresholds and start focusing on issues that actually matter. Directional triggering and configurable sensitivity give administrators full control over what gets flagged, without requiring statistical expertise.

ControlUp Pulse AI Detect transform IT monitoring from a noisy, threshold-driven chore into a precise, intelligent, and low-maintenance capability.

## BENEFITS OF PULSE AI DETECT

Pulse Detect reduce alert fatigue by learning what normal looks like for your environment and only firing when behavior is truly out of character.

Catch issues static thresholds miss by detecting subtle, gradual degradations that never cross a fixed number but still signal a real problem.

Eliminate constant threshold tuning by building dynamic baselines that self-adjust as your environment grows, changes, or shifts usage patterns over time.

Improve MTTR with higher-confidence alerts that give IT teams actionable, meaningful signals instead of noise to sift through before investigation can begin.

| | | |
|---|---|---|
| **Automated Baseline Learning** | ControlUp analyzes historical device data to automatically build an expectation of normal behavior for each device or group at any given time of day or day of week. | Baselines built from CPU, disk I/O, memory, network latency, and more |
| | | Automatically accounts for peak logon periods, patching windows, and business cycles |
| | | No manual baseline configuration required |
| **Dynamic Sensitivity Control** | Rather than setting a fixed percentage threshold, administrators define a sensitivity level to control how far a metric must deviate from the baseline before an alert fires. | Low, Medium, and High sensitivity settings to match operational tolerance |
| | | Eliminates the need to find the perfect threshold number |
| | | Adjusts automatically as the environment naturally evolves |
| **Directional Triggering** | Alerts can be configured to fire when a metric is unexpectedly too high, too low, or either, enabling detection of both performance degradations and unusual off-hours activity. | Detect critical negatives such as unexpected memory exhaustion |
| | | Identify subtle positives such as unusual application usage during off-hours |
| | | Covers security and performance use cases in a single alert type |
| **Flexible Scope Configuration** | Pulse Detect can be scoped to the full organization, a specific group of devices, or an individual machine, giving IT the right level of granularity for each scenario. | Org-wide alerts for fleet-level trend detection |
| | | Group or tag-based scoping for targeted environment segments |
| | | Per-device alerts for high-priority or sensitive endpoints |
| **Scheduled Pause Support** | IT teams can pause Pulse Detect during planned maintenance windows, deployments, or known instability events to prevent false positives without disabling the alert entirely. | Schedule pauses in advance for planned maintenance windows |
| | | Prevent alert noise during known operational changes |
| | | Resume automatically when the maintenance window closes |

ControlUp is the AI company for IT operations that keeps the digital workplace running. Leading DEX capabilities and agentic AI come together to see, detect, ask, and remediate issues before they reach employees, enabling Autonomous Endpoint Management (AEM). IT leads, employees thrive, and work flows.

Get a Demo  Start a Free Trial

controlup.com