ACTONIX

ENDPOINT INTELLIGENCE

Elevate Digital Experience with Autonomous Intelligence: Detect, Diagnose, and Self-Heal

Highlights

35% Digital Experience & Performance Analytics

Autonomous Remediation (Self-Healing)

Adaptive Security & Hardening

Full-Spectrum Inventory & Lifecycle

ACTONIX

Actonix Endpoint Intelligence (AEI) is an advanced Digital Employee Experience (DEX) and automated governance module. By combining deep-system telemetry with autonomous remediation, AEI transforms the workstation from a managed asset into an intelligent, self-healing node. It ensures that every device is secure, compliant, and optimized for peak human performance.

Key Intelligence Modules

1. Digital Experience & Performance Analytics

AEI continuously monitors the "vitals" of the workstation to ensure the user's digital journey is never compromised.

- Smart-Login Diagnostics: Analyzes boot sequences and LoginProfiles.ps1 loads to eliminate startup lag and identify inefficient GPOs or scripts.
- Predictive Health Scoring: Generates real-time stability scores based on disk health, memory pressure (Process-Memory Stats.ps1), and driver reliability.
- Application Sentiment Audit: Monitors resource-heavy or crashing applications to identify software friction before it leads to a support ticket.
- OS Readiness: Real-time assessment of fleet compatibility for Windows 11 transitions (Win11Readiness.ps1).

ACTONIX

Autonomous Remediation (Self-Healing)

Turn your IT expertise into a 24/7 automated force. AEI detects failures and fixes them silently in the background.

- OS Resiliency Engine: Automatically triggers SFC and DISM repairs when system file corruption or image decay is detected.
- Automated System Hygiene: Silently optimizes performance by clearing system bloat, flushing DNS caches, and managing disk quotas.
- Service Watchdog: Instantly identifies and restarts critical failed services (Print Spooler, Update Services, etc.) to maintain business continuity.
- Disaster Recovery: Automated creation of System Restore points prior to major software upgrades

Adaptive Security & Hardening

AEI enforces a Zero-Trust posture at the edge, adapting to the threat landscape in real-time.

- System Immunization: Enforces industry-standard hardening templates (ApplyHardenTemplate.ps1) and locks down folder/registry permissions automatically.
- Vulnerability Rapid-Response: Deploys specific "Intelligence Packs" to audit and remediate zero-day threats (e.g., WebP or MOVEit vulnerabilities) within minutes.

ACTONIX

- Identity & Access Guard: Automated cleanup of unauthorized local accounts, continuous auditing of BitLocker status, and Antivirus health monitoring.
- Network Defense: Real-time auditing of firewall rules and default blocking of public inbound traffic.

Full-Spectrum Inventory & Lifecycle

Eliminate blind spots with a "single source of truth" for your entire hardware and software estate.

- Deep-Level Inventory: Comprehensive reporting on SCSI controllers, network adapters, and disk partitions.
- Software Transparency: Full visibility into installed applications, active processes, and browser extensions.

Unified Patching: Automated monitoring and deployment of updates for Windows, system drivers, and 3rd-party applications.