ACTONIX

DATASHEET

Endpoint Intelligence

Elevate digital experience with autonomous intelligence: detect, diagnose and self-heal every Windows workstation.

HIGHLIGHTS

Digital experience analytics

Boot, login, stability and application health — measured continuously

Autonomous remediation

System repair, hygiene and service recovery without a ticket

Adaptive security & hardening

Zero-Trust posture enforced at the edge

Full-spectrum inventory

One source of truth for hardware and software

OVERVIEW

From managed asset to self-healing node

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 each workstation from a managed asset into an intelligent, self-healing node — secure, compliant and optimised for peak performance.

MODULE 1

Digital experience & performance analytics

AEI continuously monitors the vitals of every workstation so the user's digital journey is never compromised.

- **Smart-login diagnostics** — analyses boot sequences and profile loads to eliminate start-up lag and pinpoint inefficient GPOs or logon scripts.
- **Predictive health scoring** — real-time stability scores based on disk health, memory pressure and driver reliability.
- **Application sentiment audit** — flags resource-heavy or crashing applications before they turn into support tickets.
- **OS readiness** — real-time assessment of fleet compatibility for Windows 11 transitions.

MODULE 2

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 runs SFC and DISM repairs when system-file corruption or image decay is detected.
- **Automated system hygiene** — clears system bloat, flushes DNS caches and manages disk space to keep performance high.
- **Service watchdog** — identifies and restarts failed critical services, such as Print Spooler and update services, to maintain continuity.
- **Disaster recovery** — creates System Restore points before major software upgrades.

MODULE 3

Adaptive security & hardening

© 2026 Actonix Software Pvt Ltd · www.actonix.in

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

- **System immunisation** — applies industry-standard hardening templates and locks down folder and registry permissions automatically.
- **Vulnerability rapid-response** — deploys targeted intelligence packs to audit and remediate zero-day threats, such as the WebP and MOVEit vulnerabilities, within minutes.
- **Identity & access guard** — removes unauthorised local accounts and continuously audits BitLocker status and antivirus health.
- **Network defence** — real-time auditing of firewall rules, with public inbound traffic blocked by default.

MODULE 4

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 storage controllers, network adapters and disk partitions.
- **Software transparency** — full visibility of installed applications, active processes and browser extensions.
- **Unified patching** — automated monitoring and deployment of updates for Windows, system drivers and third-party applications.

See Actonix on your own endpoints

Book a live demo, or talk to our team at sales@actonix.in.

actonix.in/demo

© 2026 Actonix Software Pvt Ltd · www.actonix.in