ACTONIX

DATASHEET

Windows & Third-Party Patch Management

Autonomous, CVE-driven patching for Windows and third-party applications — delivered by one signed agent, with no inbound ports and no domain join.

HIGHLIGHTS

Risk-driven prioritisation

NVD, FIRST EPSS and the CISA KEV catalog decide what gets patched first

User-aware deployment

Consent, snooze and deferral within the policy you set

Pre-install integrity checks

Every installer's signature and publisher verified before it runs

Audit-ready logging

Native Windows Update history plus structured NDJSON for your SIEM

OVERVIEW

Close the patch gap — automatically

Actonix eliminates the risk of unmanaged third-party apps and inconsistent Windows patching. Delivered as a single, signed agent, it unifies deep software discovery, CVE-driven threat intelligence and user-aware deployment — with no open inbound ports or domain join required.

CORE ARCHITECTURE & KEY CAPABILITIES

How Actonix patches your fleet

User-centric controls

An interactive desktop notifier shows update details, CVE scores and countdowns. Users can approve, snooze or defer within the policies you set. Critical updates, such as major runtime upgrades, require explicit consent before they proceed.

Resource & session intelligence

Continuously monitors CPU, memory, disk load and active user sessions. Installs defer to idle windows when thresholds are exceeded, while SLA safeguards ensure critical security patches are never delayed indefinitely.

Layered discovery & multi-tier pipeline

Audits the registry, MSI database, file paths and running processes to find even obscure or script-installed software. Vendor APIs, release feeds, community repositories and web sources are queried through a confidence-scored resolver to find the precise update.

Pre-install binary integrity

Installers are downloaded to a temporary location and their Authenticode signature and vendor identity verified. Mismatched, unsigned or revoked certificates trigger an immediate hard stop and a security log entry.

CVE & risk-driven prioritisation

Applications are mapped to CPEs and enriched daily with CVSS scores, EPSS exploit probability and the CISA KEV catalog. A composite risk score ensures actively exploited threats are patched first.

Audit-ready logging

OS updates log natively into Windows Update history. Third-party patch telemetry is written as structured NDJSON for direct ingestion into SIEM, Trino or data-warehouse pipelines.

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

TECHNICAL SPECIFICATIONS

At a glance

Feature	Details
Supported OS	All supported Windows versions — workstations and servers
Deployment model	SaaS-managed; lightweight signed agent; outbound-only communication
Integrations	Native Windows Update Agent (COM / WinRT), NDJSON telemetry, NVD, FIRST EPSS, CISA KEV
Prerequisites	No domain join required; runs on existing Windows Task Scheduler infrastructure

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