ACTONIX

WINDOWS & THIRD-PARTY PATCH MANAGEMENT

Highlights

35% NVD , FIRST EPSS, CISA KEV Catalog

Autonomous Remediation (Self-Healing)

Adaptive Security & Hardening

Full-Spectrum Inventory & Lifecycle

ACTONIX

Actonix eliminates the risks of unmanaged third-party apps and inconsistent Windows patching. Delivered as a single, signed agent, Actonix 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

- **User-Centric Controls:** An interactive desktop notifier displays update details, CVE scores, and countdowns. Users can approve, snooze, or defer within set policies. Critical updates (e.g., major runtime jumps) require explicit user consent before proceeding.

- **Resource & Session Intelligence:** Continuously monitors CPU, memory, disk load, and active user sessions. Installs automatically defer to idle windows if thresholds are exceeded, while SLA safeguards ensure critical security patches aren't indefinitely delayed.

- **Layered Discovery & Multi-Tier Pipeline:** Audits the registry, MSI database, file paths, and running processes to discover obscure or script-installed software. Queries vendor APIs, release feeds, community repos, and web sources using a confidence-scored resolver to find precise updates.

- **Pre-Install Binary Integrity:** Downloads installers to temporary paths to verify Authenticode signatures and vendor identity match. Mismatched, unsigned, or revoked certificates trigger an immediate hard stop and security log.

- **CVE & Risk-Driven Prioritization:** Maps applications to CPEs and enriches them daily with CVSS scores, EPSS exploitation probability, and the CISA KEV catalog. Computes composite risk scores so 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 logs for direct ingestion into SIEM, Trino, or data warehouse pipelines.

Technical Specifications

Feature	Details
Supported OS	All Supported Windows OS
Deployment Model	SaaS-managed; lightweight signed agent; outbound-only
Integrations	Native WUA COM/WinRT, NDJSON, NVD, EPSS, CISA KEV
Prerequisites	No domain join required; runs on existing job infrastructure