

Actonix v/s Manage Engine Patch Manager Plus

Capability	Function Description	Actonix	ManageEngine Patch Manager Plus
Architecture	Defines how the patch-management platform is deployed and operated.	Cloud-first SaaS + lightweight endpoint agent	Cloud or on-premises deployment
Infrastructure Required	Infrastructure needed to operate the patch-management platform.	No customer patch server required for SaaS deployment	On-premises deployment requires server/infrastructure
VPN Dependency	Determines whether endpoints need corporate network/VPN connectivity for management.	Designed for Internet-connected remote endpoints	Depends on deployment architecture/network configuration
Windows Patching	Detects, approves, schedules and deploys Windows OS updates.	✓	✓
Windows Server Patching	Manages security and quality updates for Windows Server systems.	✓	✓
macOS Patching	Detects and deploys supported macOS updates.	Roadmap	✓
Linux Patching	Detects and deploys supported Linux updates.	Roadmap	✓
Third-Party Application Patching	Identifies outdated third-party applications and deploys available updates.	✓	✓
Application Inventory	Maintains installed application name, version and endpoint inventory.	✓	✓
Real-Time Endpoint Inventory	Provides current endpoint/application information from managed agents.	✓	✓
CVE Visibility	Identifies vulnerabilities associated with installed software.	Native CVE/application mapping architecture	⚠

Capability	Function Description	Actonix	ManageEngine Patch Manager Plus
CVE → Application → Endpoint Mapping	Correlates a CVE with the affected application version and endpoints.	Core design	⚠
Patch → CVE Remediation	Connects an identified vulnerability directly to the required remediation/patch.	Designed as integrated workflow	Strong, but vulnerability capabilities can involve VMP
NVD/CVE Intelligence	Uses vulnerability intelligence to identify known software vulnerabilities.	✓	✓
Application → CPE Mapping	Maps installed applications to standardized CPE identifiers for vulnerability correlation.	Actonix mapping engine	Mature vulnerability/application database
Custom Application Repository	Stores and manages software packages outside the standard vendor catalog.	Actonix repository architecture	⚠
Private Software Repository	Provides a controlled repository for software installers/packages.	Actonix-controlled repository	⚠
Current + Previous Application Versions	Maintains multiple application versions for controlled deployment or rollback scenarios.	Designed for repository/version management	⚠
Automated Patch Download	Automatically obtains required patch installers/packages.	✓	✓
Patch Scheduling	Allows patches to be deployed according to defined schedules.	✓	✓
Maintenance Windows	Restricts patch deployment to approved maintenance periods.	✓	✓
Patch Rollback	Reverses a deployed patch where supported by the patch/application.	Support/validate per patch type	✓
Reboot Management	Controls endpoint reboot requirements after updates.	Dedicated reboot/update	Supported deployment/reboot

Capability	Function Description	Actonix	ManageEngine Patch Manager Plus
		notification workflow	controls
User Reboot Notifications	Notifies users that a reboot is required and provides appropriate prompts.	Dedicated Actonix notifier	Available deployment/reboot options
Reboot Deadline Enforcement	Enforces a reboot deadline when security updates require system restart.	Yes, via Actonix reboot coordination	Supported deployment controls
Software Deployment	Installs applications on endpoints even when the application is not being updated.	✓	⚠
Software Repository	Provides a controlled source from which application installers can be deployed.	✓	⚠
Admin-Approved Software Catalog	Administrators define which applications are available for endpoint installation.	✓	⚠
User Self-Service Portal	Gives users a controlled interface to initiate approved software/patch installations.	✓	✓
Self-Service Software Installation	Allows users to install administrator-approved applications on demand without manual IT deployment.	✓	⚠
Self-Service Patch Installation	Allows users to initiate approved patch installation from the self-service interface.	✓	⚠
Software Installation Control	Administrators control which applications users are permitted to install.	✓	⚠
Software Uninstall from Portal	Allows approved software to be removed from an endpoint through the portal/workflow.	✓	⚠
Unauthorized Software	Detects/removes applications that are outside	✓	⚠

Capability	Function Description	Actonix	ManageEngine Patch Manager Plus
Removal	the organization's approved software list.		
Install Software on Demand	Allows approved applications to be installed whenever an endpoint/user requires them.	✓	⚠
Deployment Complexity	Measures the effort required to deploy and operate the platform.	Low	Can be higher, particularly on-premises
Time to First Patch	Measures how quickly an organization can begin deploying patches after implementation.	Minutes — target positioning	Installation/configuration dependent
On-Premises Deployment	Allows the complete patch-management platform to be hosted within the customer's infrastructure.	SaaS only	✓ Strong