

POINTRYX



Endpoint Manager

Centralized endpoint management
Clearer visibility across IT operations

Business and technical overview
October 2026

Why POINTRYX?

Target value: turn disconnected endpoint tasks into a coordinated operational workflow.

Unified visibility

Bring device information, installed software and connectivity status into one management workspace.

Organized operations

Coordinate updates, tasks and execution schedules while reducing repetitive manual intervention.

Faster support

Connect device context with support tools to simplify troubleshooting and decision-making.

These are intended benefits, not measured performance results or contractual guarantees.

Scope and feature status

A clear distinction between the project description and release-specific capabilities requiring confirmation.

Project capabilities

Inventory, device management, patching, support tools, MFA, backup and licensing, based on the project discussions.

Priority development

Security Posture and Scheduled Reports are previously requested enhancements; availability in a customer release is not assumed.

Future integrations

INFRYX ITSM integration, an AI assistant and multichannel alerts are presented as proposed directions.

No release files or interface captures were reviewed for this presentation. Images are illustrative, not screenshots.

Centralized, agent-based architecture

A simplified component overview, not an approved implementation network diagram.



Management console

A workspace for monitoring devices, tasks and reports.

POINTRYX server

A central service for managing data and coordinating tasks.

Windows endpoint agent

Collects status and executes authorized tasks.

Inventory and asset visibility

Structured information to support operational and support decisions.

Hardware Inventory

View device information and core specifications to support monitoring, refresh planning and expansion.

Software Inventory

Track installed applications and versions to build a clearer picture of the working environment.

Device Status

Monitor connectivity and the latest agent contact. An offline status does not necessarily indicate device failure.

Available fields and refresh intervals must be confirmed against the deployed release.

Patch management and scheduling

Patch Management & Installation Scheduling

Define the scope

Select target devices and review suitable updates or installation packages before execution.

Schedule execution

Align installation times with maintenance windows and business requirements.

Track outcomes

Review successful, failed and offline devices, then determine the next action.

Supported operating systems and products require release-specific confirmation. Universal application coverage is not assumed.

Deferred restart

Deferred Restart: clearer control over the final step in the update lifecycle.

After installation

Use the deferred restart workflow when the appropriate task policy is selected and installation succeeds.

Business-friendly timing

Separate update installation from restart timing to reduce unplanned interruptions.

Verify before rollout

Test the scenario on pilot devices and review deferred task behavior before broad deployment.

Notification behavior, deferral options and policy limits depend on the implementation; unconfirmed options are not assumed.

Technical support and system tools

Keep support tools close to device context instead of switching between disconnected workflows.

Remote Control

Provide remote assistance within approved permissions, consent requirements and organizational policies.

System Tools

Bring administration and diagnostic tools together to simplify endpoint troubleshooting.

User communication

Chat and announcements are project directions discussed to improve coordination between support teams and users.

Available tools, user-consent requirements and session logging must be reviewed in the actual release.

Security and access protection

MFA is within the project scope; operational safeguards must be approved before production use.



Multifactor authentication

TOTP, recovery codes and administrator reset procedures are included in the project discussions.

Production readiness

Apply least privilege, protect service keys and secrets, secure communications and review administrative access.

Backup and recovery

Protect management-platform data and support operational continuity.

Scheduled backups

Organize periodic platform-data backups according to the retention policy required by the organization.

Backup verification

Review backup integrity and usability rather than relying only on the existence of a backup file.

Controlled recovery

Use .ptxbak files within recovery procedures compatible with the deployed release.

Platform backup does not imply backup of every endpoint file. A practical restore exercise is required.

Security Posture

A previously requested development priority; release availability requires confirmation.

Risk visibility

A proposed consolidated view of endpoint security-status indicators.

Prioritization

Highlight devices requiring review using clearly defined rules and data sources.

Improvement tracking

Connect findings with actions and follow-up instead of presenting indicators without a remediation workflow.

Not a replacement for EDR or SIEM, and not a security certification or automatic compliance guarantee.

Reporting and scheduled reports

Scheduled Reports is a development priority, not a confirmed capability in the current release.

Operational reporting

A proposed summary of inventory, device status, task outcomes and patch results.

Recurring schedules

Prepare daily, weekly or monthly reporting aligned with operational and management needs.

Controlled distribution

Define recipients, output formats and permitted data before enabling report delivery.

Export formats, delivery channels and execution schedules will be defined when implementation is approved.

Integration with INFRYX

A proposed architectural direction to connect endpoint management with service management.

Link assets and tickets

Proposed mapping between a POINTRYX endpoint and its asset record and ticket in INFRYX ITSM.

Actionable alerts

Convert selected conditions into notifications or tickets while avoiding duplicates and excessive alerts.

Integration interfaces

Design documented APIs and webhooks with permissions and event logging before enabling integration.

Existing ITSM interfaces or integrations are not assumed to be available within POINTRYX.

Editions and licensing model

Edition names were previously discussed; final feature allocation requires commercial and technical approval.

Essentials

Proposed positioning for core needs: endpoint visibility, inventory and initial operations.

Professional

Proposed positioning for teams needing scheduling, patch management and broader support tools.

Enterprise

Proposed positioning for advanced requirements, integrations and reporting within an agreed scope.

Device and user limits, license term, pricing and support will be defined in a separate quotation.

Phased deployment plan

A proposed implementation approach, not an approved capacity specification.

Prepare the environment

Define the management server, connectivity requirements, permissions, backups and operational ownership.

Run a limited pilot

Deploy the agent to representative devices and exercise inventory, tasks, patching and restart behavior.

Expand in stages

Roll out in batches after documenting results and approving support and rollback procedures.

Server sizing and rollout batch sizes must follow load testing and assessment of the actual environment.

Customer demonstration scenario

A practical demo that connects each product claim with behavior that can be demonstrated.

Explore an endpoint

Show a test device, its information, installed software and agent connectivity status.

Execute a task

Schedule a safe task on a test endpoint, then review its status, outcome and restart behavior.

Demonstrate operations

Show MFA, a backup and a restore exercise, clearly separating available features from development items.

Use an authorized test environment, not production endpoints without approval.

How do we measure pilot success?

Proposed evaluation metrics; this presentation contains no assumed performance figures.

Management coverage

Measure enrolled devices against the target population and review the freshness of agent contact.

Execution quality

Track task success, failure causes and devices requiring a restart.

Operational readiness

Review support-scenario completion time, restore-exercise success and feedback from the IT team.

Agree on a baseline and acceptance targets before the pilot, then use actual results only.

Proposed product roadmap

Priorities remain subject to review, with no commitment to unconfirmed dates or availability.

First priority

Stabilize patching, scheduling and restart workflows, then complete Security Posture and Scheduled Reports.

Second priority

Design INFRYX ITSM integration and notification channels after defining the required use cases.

Later phase

Evaluate an AI assistant and refine the management experience using usage data and customer feedback.

Software Center is excluded from scope, consistent with the earlier decision to omit it.

From endpoint visibility to organized operations

POINTRYX Endpoint Manager | INFRYX

**Start with a focused pilot.
Review the results.
Then expand with confidence.**

Recommended next step: define device scope, review the available release, and agree on clear acceptance scenarios before the final quotation.

Based on the discussed project scope. Not a compliance certificate or a contractual feature schedule.