N-ABLE N-central
Endpoint Management

Service Description



N-ABLE™

1. Executive Summary

N-central is a security-first Unified Endpoint Management (UEM) platform that enables IT teams to proactively secure, automate, and manage environments, delivering endpoint resilience and operational efficiency at scale.

- **Reduced risk and stronger security posture:** Autonomous endpoint hardening, continuous vulnerability management, and policy-driven security controls minimize the attack surface across Windows, macOS, Linux, cloud, and network devices
- **Faster operations through embedded AI:** N-zo, an embedded AI assistant, delivers context-aware guidance, troubleshooting, and risk insights grounded in live environment data, enabling up to 70% faster IT operations across common tasks
- **Greater efficiency through deep automation:** Powered by the Infinity Core™ engine, N-central provides unmatched flexibility with data-centric filtering, adaptive rules, policy-driven workflows, and AI-assisted scripting, amplifying team output and driving standardization across the device lifecycle
- **Simplified compliance and reduced tool sprawl:** N-central unifies asset management, remote access, monitoring, patching, security, and vulnerability management into a single platform, reducing complexity and supporting compliance with SOC 2 Type II, ISO 27001, HIPAA Type 1, and CMMC readiness
- **Open, extensible ecosystem:** Broad out-of-the-box integrations, extensive REST and GraphQL APIs, an AI-powered Developer Portal, and MCP Server connectivity let IT teams build seamless workflows across their ideal tech stack—without vendor lock-in

N-central continuously discovers, secures, automates, and learns from every endpoint, transforming devices from potential vulnerabilities into a hardened first line of defense.

2. Functional Capabilities

N-central delivers a comprehensive set of capabilities across endpoint management, security, automation, AI, remote access, and integration, designed to work together as a unified platform for stronger endpoint resilience and greater operational efficiency.

Endpoint Visibility and Discovery

- **Cross-platform endpoint management:** Provides visibility and monitoring across Windows, macOS, and Linux endpoints, including Azure and Windows 365 cloud workloads
- **Continuous network discovery:** The probe-and-agent architecture continuously scans the environment, automatically detecting devices joining or leaving the network
- **Automated device onboarding:** Automatically discovers and imports managed devices into monitoring, configuration, and lifecycle management workflows
- **Self-healing monitoring:** Delivers configurable notification templates, active dashboards, and alerts with automated self-healing responses
- **Network device monitoring:** Supports monitoring for Cisco, Fortinet, HP, Juniper, SonicWall, and other network devices with SSH, SNMP, and custom MIBs
- **Apple device management (MDM):** Provides full MDM capabilities for macOS, iPadOS, and iOS with seamless Apple Business Manager integration, managed alongside Windows in a single dashboard

Security, Patching, and Vulnerability Management

- **Automated patch management:** Detects and patches all Microsoft operating systems (including out-of-band updates) and 300+ third-party applications with 99.9% patch reliability. Supports on-schedule, on-demand, and wake-to-patch deployment, including closed networks
- **Built-in vulnerability management:** Performs continuous vulnerability scanning across 900+ applications with risk-based prioritization using CVSS scoring, exploitability, and CISA KEV status. Supports remediation through patching, software management, and automation
- **Security configuration and hardening:** Enforces security configurations and standards aligned with NIST and CIS controls through automation. Continuous monitoring detects configuration drift and brings endpoints back into compliance
- **Application allow/block controls:** Prevents risky software execution and reduces app sprawl across managed environments

- **Device encryption ,anagement:** Manages device encryption, monitors compliance status, and stores recovery keys securely
- **Integrated threat protection (optional add-on):** Provides integrated EDR, XDR, and MDR capabilities powered by SentinelOne, with 24/7 SOC monitoring, investigation, and response. Mass deploys and monitors endpoint security software
- **Shadow AI detection (upcoming):** Identifies unauthorized AI tools on managed endpoints, including installed applications, browser extensions, and network-level AI traffic via DNS classification
- **Secure-by-design architecture:** Built to meet SOC 2 Type II, ISO 27001, HIPAA Type 1, and CMMC 2.0 Level 2 compliance standards. Granular RBAC, encrypted communications, audit logging, and SIEM integration via syslog

Automation and Scripting (Infinity Core™)

- **Infinity Core™ engine:** N-central's unique data-centric architecture, comprising seven components—data-centric filtering, notification profiles, service templates, rules engine, policy-based configurations, scheduling and automation, and custom properties—enables unmatched flexibility and control over endpoint management
- **Data-centric filtering:** Allows for quick device segmentation using hundreds of data points to build dynamic, highly targeted filters for automation, policies, and reporting
- **No-code automation builder:** Provides a drag-and-drop workflow builder for creating automated processes without scripting knowledge
- **Pre-built automation library:** Includes 700+ ready-made scripts and recipes in the Automation Cookbook, with support for custom additions
- **AI-assisted scripting:** Translates natural-language requests into ready-to-run scripts in seconds using generative AI
- **Self-healing and scheduled workflows:** Supports automated patching, software management, onboarding, security deployment, and ticket automation to PSA systems, with inline automation embedded into policies and tasks

AI and Intelligence

- **N-zo – embedded AI assistant:** An in-product AI assistant inside N-central that delivers context-aware insights, troubleshooting, and risk guidance grounded in live environment data. Specialized expert agents include the Managed Assets Expert and Product Knowledge Expert (live), with Patch Expert, Script Expert, and Vulnerability Expert coming soon

- **MCP server:** An open-standard connection that lets any MCP-compatible AI tool (Claude, ChatGPT, Copilot, and others) connect directly to live N-central data to query environments, carry out supported actions, orchestrate multi-tool workflows, and build toward autonomous operations—without custom code or vendor lock-in
- **AI-powered Developer Portal:** Interactive API reference with built-in AI chat for N-central REST and GraphQL APIs. Developers can ask questions about documentation, discover automation recipes, and accelerate tech stack integration

Remote Access and Support

- **Integrated remote access:** Instant connection for management of servers, workstations, mobile devices, and network equipment (average 8-second connect time)
- **Backend device access:** Direct access to services, processes, files, registries, and more without interrupting end users
- **Live chat:** In-session and out-of-session live chat directly from the console
- **Support toolkit:** Built-in common scripts and tools for everyday technician tasks
- **Secure session management:** Fault-tolerant, AES-256 encrypted remote access with full session logging, audit trails, and session summary details

Reporting, Analytics, and Integration

- **Embedded Power BI analytics:** The only RMM with Microsoft Power BI embedded, providing industry-tested pre-built dashboards, custom analytics, and click-and-drill-down graphical interfaces
- **Open ecosystem integrations:** Out-of-the-box integrations with leading PSA/ticketing systems (Autotask, HaloPSA), IT documentation, and security solutions
- **Extensive APIs:** REST and GraphQL APIs for custom integrations, with AI-assisted documentation through the Developer Portal

3. Technical Interface

- **Endpoint/URL:** https://<n-central-server>/api
- **Protocol:** REST, SOAP (legacy); MCP Server for AI connectivity (future state)
- **Data formats:** JSON, XML
- **Authentication:** OAuth2 / JWT bearer tokens, API Keys
- **Interface documentation:** N-able Developer Portal https://developer.n-able.com

4. User Access

- **Web-based console:** Per-tenant N-central console at https://<n-central-server>/; Partner Success Portal at https://me.n-able.com/s/
- **Required single sign-on URL access:** SSO is optional, not required
- **Two-factor / multifactor authentication (2FA/MFA):** Configurable per partner/tenant; can be enforced for all users
- **Supported 2FA/MFA authenticators:** TOTP authenticator apps (e.g., Google Authenticator, Microsoft Authenticator, Authy)

5. Quality of Service (QoS) and SLAs

Availability (Uptime)	Latency (Average)	Recovery Time (RTO)
99.9% (excluding scheduled maintenance)	< 200 ms for standard requests	4 hours in case of major region failure

6. Security and Governance

- **Data sensitivity:** Restricted
- **Compliance:**
  - GDPR
  - SOC 2 Type II
  - HIPAA Type 1
  - ISO/IEC 27001
- **Auditing:** Audit logs retained per platform policy; available via syslog / SIEM integration

7. Dependencies

Upstream Dependencies

- **Upstream dependencies:** AWS / cloud infrastructure; Microsoft (Windows Update catalog, Entra ID, Azure); Apple Business Manager / APNs; SentinelOne (for optional EDR/XDR/MDR add-on)
- **Downstream consumers:** PSA/ticketing systems (Autotask, HaloPSA); partner-built integrations via REST/GraphQL APIs; MCP-compatible AI tools (future state)

8. Support and Communication

- **Technical support details:** 24x7 phone, email, and chat support (premium support options available at a further cost).
- **Public status page:** https://status.n-able.com/
- **Partner success portal:** https://me.n-able.com/s/
- **Customer-facing communication:** Service availability, incidents, and planned maintenance activities are shared through the official N-able status page and established customer communication channels. Where relevant, additional context may be provided via in-product messaging or support notifications.
- **Maintenance windows:** N-central adheres to standard N-able SaaS maintenance policies. Planned maintenance with potential customer impact is communicated in advance via official status and notification channels, aligned with regional and platform-level maintenance windows.



N-able protects businesses from evolving cyberthreats. Our AI-powered cybersecurity platform delivers business resilience to more than 500,000 organizations worldwide, leveraging advanced end-to-end capabilities, simplified workflows, market-leading integrations, and flexible deployment options to improve efficiency and drive critical security outcomes. Our partner-first approach pairs our technology with experts, training, and peer-led events that empower customers to be secure, resilient, and successful. n-able.com

---

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.