NthEndpoint

SERVICE BROCHURE

Next-Generation Endpoint Management, Fully Managed

Patch management, MDM, endpoint security, and compliance reporting -- run as one managed operation, inside your own tenant.

nthendpoint.com · contact@nthendpoint.com

OVERVIEW

One managed operation, not five different tools.

NthEndpoint runs your entire endpoint console as a fully managed service -- patch management, mobile device management, endpoint security, and compliance reporting -- inside your own tenant. You keep visibility and ownership of the data; our operations team keeps it tuned, patched, and quiet. This brochure covers every capability included in every plan, in detail.

30+ hrs	99.9%	Zero	24/7
Given back to IT every month	Patch compliance, not best-effort	Surprise line items	Monitored operations

WHAT'S INSIDE

- Patch Management
- Vulnerability Management
- Endpoint Detection & Response (EDR)
- Data Loss Prevention & Encryption
- Browser Security
- Application & Device Control
- Secure Private Access (ZTNA)
- Mobile Device Management (MDM)
- Remote Control & Support
- Asset & Software Inventory
- Device Deployment & Imaging
- Digital Employee Experience (DEX)
- Compliance & Reporting

CAPABILITIES, IN DETAIL

Patch Management

OS and third-party patches are tested through a staging ring, scheduled around business hours, and rolled out fleet-wide.

- ✓ Windows, macOS, and Linux patched on one coordinated schedule
- ✓ Browsers, PDF readers, and collaboration software patched alongside the OS
- ✓ Canary and pilot rollout rings catch issues before fleet-wide release
- ✓ Same-day rollback if a patch causes regressions
- ✓ Typical patch window: 24-48 hours from release

Vulnerability Management

Continuous CVE scanning with fixes ranked by real-world exploitability, not just severity score.

- ✓ Continuous scanning for CVEs and risky misconfigurations
- ✓ Risk-based prioritization by exposure and asset criticality
- ✓ End-of-life and unsupported software flagged automatically
- ✓ Findings tracked from discovery to close with an owner and timeline
- ✓ Monthly exposure trend reporting

Endpoint Detection & Response (EDR)

Behavioral threat detection catches what signature-based antivirus misses, with rapid containment when it matters.

- ✓ ML-based behavioral threat detection across the fleet
- ✓ One-click isolation of compromised endpoints
- ✓ 24/7 monitored triage, not a dashboard nobody checks
- ✓ Full attack timeline and root-cause investigation
- ✓ Typical isolation response: under 5 minutes

Data Loss Prevention & Encryption

Sensitive data is tracked and controlled at the endpoint, with fleet-wide disk encryption enforced and verified.

- ✓ Pattern-based sensitive data monitoring across email, USB, and cloud uploads
- ✓ Fleet-wide disk encryption enforcement with secure key escrow
- ✓ PCI-DSS, HIPAA, and GDPR-aligned controls
- ✓ Continuous compliance logging, not a point-in-time attestation
- ✓ 100% encryption coverage on managed devices

Browser Security

Extension policy and safe-browsing enforcement applied fleet-wide, with no per-user configuration required.

- ✓ Extension allow/block lists enforced per role
- ✓ Real-time malicious and risky-site blocking
- ✓ Consistent policy across Chrome, Edge, and Safari
- ✓ Fleet-wide compliance reporting, not individual browsing logs

Application & Device Control

Every endpoint runs on a least-privilege default, with application and peripheral policy tuned per role.

- ✓ Application allow/block lists set per role
- ✓ Endpoint privilege management with just-in-time elevation
- ✓ USB and peripheral device control fleet-wide
- ✓ Monthly policy review as roles and tools change

Secure Private Access (ZTNA)

Zero-trust access to internal apps and file shares, with no traditional VPN and no exposed network perimeter.

- ✓ Per-application access instead of full network access
- ✓ Device compliance re-checked at every connection, not just login
- ✓ No internet-facing VPN endpoint to attack
- ✓ Full connection and access audit trail

Mobile Device Management (MDM)

Phones and tablets get the same operational discipline as laptops -- enrolled, policy-managed, and remotely wipeable.

- ✓ Zero-touch enrollment with policy applied automatically
- ✓ Work-profile isolation keeps corporate and personal data separate
- ✓ Remote lock and wipe within minutes of a reported loss
- ✓ Passcode, encryption, and jailbreak/root detection enforced
- ✓ Full iOS and Android platform coverage

Remote Control & Support

Live remote sessions to fix issues in real time, logged to your existing help desk process.

- ✓ Direct remote control for real-time diagnosis and fixes
- ✓ Sessions visible to the user -- no silent background access
- ✓ Every session logged against your existing help desk ticket
- ✓ Same-day response commitment on fleet-impacting incidents

Asset & Software Inventory

A live, real-time record of every device, application, and license -- not a quarterly audit project.

- ✓ Full hardware specification and warranty tracking per device
- ✓ Real-time installed-application tracking, fleet-wide
- ✓ License reconciliation surfaces overspend and compliance risk
- ✓ On-demand export for budgeting, audits, or due diligence

Device Deployment & Imaging

New devices go from box to fully provisioned and policy-compliant before a new hire's first login.

- ✓ Zero-touch provisioning -- ships direct to the end user
- ✓ Standardized OS images across hardware models
- ✓ Encryption, patch baseline, and EDR enrollment before first use
- ✓ Secure wipe and re-imaging for redeployed hardware

Digital Employee Experience (DEX)

Real-time monitoring of how endpoints actually feel to use, catching problems before they become tickets.

- ✓ Boot time, crash rate, and battery health tracked continuously
- ✓ Per-device experience scoring across the fleet
- ✓ Proactive fixes before a support ticket is ever filed
- ✓ Hardware refresh recommendations based on real degradation data

Compliance & Reporting

Every policy, patch, and access event is logged and mapped to your compliance framework automatically.

- ✓ Ongoing audit against 75+ CIS benchmarks
- ✓ Automatic certificate lifecycle tracking and renewal
- ✓ Mapped to PCI-DSS, HIPAA, and GDPR as relevant
- ✓ Audit-ready report delivered automatically, every month

PRICING

Priced per endpoint, not per headache.

Every tier includes the platform license, our operations team, and a monthly fleet-health report. Billed monthly in USD internationally or INR in India, with a 25-endpoint minimum.

ESSENTIALS

Patch management & inventory

$3.50 / endpoint
billed monthly, 25 endpoint minimum

- ✓ OS & third-party patching
- ✓ Hardware & software inventory
- ✓ Business-hours support
- ✓ Monthly compliance report

MANAGED FLEET

Full patching, MDM & remote support

$6.25 / endpoint
billed monthly, 25 endpoint minimum

- ✓ Everything in Essentials
- ✓ Mobile device management
- ✓ Remote control & support
- ✓ 24/7 monitoring with SLA

ENTERPRISE

Custom compliance & security policy

Custom
volume pricing above 500 endpoints

- ✓ Everything in Managed Fleet
- ✓ App & device control policy
- ✓ Custom compliance frameworks
- ✓ Dedicated operations lead

GET STARTED

Get a free fleet audit before you commit to anything.

We'll show you exactly where your patch posture and security gaps stand today, delivered within 48 hours.

nthendpoint.com · contact@nthendpoint.com