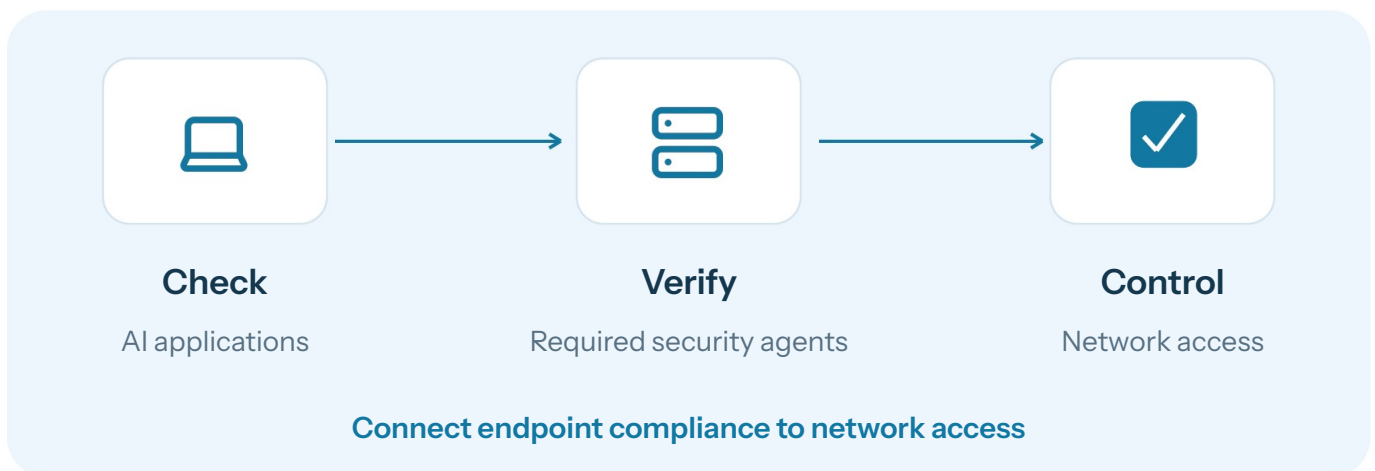


## WHITE PAPER

# Managing Shadow AI with EasyNAC

## Application checks and endpoint compliance

Use the EasyNAC endpoint agent to check AI desktop applications and require data loss prevention (DLP) and other inspection agents to be running before granting network access.



### FOR IT AND SECURITY TEAMS

An agent-based deployment approach, four practical scenarios and a standalone pilot for IT and security teams managing Shadow AI risk.

EasyNAC and vLinks are trademarks of InfoExpress, Inc. Other product and service names are trademarks and service marks of their respective owners.

Copyright © 2026 InfoExpress Incorporated. All Rights Reserved. InfoExpress products and services are protected by one or more of the following U.S. Patents: 8347351, 8347350, 8117645, 8112788, 8108909, 8051460, 7523484, 7890658, 7590733. Additional patents pending.

## 01 / EXECUTIVE SUMMARY

# Make endpoint compliance a condition of access

Use EasyNAC endpoint agents on managed devices to check selected AI desktop applications and verify that required security agents are installed and running. Connect those results to network access policy so a failed compliance check leads to restricted access, with a defined path to recovery. [3]

Shadow AI is the use of AI tools, models or autonomous agents outside an organization's approval and oversight. A desktop assistant or local inference application may run on an otherwise trusted laptop. A user may also stop the DLP or web inspection agent intended to protect that laptop. Device ownership alone does not address either situation.

## Connect three endpoint questions to access

| Question                                            | Why it matters                                                                                                                |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Which AI applications are present or running</b> | Check defined process, version, file or registry indicators against your approved application policy.                         |
| <b>Are required protection agents running</b>       | Require the selected DLP, web inspection or endpoint security processes to pass the configured checks.                        |
| <b>What access follows the result</b>               | Grant the required access only when the rules pass. Define restricted access for failed, missing or stale compliance results. |

Use agentless discovery alongside the agent to control unknown hardware and devices that cannot run it. Maintain an approved AI inventory and incident response process as part of wider governance. [1] Reassess trust beyond device ownership or network location. [2]

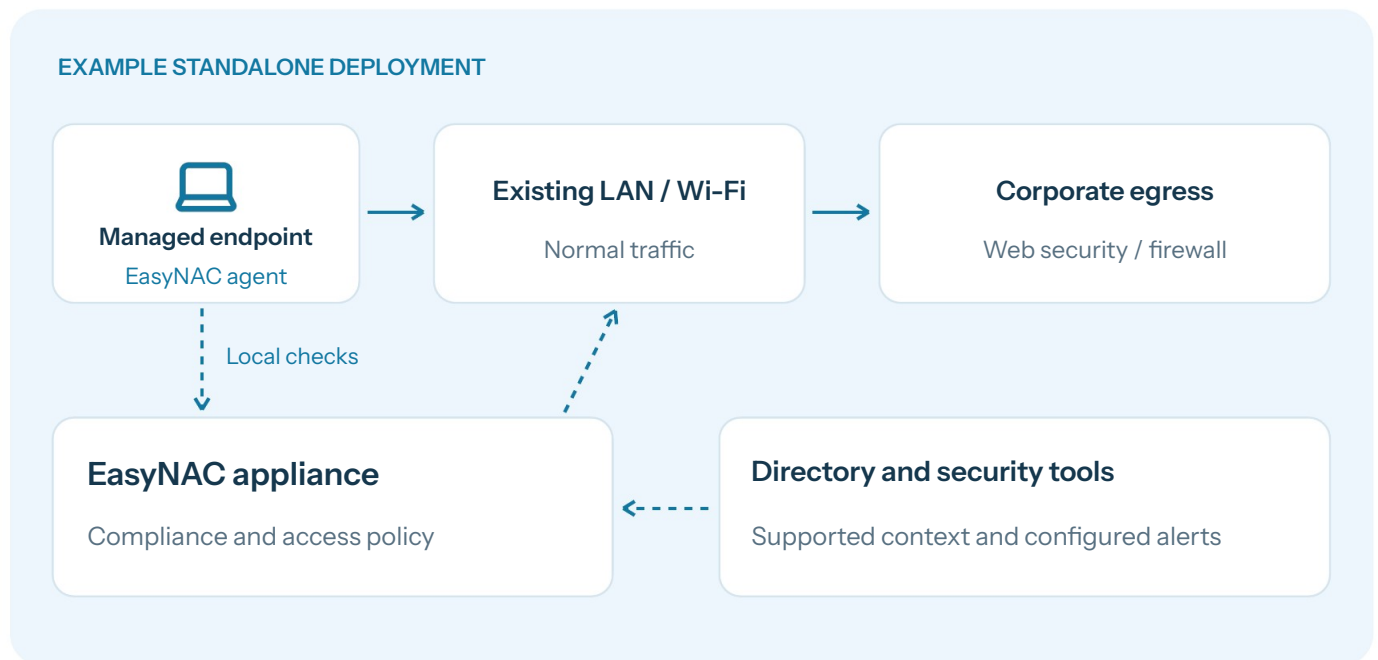
## Check protection readiness and control access

EasyNAC checks the endpoint conditions you configure and applies device access policy. DLP and other inspection products examine content and activity. An application or process check does not inspect AI prompts, and a running process alone does not prove that every function of a security product is healthy.

## 02 / DEPLOYMENT APPROACH

# Add agent checks to your network

Install the EasyNAC agent on the managed endpoints in scope and configure their compliance policies on the standalone appliance. The agent supplies local check results. EasyNAC uses out-of-band ARP enforcement on covered network segments while normal permitted traffic follows its existing path. [3]



Configure the endpoint agent to audit the chosen application indicators and required security processes. Tie a passing result to the access the device needs. Give a failing or unavailable result a defined restricted policy. Validate agent support, licensing and communication requirements for the endpoint platforms in your pilot.

## Cover both managed and unmanaged devices

Agentless discovery and unknown-device policy complement agent checks for personal laptops, printers, IoT and unapproved lab hardware. Confirm appliance connectivity and enforcement on the actual wired and wireless paths. Enforcer Sensors can extend coverage to selected branches when the deployment requires them. [5]

### Keep the surrounding controls connected

Existing 802.1X can remain in place alongside EasyNAC. Your network routing and security tools still control the inspection path; off-network traffic needs the appropriate endpoint and web controls. Start with a standalone appliance and the endpoints in scope.

## 03 / ENDPOINT COMPLIANCE

# Check applications and required protection

EasyNAC agents support running-process and version checks, registry values, files and locations, and other local compliance checks. [3] Choose the indicators that answer your actual access requirements and test them on representative endpoints.

## Identify selected AI desktop applications

Build rules for the AI assistants, desktop clients and local inference tools relevant to your environment. A running-process check identifies a configured application while it is active. File or registry indicators can establish its presence when it is not running. Use the appropriate combination to distinguish an installed application from one currently in use.

Decide whether each application is approved, permitted only for a particular team, or prohibited on endpoints with sensitive access. Maintain the indicators as applications change. These configured checks do not establish a complete inventory of all AI software or every use of a browser-based service.

## Require DLP and inspection agents to be running

Make the required DLP, secure web gateway (SWG), endpoint detection and response (EDR), or other content detection agent part of the compliance policy. Check installation and the expected running processes. Add version or configuration indicators where supported and validated for that product. Grant the required access only after the applicable checks pass.

## Recheck compliance while the device is connected

Use ongoing compliance checks to respond when a required process stops or a disallowed application starts. Define how missing or stale audit results affect access. Check frequency and enforcement timing are pilot measurements, not assumptions. Add supported security-tool health signals when process state alone is insufficient.

### Give failed checks a recovery path

Allow only the approved remediation access needed to restore compliance. EasyNAC agents can support configured remediation scripts or executables. Use approved actions, then recheck the endpoint before restoring normal access. [3]

## 04 / PRACTICAL SCENARIOS

# Act on AI application and protection checks

These agent-based scenarios turn an endpoint condition into a clear access decision. Use approved test applications and dummy data so the pilot does not expose business information.

**SCENARIO 01**

## An unapproved AI desktop application

**The risk.** An employee starts an unapproved AI assistant or local inference tool on a company laptop that otherwise meets normal device trust rules.

**The EasyNAC response.** Use the EasyNAC agent to check the defined process and, where needed, version, file or registry indicators. Apply the configured restricted access policy when the prohibited condition is detected. Keep any approved exception specific to the device and business need.

**What to prove.** The selected application indicator changes the endpoint compliance result and access as intended. An approved application and a healthy peer remain unaffected. Recheck after closing or removing the prohibited application.

**SCENARIO 02**

## A required DLP or inspection agent stops

**The risk.** An endpoint has access to business resources even though its required DLP or inspection process is stopped, missing or no longer meets the configured compliance rule.

**The EasyNAC response.** Require installation and running-state checks for the selected security agent before granting the required access. Continue checking while connected. If the rule fails, restrict access to the defined remediation scope and guide the user to restore protection.

**What to prove.** Stop the selected process in the approved lab. Confirm the failed check and resulting access restriction. Restart it, recheck compliance and verify the intended restoration path and an unaffected healthy peer.

The access decision uses the conditions actually checked. If a security product can remain running while inspection is disabled, add a validated configuration or health signal for that condition.

## 05 / PRACTICAL SCENARIOS

# Control unknown hardware and approved AI hosts

Agent compliance on managed endpoints works alongside network discovery and access policy. Use that combination to cover devices that cannot run the agent and to limit the reach of approved AI infrastructure.

## SCENARIO 03

## An unmanaged laptop or unauthorized AI host

**The risk.** An employee connects a personal laptop, or a team adds an unapproved GPU workstation to the corporate network. The device has no approved endpoint compliance result.

**The EasyNAC response.** Use agentless discovery and the unknown-device policy to restrict its access. Provide only the approved registration or remediation destinations where configured. A legitimate lab exception needs a defined scope and expiry.

**What to prove.** The unknown device cannot reach selected internal resources, while an approved peer continues working. Confirm discovery and enforcement timing and verify that an expired exception restores the intended default.

## SCENARIO 04

## An approved AI host with excessive reach

**The risk.** A sanctioned inference or retrieval host can reach unrelated business systems. Its application may be approved while its network permissions are broader than the project needs.

**The EasyNAC response.** Define the host's required destinations and access policy. On supported managed hosts, add the relevant agent compliance checks. Keep model API authentication, service identities and repository permissions with their application owners.

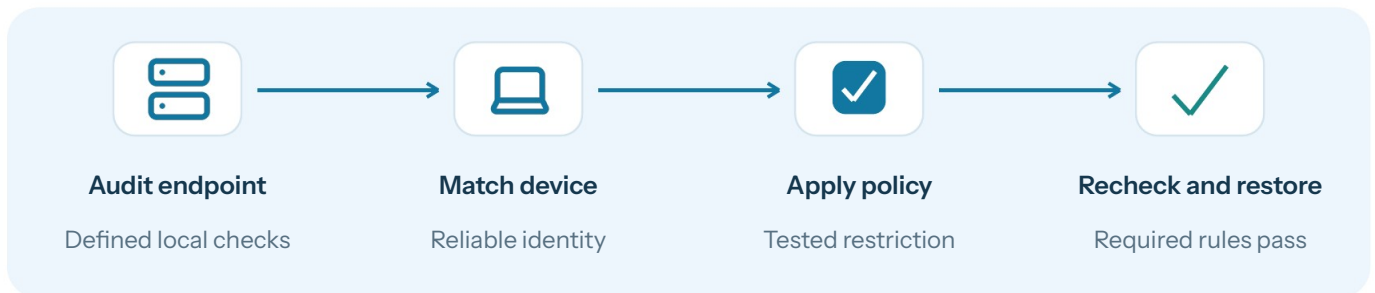
**What to prove.** Required connections work and the selected out-of-scope destinations are restricted on covered paths. Recheck both access and endpoint compliance after a deployment or policy change.

Unknown hardware can be restricted because it is unknown. Identifying it as an AI server needs application evidence. Device access policy does not grant separate permissions to every process or AI agent sharing an allowed host.

## 06 / DETECTION AND RESPONSE

## Connect compliance to access

Build a complete workflow around the compliance result: check the endpoint, apply the appropriate access rule, help restore protection, and recheck before release. Add external security events where they provide useful evidence about AI activity or content risk.



### Use the compliance result for the condition it proves

An EasyNAC agent check can establish that a configured AI application is active or that a required security process has stopped. Record the failing rule and affected device so the user and support team know what to fix. For missing or stale results, follow the explicit access policy rather than assuming the last passing state remains valid.

### Add content and threat signals from their owners

EasyNAC can use supported security integrations and configured syslog or email alerts. [3] When DLP, EDR or web security identifies a confirmed event, validate its delivery and endpoint match before applying a network response. The originating product determines the content or threat finding; EasyNAC supplies the configured device access action.

Match events to the correct endpoint, including multiple adapters and reused IP addresses. Lateral-spread and deception events can also support containment; they do not establish an AI-specific attack. [4]

### Restore protection before restoring required access

Tell the user which condition failed and provide the approved remediation path. Use configured agent scripts where appropriate. Recheck required rules after repair; retain analyst approval where the incident needs review. Verify normal access and a healthy peer when the response is complete.

#### Keep the response proportional

Restrict the access required by policy on the covered paths. Network containment supports investigation and repair; it does not erase information already disclosed or replace application cleanup and credential review.

## 07 / STANDALONE PILOT

# Prove application and protection checks

Use a standalone appliance, one protected subnet, two supported managed endpoints and an unknown test device. Install the EasyNAC agent on the managed endpoints. Agree the AI application indicators, required security processes and pass or fail access policies before enforcement.

| Test                           | Success to demonstrate                                                                                                                                                |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Establish a passing baseline   | Agent checks pass with required security processes running. Approved AI applications and required business access work.                                               |
| Check an AI application        | Start the selected test process. Confirm the configured indicator and policy response. Separately test an installed-but-closed application if that condition matters. |
| Stop a required DLP agent      | Stop the chosen process in an approved lab. Confirm a failed check, restricted access and an unaffected healthy peer. Test a missing installation where relevant.     |
| Test unavailable audit results | Interrupt the EasyNAC agent reporting path safely. Verify the configured treatment of missing or stale results and record the timing.                                 |
| Restrict unknown hardware      | Connect a labelled device without an approved compliance result. Verify its defined registration or restricted access scope.                                          |
| Repair and recheck             | Restore the required protection or remove the prohibited condition. Recheck compliance and verify normal access follows the agreed release policy.                    |

## Measure timing and effort on your own endpoints

Measure audit freshness, detection-to-restriction time, recovery time and the work needed to maintain application rules. Test both initial access and changes after connection. Keep a rollback plan and use dummy data; stop security processes only on the approved pilot endpoints.

The Agentless NAC Evaluation Kit provides the network deployment foundation. [6] Add the agent checks above for this use case. No central management or branch rollout is needed for this standalone pilot.

## 08 / OPERATING MODEL

# Keep application rules and access aligned

The lasting benefit comes from making approved AI use and required endpoint protection part of everyday access policy. Assign owners to the checks, their exceptions and the recovery process so they stay useful after the pilot.

## Maintain the AI application rules

Keep an approved inventory with the business purpose, application or service, responsible team and permitted data. [1] Maintain the process, version, file or registry indicators used by EasyNAC. Revalidate them after application updates, and distinguish observation rules from rules that restrict access.

## Own the required protection baseline

Identify the required DLP and other inspection agents for each endpoint group. Document which installation and running-state checks must pass and which additional health signals matter. Agree the audit freshness rule, remediation destinations and restoration conditions with the teams that operate those products.

## Make exceptions specific and temporary

A research team may need an AI tool that ordinary users cannot run. Specify the device group, application, permitted destinations, approver and duration. Review exceptions and remove them when the work ends. An exception for an AI application should not silently waive required DLP or endpoint protection checks.

## Retain content controls and review changes

DLP and web controls continue to govern prompts, uploads and browser-based AI use. Application owners retain repository permissions and model API authentication. Review compliance failures and user recovery experience; revalidate rules after agent, security-tool or network changes. Off-network activity needs the controls designed for that path.

### Use the agent where the endpoint condition matters

EasyNAC connects selected AI application checks and required security-agent state to network access. Agentless discovery complements it for unmanaged hardware. Demonstrate the restriction and recovery workflow on your own endpoints, then expand the policies that deliver useful results.

Plan an EasyNAC endpoint agent pilot

Use the Evaluation Kit for the network pilot foundation

# References and further reading

The references below support the governance principles and published product capabilities discussed in this paper. The deployment scenarios and pilot measures are practical recommendations for applying those capabilities to Shadow AI risk.

## [1] NIST AI 600-1

Artificial Intelligence Risk Management Framework Generative Artificial Intelligence Profile  
July 2024. AI inventory, acceptable use and incident response actions.

## [2] NIST SP 800-207

Zero Trust Architecture  
August 2020. Device and user trust beyond network location or ownership.

## [3] EasyNAC FAQ

Endpoint agents and compliance checks  
Running processes and versions, registry values, files and remediation.

## [4] EasyNAC Solutions

Use cases and deployment concepts  
Unknown devices, fingerprinting, guests, BYOD, lateral spread and deception.

## [5] EasyNAC Products

Appliances and Enforcer Sensors  
Deployment options for existing networks.

## [6] EasyNAC Evaluation Kit

Agentless NAC Evaluation Kit  
Network pilot foundation. Add the endpoint agent tests in this paper.

Published October 2026 by InfoExpress Inc.  
Product sources accessed 9 October 2026.