A PRACTICAL PROOF-OF-CONCEPT GUIDE

Agentless NAC Evaluation Kit

See what is connected.
Prove what you can control.

A standalone pilot plan, ten hands-on tests and an editable scorecard to help you evaluate EasyNAC on your network.



Discover
Inventory

Verify
Device context

Control
Tested access

Your devices. Your policies. Your evidence.

INCLUDED IN THE KIT

Pilot planning and architecture / Ten repeatable tests
Deployment checklist / Results and decision workbook

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.

infoexpress www.easynac.com

01 / PLAN THE PILOT

Start with a decision to make

Use a representative slice of your network to answer a specific buying question.

EXAMPLE EVALUATION OBJECTIVE

Can our team identify unexpected devices and apply the right access policy on the selected network paths, with a recovery process we can operate?

01

Scope

Choose the devices, traffic paths and integrations for a standalone appliance. Define what a successful pilot must demonstrate.

02

Observe

Build a baseline inventory. Reconcile it with your reference list and review profiles before enabling enforcement.

03

Exercise

Run the selected tests. Mark unselected integrations or workflows as N/A with a scope reason. Capture console evidence and real endpoint traffic results.

04

Decide

Review the evidence, exceptions, effort and unresolved gaps. Agree whether to expand, retest or close the evaluation.

USE THE COMPANION WORKBOOK

Deployment checklist: record readiness and outstanding actions.
Scorecard: agree a criterion for each test, record actual results and select an outcome. Use the same test IDs as this guide.

02 / MAP THE DEPLOYMENT

Know what goes where

Start with a standalone appliance. Add branch coverage only if it is part of your pilot.

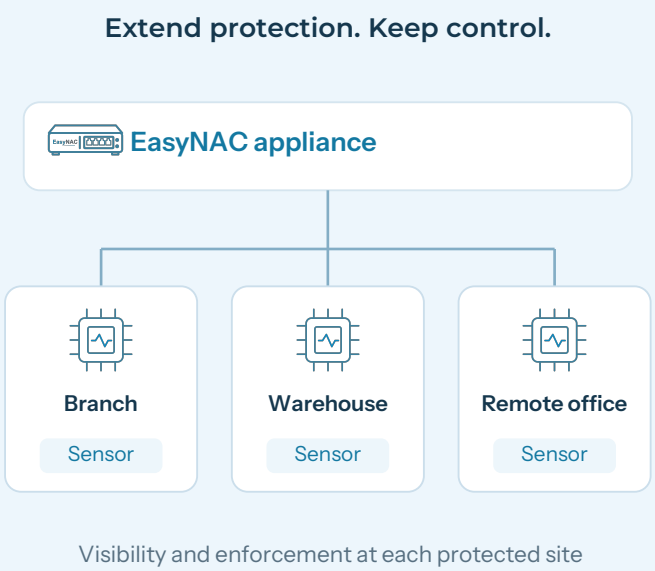


START HERE / STANDALONE

One appliance. A complete local pilot.

Discover devices, verify posture and enforce access policies on your selected network.

Use your existing switches and Wi-Fi.



OPTIONAL / SELECTED SITES

Enforcer Sensors

Extend local visibility and enforcement under the direction of your EasyNAC appliance.

Not required for a local standalone pilot.

Windows · Linux · Raspberry Pi

Illustrative product relationships, not network traffic paths. The rack represents one appliance, available as hardware or virtual. Include only the sites selected for your pilot.

03 / PREPARE

Make the pilot repeatable

Complete the Deployment checklist before moving from observation to enforcement.

01 Define the sample

Include managed and unmanaged devices, wired and wireless paths, and a branch if relevant. Record which critical systems remain observe-only.

02 Confirm the topology

Connect the appliance to the protected VLANs and assign the required addresses. A SPAN/mirror port is not required. Confirm placement for the selected LAN and Wi-Fi. [1, 2]

03 Prepare integrations

Prepare AD Auto Trust and the supported AV/EDR/patch sources selected for the pilot. Confirm device matching, available fields and data freshness.

04 Set the access rules

Write down permitted, blocked and remediation destinations. Define what happens when a device is unknown or posture evidence is absent.

05 Arrange recovery

Name the rollback operator, preserve administrator access and agree a test window. Keep the procedure with the evidence folder.

WHAT AGENTLESS MEANS IN THIS EVALUATION

No dedicated NAC agent is installed on test endpoints. The standalone appliance discovers devices and applies the selected policies. Detailed security posture comes from the supported integrations selected for your pilot. [2, 3]

04 / TESTS 01-02

See devices. Establish trust.

Discover the device sample and validate trust against Active Directory.

01 Agentless network visibility

Can you see managed and unmanaged devices?

Set up. Choose known laptops, phones, printers and IoT devices on the pilot LAN and Wi-Fi. Keep a reference inventory.

1. Connect the sample without installing a NAC agent on the endpoints.
2. Compare discovered MAC/IP addresses, hostnames and available device details with the reference list.
3. Reconnect a test device and check the updated inventory. Resolve missing or duplicate records.

Record. Inventory export, expected device list and discovery timestamps.

Accept when. The agreed device sample is visible within the agreed interval, without endpoint NAC agents.

02 Active Directory Auto Trust

Can domain membership drive device trust?

Set up. Connect a supported AD integration. Use one valid domain computer and one designated non-domain test device.

1. Check the AD match and Auto Trust result for the domain computer.
2. Connect the non-domain device and verify it does not receive domain-based trust.
3. Check access for both devices against the agreed domain and unknown-device policies.

Record. AD match, trust decision, assigned policy and endpoint traffic results.

Accept when. Valid AD computers receive the agreed trust policy; the non-domain device follows its separate access policy.

05 / TESTS 03-04

Verify posture and identity

Use security integrations and device fingerprints to inform access.

03 Agentless security compliance

Can existing security tools inform access?

Set up. Select a supported AV, EDR or endpoint-management integration and the posture fields it actually supplies.

1. Record a compliant device and its source status, such as AV health or patch status where available.
2. Use an approved test noncompliance condition and check the resulting access or remediation policy.
3. Restore compliance, refresh the integration and verify the intended access returns.

Record. Source status and time, device match, policy change and traffic checks.

Accept when. The selected compliance signal drives the agreed restriction and restoration within the agreed interval.

04 Device profiling & MAC-spoofing protection

Can trust go beyond an allow-listed MAC address?

Set up. Profile known device types. Reserve two isolated lab endpoints and test identities for the spoofing check.

1. Compare device type, OS and hostname where available; apply the agreed profile or custom tag.
2. With the original lab endpoint disconnected, reuse its test MAC on the second lab endpoint.
3. Check the fingerprint mismatch, trust decision and configured response; restore the test identity.

Record. Profiles, fingerprint differences, trust decision and access results.

Accept when. The agreed profiles are usable, and the simulated impersonator does not inherit trusted access.

06 / TESTS 05-06

Restrict unknown and risky devices

Test rogue-device control and lateral-spread protection on the pilot network.

05 Rogue-device detection & restriction

Can you restrict an unknown device on its VLAN?

Set up. Trust the approved pilot devices. Define allowed, blocked and remediation destinations for one unknown test device.

1. Connect the unknown device and record detection, alert and assigned access policy.
2. Test its allowed and blocked destinations on the existing VLAN, without moving it to a quarantine VLAN.
3. Check an approved peer remains connected, then approve or release the test device and verify access.

Record. Device record, ACL/policy, alerts, traffic results and release record.

Accept when. The unknown device is restricted as agreed while the approved peer retains access on the existing network.

06 Lateral-spread protection

Can suspicious scanning trigger protection?

Set up. Enable the agreed detection policy. Use a designated lab source and reserved test targets; use no actual malware.

1. Run a bounded, benign scan using the agreed lab procedure and targets.
2. Check the detected activity, source device and configured alert or restriction.
3. Verify the source access result and an unaffected peer, then release the test device and restore access.

Record. Test scope, detection event, response policy and traffic checks.

Accept when. The agreed scan is detected and triggers the configured response against the correct test device.

07 / TESTS 07-08

Register with control

Give staff and visitors the access they need under separate policies.

07 Controlled BYOD registration

Can staff register devices within your rules?

Set up. Prepare the BYOD portal, permitted user groups and device rules. Use test users and personal test devices.

1. Register a device as an eligible user and check the owner association and assigned policy.
2. Check permitted and restricted destinations from the registered device.
3. Test an excluded user or device and, if configured, the per-user device limit. Revoke the test registration.

Record. Registration, user/device rules, policy, traffic and revocation records.

Accept when. Eligible BYOD devices receive the agreed access; excluded registrations and configured limits are enforced.

08 Guest & consultant access

Can visitors get only the access they need?

Set up. Prepare a guest template or consultant role, a test sponsor, permitted resources and an access expiry time.

1. Pre-register or approve the visitor through the selected sponsor workflow.
2. Connect the visitor device and check its limited-access policy against allowed and blocked destinations.
3. Confirm access expires or is revoked as configured, and retain the sponsor and visitor records.

Record. Approval, visitor policy, traffic checks and expiry/revocation record.

Accept when. The approved visitor receives only the agreed access, which ends at expiry or revocation.

08 / TESTS 09-10

Detect. Respond. Verify.

Turn security alerts and deception events into a traceable response.

09 Automated threat response

Can a security alert trigger network restriction?

Set up. Configure a supported security alert source and response rule. Use a benign event identifying a designated lab endpoint.

1. Send the test alert through the agreed integration or monitored alert mailbox.
2. Check the endpoint match, response rule and actual restriction; confirm an approved peer remains connected.
3. Review the event trail and optional SIEM/syslog output, then authorize release and verify access returns.

Record. Source event, endpoint match, action log and traffic results.

Accept when. The alert restricts the correct endpoint as agreed, with an event trail and a verified release procedure.

10 Deception & hacking detection

Can a decoy expose suspicious activity?

Set up. Enable deception and identify the lab decoy/service and test source with the EasyNAC engineer.

1. Make a harmless connection or dummy login attempt to the designated decoy service.
2. Review the detection, source device and configured alert or response policy.
3. Check the recorded outcome and any configured restriction, then clear the test condition and restore access.

Record. Decoy/service, test event, source identity and configured response.

Accept when. The agreed decoy interaction is detected, attributed to the correct source and handled by the configured policy.

09 / REVIEW THE EVIDENCE

Turn the pilot into a decision

Record criteria, actual results and outcomes in the workbook. No evidence-link or test-owner fields are required.

MEASURE THE OUTCOMES THAT MATTER

Inventory coverage	Matched expected devices / expected test devices. Keep the same sample and observation window.
Profile accuracy	Correct agreed attributes / attributes checked. Record unknown and inferred values separately.
Response interval	Time from the agreed start event to verified restriction. Record the start event and each repetition.
Operating effort	Minutes spent on setup, exceptions, investigation and recovery. Separate one-time work from recurring tasks.

ONE-PAGE MANAGEMENT SUMMARY

Problem and scope	Which business exposure did the pilot address, and where?
Evidence and gaps	Which mandatory criteria were met? What needs a retest or an accepted exception?
People and cost	Account for licences, appliances/sensors, support, platform capacity, integration work and administration.
Recommendation	Expand, retest or close. Agree the next action and target date.

A passed test requires evidence against its agreed criterion. A blocked, untested or out-of-scope test is not a pass.

10 / NEXT STEPS

Evaluate EasyNAC on your network

Bring your device mix and access requirements. Use the kit to structure a focused technical discussion.

BRING THESE THREE THINGS

1. A simple site, subnet and wireless network map.

2. Your priority device groups and security integrations.

3. The access problem you want the pilot to resolve.

Request a guided evaluation

Discuss pilot scope, deployment requirements and the evaluation arrangements with EasyNAC.

TECHNICAL RESOURCES

1 **Standalone appliances and sensors**
Compare deployment components and current capacity tables.

2 **EasyNAC capabilities and FAQ**
Review agentless checks, access policies and integrations.

3 **Use cases and illustrated workflows**
Connect the tests to EasyNAC device and access scenarios.

4 **Resource Center**
Open the current deployment, compatibility and architecture documents.

Version 1.2, 9 October 2026. Based on the EasyNAC standard agentless POC plan and product documentation. Confirm release-specific setup, supported integrations and evaluation terms with the EasyNAC team.