

WHITE PAPER

Secure credit union networks without the heavy lifting

Agentless NAC for US credit unions

Strengthen device visibility, control network access and support compliance evidence while keeping your existing network architecture.



For IT leaders, security teams and risk officers
October 2026 | InfoExpress Inc.

A practical guide to protecting branch networks and member-facing operations with a manageable, staged approach to network access control.

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.

Protect members and keep work moving

Credit union security is inseparable from member service. A workstation that cannot reach a lending system, an unexpected device on a branch network or a compromised endpoint communicating with its neighbors can become an operational issue as well as a security issue. The challenge is to strengthen control without making routine service harder to deliver.

In its June 2026 report, NCUA recorded 588 cyber incidents reported by credit unions between May 1, 2025 and April 30, 2026. The reported incidents included ransomware, phishing, email compromises, ATM jackpotting and third-party provider incidents. This is a count of reported incidents, not a count of credit unions breached.¹

Make device trust an operational decision

A device being connected does not establish that it belongs there or that it should reach every resource. Network access control, or NAC, addresses that gap by making network access conditional on device trust and the organization's policy. For a credit union, useful questions are straightforward: What is connected? Who owns it? Does it meet the required security checks? What should it be allowed to reach?

EasyNAC combines agentless device discovery and profiling with access enforcement on protected network segments. Information from supported directory, endpoint protection, patch and device-management systems can inform access decisions. Guest registration, device fingerprinting, deception and automated responses to security alerts add further controls.^{5,6}

Three outcomes worth evaluating

Know what is connected. Compare observed devices with approved inventory, identify unknown equipment and assign an owner or an exception instead of relying on an old spreadsheet.

Control exposure. Limit untrusted or risky devices according to policy, and give guests or contractors access only to the resources their work requires.

Show the control working. Retain tested policy decisions and incident records alongside the credit union's approval and review process. Evidence is stronger when it demonstrates an outcome rather than only a product installation.

Security support within the wider program

Federally insured credit unions must maintain a written security program under 12 CFR 748.0. Appendix A provides guidelines for safeguarding member information under the Gramm-Leach-Bliley Act, or GLBA. EasyNAC can support selected technical controls; governance, risk decisions and the overall compliance determination remain with the credit union.²

This paper explains the network approach, illustrates credit union use cases, maps relevant control objectives and provides an evaluation plan. The examples are hypothetical and do not represent customer results.

02 / DEPLOYMENT APPROACH

Keep the network you already have

EasyNAC uses out-of-band Address Resolution Protocol, or ARP, enforcement on protected LAN and wireless segments. Trusted devices retain their existing traffic path. Traffic to and from restricted devices is redirected through the appliance, which forwards only what the assigned access-control policy permits. A hardware or virtual appliance provides policy and visibility; Enforcer Sensors extend local enforcement to branches.⁶



Illustrative relationships, not packet paths. Trusted devices retain their existing network path; restricted-device traffic is redirected for policy enforcement. Confirm Layer 2 reach during design.

Agentless means less endpoint deployment work

These use cases require no additional EasyNAC endpoint agent. Existing endpoint protection and management agents remain in place and can supply information through supported integrations. The security details available still vary by device and integration.

Use local reach with central policy

The appliance needs Layer 2 reach to protected segments through physical connections or a VLAN trunk. A branch Enforcer Sensor reports device information and applies assigned access policy locally. The team can reuse policy across locations while retaining justified branch exceptions.⁶

Confirm coverage before promising protection

Document protected subnets and device scope. Test wired and wireless access, integrations, appliance and sensor capacity, and failure behavior, including restricted-device traffic. EasyNAC is compatible with dual-stack IPv4/IPv6 endpoints. IPv4 is required for management and most key features; IPv6-only environments are not recommended.⁶

This approach can avoid switch replacement or a wholesale network redesign and can work alongside an existing 802.1X deployment. Connectivity, configuration, policy testing and change control are still required.

03 / BRANCH ACCESS SCENARIOS

Put branch access policy into practice

The following scenarios show how a credit union could apply EasyNAC. Each starts with a defined policy and a protected segment. They are evaluation examples, not claims that a particular credit union has achieved these results. Product functions are described in InfoExpress's EasyNAC materials.^{5,6}

01

An unknown device appears at a branch

A contractor plugs a laptop into an available network jack. EasyNAC discovers and profiles it, then applies the configured trust policy. An unapproved device can remain restricted while an administrator or sponsor verifies its owner and purpose. If approved, the contractor receives access to the required resources, with an expiration where appropriate.

Evaluate the outcome. Verify that the device is detected, that an approved service remains usable and that the contractor cannot reach resources outside the agreed scope. Record the approval and expiration.

02

A managed workstation fails a security check

A loan officer's workstation is known to the organization, but a supported security integration reports that it fails an agreed protection or patch condition. EasyNAC can use that information to apply a more restrictive access policy. Where configured and tested, the policy can preserve access to remediation resources while reducing exposure to sensitive systems.

Evaluate the outcome. Use a safe test endpoint to validate the failed check, restriction, permitted remediation path and return to approved access. The endpoint or patch platform performs the repair; EasyNAC controls network access.

Put branch access policy into practice

03

A trusted device begins suspicious activity

An endpoint attempts unusual peer connections or probes a configured decoy service. Alternatively, a third-party security tool sends an actionable event through a configured alert channel. EasyNAC can identify the source device and restrict its access according to policy, including local communication on protected segments. The response team then investigates and determines recovery steps.

Evaluate the outcome. Simulate the agreed behavior in an authorized test environment. Confirm the correct device is restricted and that approved neighboring devices keep working. Review legitimate scanning tools before enabling automatic responses.

04

A printer or other device cannot run a NAC agent

A branch printer, camera or other appliance is profiled and assigned an approved role. Ownership and expected behavior support the access decision. Fingerprinting can help identify changes inconsistent with the approved device, while policy limits access to necessary resources.

Evaluate the outcome. Confirm the normal service still works, test an unauthorized destination and review a device change. Discovery and fingerprinting do not replace vulnerability assessment or the vendor's maintenance process.

04 / COMPLIANCE ALIGNMENT

Link device controls to compliance

Appendix A guidelines address risk assessment, access controls, monitoring, response, testing and board reporting. FFIEC guidance also addresses device access. This table links selected objectives to proposed EasyNAC use and credit union responsibilities. It is an implementation aid, not a certification or complete compliance checklist.^{2,3}

As of October 9, 2026, Appendix A remains in the eCFR. NCUA has proposed relocating these guidelines to a Letter to Credit Unions; they are not independently enforceable. The security-program requirement in 12 CFR 748.0 remains binding.^{2,11}

Control objective	How EasyNAC can contribute	Evidence and credit union responsibility
Risk assessment Appendix A III.B	Device discovery and profiles help identify unknown equipment and access exposure on protected segments.	Reconcile observations with inventory and owners. Document coverage gaps, critical services and risk decisions.
Device access FFIEC Appendix	FFIEC guidance includes devices among users and describes device access controls. Trust policies and resource restrictions can support this layer.	Keep policy approvals and access-test results. Appendix A III.C.1.a concerns authorized individuals; retain identity and application controls.
Attack monitoring Appendix A III.C.1.f	Deception, suspicious local behavior and integrated alerts can identify devices requiring action.	Keep sample events and correlation records. Define triage ownership, tuning and handling of authorized scans.

04 / COMPLIANCE ALIGNMENT / CONTINUED

Link device controls to compliance

Control objective	How EasyNAC can contribute	Evidence and credit union responsibility
Incident response Appendix A III.C.1.g	Configured device restriction can support containment while responders investigate.	Maintain the response plan, action timeline and restoration approval. Management owns impact assessment and notification.
Control testing Appendix A III.C.3	Repeatable device and policy scenarios help demonstrate whether restrictions work as intended.	Record expected and actual results and exceptions. Arrange appropriate independent testing or review.
Board reporting Appendix A III.F	Device and access findings can inform a concise account of control coverage and unresolved exposure.	Combine findings with the wider program report. Management explains residual risk, decisions and next actions.

Keep the other security layers

FFIEC guidance describes layered access security and risk-based authentication, including multifactor authentication or controls of equivalent strength where appropriate. A device access decision is only one layer. EasyNAC should complement the credit union's identity controls, endpoint protection, firewalls, patching, encryption, backups and service-provider oversight.³

NAC does not establish that a transaction is authorized, prevent every phishing attack or validate a hosted core provider's security. Those risks need their own controls and evidence.

05 / OPERATING THE CONTROL

Make device control easier to manage

Less heavy lifting comes from repeatable device decisions. The team can reuse approved rules, review exceptions and act on relevant events instead of investigating every network appearance separately. People remain accountable for policy.

Reuse the information already available

Supported directory, endpoint security, patch and mobile device management integrations can supply existing trust and posture information. Agree which conditions affect access, how current the evidence must be and what happens when the source cannot be reached.

Make routine access predictable

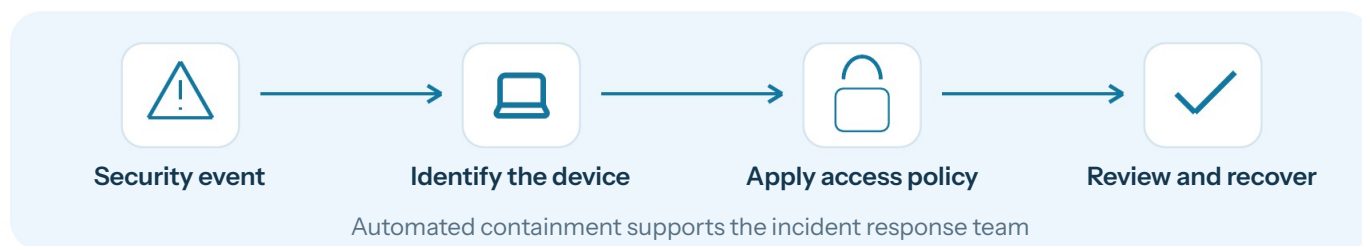
Start with employee, guest, contractor and defined appliance roles. Add detail where the risk requires it. Record exception owners, permissions and review dates. Domain membership or a recognizable MAC address should not override the required security conditions.

Manage branches consistently

Enforcer Sensors extend appliance policies to branches. Standardize the baseline and document justified differences. For multiple appliances, the optional Central Visibility Manager can consolidate administration and reporting. It is not required simply because one appliance manages several branch sensors.⁶

Automate the action that has been tested

Start with a defined alert and reliable source-device identification. Test parsing, restriction, permitted recovery resources and reversal. Review approved scanners and vendor diagnostics before enabling automatic responses. Ambiguous device identifiers need investigation rather than an uncontrolled blocking rule.



Protect service continuity

Review visibility and policy before broad enforcement. Validate teller, ATM and other critical or vendor-managed workflows with their owners. Test appliance or sensor interruption, integration outage, licensing capacity and rollback. Select redundancy and operating procedures for the service impact the credit union can tolerate.

Do not assume a fixed deployment duration or a guaranteed staff-hour saving. Measure the work avoided and the new operational tasks during the evaluation.

06 / EVALUATION PLAN

Start with a controlled evaluation

A focused evaluation should answer whether the credit union can improve device control without interrupting member service. Choose a representative headquarters segment and branch, with authorized test devices and named owners. Agree success criteria, stop conditions and a rollback path before enforcement.

01

Define scope and observe

Document segments, device classes, required resource paths and critical dependencies. Baseline approved and unknown devices, onboarding effort and manual response steps. Connect the appliance and branch sensor, then review discovery and classification before restrictive policy.

02

Build and validate policy

Configure supported integrations, trust conditions, guest sponsorship, contractor resources and exceptions. Test missing or stale data and compliant and noncompliant endpoints. Verify allowed and denied access on protected segments, including permitted remediation resources.

03

Enable limited enforcement

Begin with a small approved device group. Test unknown devices, failed security checks, expired access and an authorized threat simulation. Verify allowed and denied destinations and normal business workflows. Expand only when the agreed tests pass.

04

Review evidence and operating effort

Review results with IT, security, risk and the branch owner. Confirm alert routing, overrides, recovery approval and exception reviews. Check records, exports and retention. Document residual risks and the rollout decision, with unresolved coverage clearly identified.

06 / EVALUATION SCORECARD

Use a measurable acceptance scorecard

Measure	How to assess it
Device visibility	Reconcile known test devices with discovery results for each in-scope segment. Record unexplained gaps and unknown devices.
Access enforcement	Record expected and actual access for employee, guest, contractor and appliance scenarios. Include prohibited destinations.
Containment and recovery	Measure event receipt, device identification, restriction and authorized restoration using a controlled simulation.
Service continuity	Verify teller and other agreed business workflows. Record unexpected blocks, help-desk impact and failure tests.
Operating effort	Compare manual checks and response steps with the baseline. Include policy maintenance and exception handling.

07 / EVIDENCE AND REPORTING

Make the evidence useful when it matters

A useful record explains the relationship between a device, a rule and an outcome. Combine available EasyNAC device and event information with the credit union's approvals, security-tool records and incident tickets. That makes it possible to explain both what happened and why the response was appropriate.

Assemble a compact control evidence set

Coverage and ownership. Maintain the protected subnet list, branch and sensor relationships, approved device roles, named owners and documented exclusions.

Policy and exceptions. Record the approved trust conditions, guest and contractor permissions, exception rationale, expiration and review owner. Retain configuration revisions through the credit union's change process.

Test and action records. Keep expected and actual access results, the triggering event, device identification, applied action and recovery approval. Confirm which information the selected version records and how it is retained or exported.

Management review. Summarize unknown devices resolved, repeated failures, unintended restrictions, coverage gaps and corrective work. Store evidence under access and retention rules appropriate to its sensitivity.

Keep containment and notification connected

Under 12 CFR 748.1(c), federally insured credit unions must notify NCUA as soon as possible and no later than 72 hours after reasonably believing a reportable cyber incident occurred. For third-party incidents covered by the rule, the clock begins with the third-party notification or that reasonable belief, whichever occurs sooner. This applies to reportable substantial incidents, not every alert.⁷

An EasyNAC restriction can support containment and a device-level timeline; it does not decide reportability or file a notice. Name the escalation owner, capture notification times and preserve evidence alongside the incident assessment. NCUA Letter 25-CU-02 updates Letter 23-CU-07 and adds a secure online reporting form. Other reporting duties may also apply.⁷

Use current assessment resources

NIST CSF 2.0 organizes cybersecurity outcomes around Govern, Identify, Protect, Detect, Respond and Recover. Device inventory, access policy, monitoring and containment can contribute to selected outcomes; governance and recovery still require wider processes. This is a practical alignment, not a NIST certification.⁸

NCUA continues to offer ACET assessment resources. The FFIEC Cybersecurity Assessment Tool was sunset on August 31, 2025, so a new evaluation should use current resources rather than base its approach on that retired tool.^{9,10}

08 / NEXT STEPS

A practical next step

A focused NAC evaluation can test whether unknown devices are identified, risky access is restricted and the result can be explained, while approved member services keep working.

EasyNAC is worth evaluating when the priority is device-level control on existing LAN and wireless segments, consistent branch policy or a local response to security alerts. Its agentless approach can reduce endpoint deployment work and supported integrations can reuse information from the existing security stack.

Ask the questions that determine fit

Where is the gap? Identify the branch, segment or device group where current inventory or access control is weakest. Prioritize the member-service or information exposure it creates.

What should change? Write the access outcome for an unknown, noncompliant, guest or contractor device. Avoid a pilot that demonstrates only a dashboard.

What must keep working? List required resource paths, approved vendor activity and normal branch workflows. Make them part of acceptance testing.

What will prove value? Agree the security results, coverage, operational effort and evidence needed for the rollout decision.

Build on the security program you have

CISA's ransomware guidance emphasizes a combination of asset awareness, least privilege, segmentation, endpoint defenses and recovery preparation. EasyNAC contributes to device visibility and access containment; it should sit alongside those other investments. The goal is a clearer operational control with tested boundaries, not reliance on one product for every risk.⁴

Plan an EasyNAC evaluation with InfoExpress

Bring a network sketch, the proposed segments and branches, a list of device classes and the security platforms already in use. Include the critical workflows and access decisions you want to test. InfoExpress can help assess the deployment design, supported integrations, sizing and evaluation scope.

[Discuss a credit union evaluation](#)

sales@infoexpress.com

About InfoExpress

InfoExpress Inc. is a cybersecurity company focused on Network Access Control, headquartered in Santa Clara, California. EasyNAC combines network visibility, agentless security checks and access enforcement to help organizations control which devices use their networks.

This vendor-authored paper is educational and describes selected capabilities and implementation ideas. Product suitability and regulatory applicability depend on the credit union's environment. It does not establish compliance or imply endorsement by NCUA, FFIEC, NIST or CISA.

09 / SOURCES

Sources and further reading

Primary regulatory and security sources underpin the control discussion. Product descriptions draw on InfoExpress's EasyNAC materials. Sources were reviewed on October 9, 2026.

1 NCUA

[2026 Cybersecurity and Credit Union System Resilience Report](#)

June 2026

2 eCFR

[12 CFR 748.0 security program and Appendix A guidelines](#)

Rule and guidelines reviewed October 9, 2026

3 FFIEC

[Authentication and Access to Financial Institution Services and Systems](#)

August 2021

4 CISA, FBI, NSA and MS-ISAC

[#StopRansomware Guide](#)

October 2023 update, version 3.0

5 InfoExpress

[EasyNAC Solutions](#)

Product capabilities reviewed October 9, 2026

6 InfoExpress

[EasyNAC Products and FAQ](#)

Deployment information reviewed October 9, 2026

[EasyNAC FAQ: deployment and integration details](#)

7 eCFR and NCUA

[12 CFR 748.1\(c\) cyber incident notification requirements](#)

Rule and January 2025 guidance reviewed October 9, 2026

[Letter 25-CU-02: update and online reporting form](#)

8 NIST

[The NIST Cybersecurity Framework 2.0, CSWP 29](#)

February 26, 2024

9 NCUA

[ACET and Other Assessment Tools](#)

Current resources reviewed October 9, 2026

10 FFIEC

[CAT Sunset Statement](#)

August 2024; sunset effective August 31, 2025

11 NCUA

[Proposed relocation of Appendix A safeguarding guidelines](#)

Proposed December 11, 2025; status reviewed October 9, 2026