IMPLEMENTATION AND RESULTS REPORT

Northwest Health Center

Erick M. Linares-Pacheco

Western Governors University

D490 Cybersecurity Graduate Capstone

November 2026

Executive Summary

Northwest Health Center's cybersecurity project addressed a specific operational gap: employees could use internal systems while on-site, but the organization did not have an established, controlled method for reaching selected internal applications and file shares from external networks. The original environment was a flat, wired 10.0.10.0/24 network with on-premises Active Directory, a Windows Server domain controller and file server, and a Linux application host running Coolify. Microsoft 365 was used primarily for email and productivity. Remote access to internal resources was not part of the established environment.

The project implemented Microsoft Entra Private Access through Global Secure Access to provide identity-aware remote connectivity to selected internal resources. The implementation combined synchronized on-premises and cloud identities, hybrid Microsoft Entra join, a Private Access connector installed on NORTHWEST-DC, Global Secure Access client software on endpoint machines, Microsoft Authenticator multifactor authentication (MFA), Conditional Access, Intune device enrollment and compliance, and role-based application and file-share assignments.

The architecture is intentionally layered. The Global Secure Access client captures traffic for configured private resources and forwards it through Microsoft's service. The Private Access connector, installed inside the organization, provides the connection to internal applications and file shares. Entra ID evaluates identity and applicable access conditions. Role-group assignments limit which private applications a user may reach, while the applications and Windows file shares continue to enforce their own authorization. The internal applications retain their native username-and-password sign-in; this project did not convert them to Entra single sign-on.

Six acceptance tests (TC-01 through TC-06) were completed. Each test produced the expected allow or block outcome for its defined scenario. The evidence set includes configuration records, device-compliance information, sign-in-log exports, identity and permission exports, and test screenshots. The Conditional Access screenshots for MFA and compliant-device requirements

display report-only mode at the time of capture; the policies were enabled for the acceptance tests. Security defaults remained disabled at project completion, with the custom Conditional Access policy providing the relevant MFA enforcement. The evidence register distinguishes these point-in-time screenshots from the final tested configuration.

The result is a focused remote-access improvement, not a complete Zero Trust transformation or network redesign. The original flat LAN remains. VLAN segmentation, network access control, a full Conditional Access policy review, production licensing validation, application authentication improvements, connector resilience, and expanded monitoring remain future work. The project demonstrates a practical transition from location-based access assumptions toward identity-, device-, and role-aware access to selected resources.

1. Introduction and Project Scope

1.1 Project purpose

The purpose of this project was to enable secure remote access to selected Northwest Health Center resources without exposing the entire internal network to remote users. The chosen approach was Microsoft Entra Private Access / Global Secure Access, which supports Zero Trust Network Access (ZTNA) by allowing administrators to define private resources and assign access to specific users or groups. Microsoft describes Private Access as a way to provide access to private resources without requiring a traditional VPN and to apply Microsoft Entra access controls to those resources (Microsoft, 2026a).

1.2 Scope boundaries

The project scope was deliberately limited to remote-access enablement and the identity, endpoint, and authorization controls needed to support it. It included hybrid identity synchronization, hybrid join, MFA, Conditional Access, Intune enrollment and compliance, Private Access connector and client deployment, private application assignments, role-based access, and validation testing. It did not include redesigning the internal network, replacing OPNsense, implementing VLANs, deploying NAC, replacing the internal applications, or converting every application to Entra SSO.

The project is evaluated in three stages: (1) the pre-project baseline, (2) the implemented architecture and operating controls, and (3) the observed test outcomes and remaining work. This separation prevents proposed improvements from being described as completed capabilities.

1.3 Evaluation approach

The evaluation draws on the project evidence archive and documented implementation details. Evidence is identified by filename and identifier. Screenshots are interpreted as records of the configuration visible at the time of capture; report-only screenshots are not treated as proof of enforcement. The acceptance-test results are presented separately from configuration snapshots.

2. Pre-Implementation Environment and Security Gaps

Before implementation, the workforce operated from the organization's on-site wired environment. Internal resources were hosted on a single flat subnet. The network documentation identifies OPNsense as the gateway, NORTHWEST-DC as the Windows Server domain controller and file server, and NORTHWEST-SS as the Coolify application host. The domain was northwest.local. The address plan assigned 10.0.10.1 to OPNsense, 10.0.10.10 to NORTHWEST-DC, 10.0.10.20 to NORTHWEST-SS, and DHCP client addresses in the 10.0.10.100–200 range.

Component	Baseline configuration
Internal network	10.0.10.0/24; flat network; no VLAN segmentation
Gateway	OPNsense at 10.0.10.1
Domain controller	NORTHWEST-DC at 10.0.10.10; AD DS, DNS, DHCP, and file services
Active Directory	northwest.local; Northwest OU with departmental user, computer, and group OUs
Application host	NORTHWEST-SS at 10.0.10.20; Linux host running Coolify
Applications	Docmost, OpenEMR, Zammad, OrangeHRM, Invoice Ninja
Cloud tenant	northwesthealthlab.onmicrosoft.com
Test endpoint	NORTHWEST-L-LAB

The Active Directory design already contained departmental role groups for Billing, Scheduling, Clinical, and Admin. File shares were organized around the same business functions: ClinicFiles\Billing, ClinicFiles\Scheduling, ClinicFiles\Clinical, and ClinicFiles\Admin. The supplied role-membership export shows test accounts in these departmental groups and Erick Pacheco and Alex Rivera in IT-Admins. The access matrix documents business-facing staff and their intended application access. These artifacts establish that role-based resource boundaries existed in the lab; the project extended the use of role groups to remote application access rather than inventing departmental roles from scratch.

The main security gap was not the absence of an internal network or identity system. It was the absence of a supported remote-access path that could evaluate the user, endpoint, and requested resource before allowing connectivity. Simply extending internal network reachability would risk treating possession of a valid credential or a network connection as sufficient trust. That approach would be particularly weak if a credential were compromised or a device were unmanaged.

A second limitation was the flat network. Internal servers and workstations shared the same subnet, and the documentation records no VLANs. The Nmap discovery and service scans provide

a baseline view of visible hosts and exposed services; they are not a vulnerability assessment. The discovery scan identified the gateway, application host, domain controller, and several client addresses. The service scan showed, among other observations, DNS, SMB, and RDP services on the domain controller and SSH and web-facing services on the application host. These observations support the need for continued network hardening, but the project did not attempt to remediate the flat topology.

The pre-project state can therefore be summarized as an operational on-premises environment with established AD identities, departmental permissions, and internal applications, but without a controlled, identity-aware way for external users to reach selected internal resources.

3. Implemented Solution and Technical Architecture

3.1 Hybrid identity foundation

The project connected the on-premises northwest.local identity environment to the Microsoft Entra tenant northwesthealthlab.onmicrosoft.com. The environment documentation records Entra Connect synchronization with Password Hash Synchronization and a Cloud Sync agent on NORTHWEST-DC. The documentation identifies Classic Entra Connect as the primary working synchronization path and Cloud Sync as also enabled and healthy. The Entra Connect status screenshot (EV-06-Entra-Connect-Status.png) provides a point-in-time view of synchronization health; the Entra overview and user screenshots (EV-04-Entra-Overview.png and EV-05-Entra-Users.png) provide supporting tenant and identity context.

Hybrid join was configured and tested so that the endpoint could be represented in the hybrid identity environment. This provided the identity and device context needed for access evaluation. The implementation retained Active Directory as the on-premises directory; Entra ID supplemented rather than replaced the domain.

3.2 Microsoft Entra Private Access / Global Secure Access

The project deployed Microsoft Entra Private Access as the remote connectivity layer. The Private Access connector was installed on NORTHWEST-DC, which already had access to the internal network and hosted AD DS, DNS, DHCP, and file services. The Global Secure Access client was installed on the endpoint machines used for testing. This created both sides of the Private Access path: the client on the user's device and the connector inside the private network.

The access flow is as follows:

1. The user signs in to the endpoint and launches or uses the Global Secure Access client.
2. The client identifies traffic matching the configured Private Access resources and forwards that traffic to the Global Secure Access service.
3. Microsoft Entra evaluates the user's identity, application assignment, and applicable Conditional Access requirements.
4. If access is authorized, the service brokers the connection through the Private Access connector installed on NORTHWEST-DC.
5. The connector reaches the selected internal application or file-share destination over the existing internal network.

6. The target application or file server applies its own authentication and authorization rules.

This design is materially different from granting a remote user unrestricted network-level access. Microsoft's documentation explains that the Global Secure Access client forwards traffic for configured private applications and that the service brokers the connection through Private Network Connectors. Enabling traffic forwarding alone does not grant access to every private resource; the destination must be configured and the user or group must be assigned (Microsoft, 2026a; Microsoft, 2026b).

The project's internal applications remained on NORTHWEST-SS at 10.0.10.20, hosted through Coolify. The documented applications are Docmost, OpenEMR, Zammad, OrangeHRM, and Invoice Ninja. The application-service document contains an older OrangeCRM label in its table, but the dedicated service documentation identifies the product as OrangeHRM. This report uses OrangeHRM.

3.3 MFA and Conditional Access

The project created a Conditional Access policy named "Require MFA for all users" and used Microsoft Authenticator for the MFA workflow. The policy provides an additional authentication factor beyond a password for access to protected resources. The custom Conditional Access configuration provides the relevant MFA enforcement after security defaults were disabled.

The screenshot EV-09-CA-Require-MFA.png displays the policy details in report-only mode at the time of capture. It documents the policy configuration and its grant requirement ("Require multifactor authentication"), but does not independently establish the policy's final enforcement state. The policy was enabled for acceptance testing. The MFA test artifacts, including EV-TC03-MFA-Setup-Prompt.png and EV-TC03-MFA-Not-Setup-Blocked.png, document the MFA workflow and denied-access scenario.

The distinction between policy configuration and enforcement is important. Conditional Access evaluates access conditions and applies grant or block controls; it does not create the network path. Private Access supplies the path, while Conditional Access contributes the access decision. Microsoft describes Conditional Access as an access policy engine that evaluates signals and applies access controls (Microsoft, 2026c).

3.4 Security defaults: implementation decision and final state

Security defaults were disabled during the project so the environment could use its custom Conditional Access configuration. They remained disabled at project completion, with the custom Conditional Access policy providing the relevant MFA enforcement.

The evidence archive contains a chronology discrepancy. EV-10-Security-Defaults-Note.txt states that security defaults were re-enabled after sign-in-log collection, and EV-10-Security-Defaults-Reenabled.png shows the tenant in an enabled state. These artifacts document the state visible at capture and do not represent the final configuration. Security defaults were disabled at project completion. The final configuration is described here separately from the earlier evidence snapshots.

The security decision also creates a follow-up obligation. Disabling security defaults is appropriate only when the replacement controls are intentionally configured, tested, monitored,

and maintained. The project implemented a custom MFA policy, but the complete Conditional Access policy set was not the project's scope. A future review must assess all policies, exclusions, emergency-access accounts, authentication methods, licensing dependencies, and policy interactions. The project should not claim that the custom MFA policy reproduces every protection included in security defaults.

3.5 Intune enrollment and device compliance

Intune enrollment was enabled and the Windows endpoint NORTHWEST-L-LAB was enrolled. The screenshot EV-13-Intune-Device-Compliant-NORTHWEST-L-LAB.png shows the device as compliant. The compliance policy is named "Basic Windows Compliance - Lab" and the supplied policy screenshot (EV-14-Compliance-Policy.png) shows settings associated with encryption, BitLocker, Secure Boot, and password requirements. The remediation screenshot (EV-14-Intune-Compliance-Remediation-BitLocker-Prompt.png) provides an example of a device remediation prompt.

Intune compliance and Conditional Access perform separate functions. Intune evaluates whether a managed endpoint meets defined device requirements and reports its compliance state. Conditional Access can then use that state as a grant condition. Microsoft documents this two-stage relationship: compliance policies evaluate device state, and Conditional Access can require the device to be marked compliant before access is granted (Microsoft, 2026d).

The screenshot EV-09-CA-Require-Compliant-Device-ReportOnly.png explicitly shows the Conditional Access policy state as "Report-only (policy is evaluated but not enforced)." It documents a report-only configuration snapshot and does not independently establish enforcement. The compliant-device policy was enabled for acceptance testing, and the device-based test scenarios were executed with enforcement enabled.

3.6 Role-based access and application authentication

The project used the departmental groups Role-Billing, Role-Scheduling, Role-Clinical, Role-Admin, and IT-Admins to control access to the appropriate private resources. These groups were assigned to Private Access applications. The AD group export provides membership evidence for the lab identities, including billing1 and billing2 in Role-Billing, sched1 in Role-Scheduling, clinical1 in Role-Clinical, admin1 in Role-Admin, and Erick Pacheco and Alex Rivera in IT-Admins. The share-permission exports provide a corresponding resource-permission view.

The access matrix describes the intended business access: Billing staff use Invoice Ninja and the Billing share; Scheduling uses OpenEMR and the Scheduling share; Clinical Support uses OpenEMR and the Clinical share; Administrative staff use OpenEMR and administrative tools; IT staff have elevated administrative responsibilities appropriate to their duties. The AD export uses some lab account names while the access matrix uses staff names. The report does not assume that every lab SAM account is identical to a human-facing identity unless the mapping is established in the environment documentation.

ZTNA does not eliminate the applications' own authentication. Users still sign in to Docmost, OpenEMR, Zammad, OrangeHRM, and Invoice Ninja using each application's native username and password. Private Access adds a separate access-control layer before a remote user can reach

the application. File shares continue to depend on Windows share and NTFS permissions. Consequently, successful Private Access authorization is necessary for remote reachability but is not sufficient to establish application-level authorization.

3.7 Implementation summary

Control / component	Implemented state	Purpose in the design
Entra Connect / hybrid identity	Synchronization configured; status screenshot supplied; hybrid join configured and tested	Provides cloud identity and device context linked to on-premises AD
Private Access connector	Installed on NORTHWEST-DC	Provides service-to-private-network connectivity
Global Secure Access client	Installed on test endpoint machines	Captures and forwards traffic for configured private resources
MFA / Conditional Access	Custom MFA policy created; enabled for acceptance testing	Adds a second authentication factor to protected access
Intune	Enrollment enabled; NORTHWEST-L-LAB enrolled and compliant	Evaluates endpoint security posture
Device-based Conditional Access	Report-only screenshot captured; enabled for acceptance testing	Uses device compliance in access decisions
Role-based access	Departmental groups assigned to Private Access resources and file permissions	Limits resource reachability and preserves least privilege
Native app authentication	Retained	Maintains each application's own account and permission model

4. Policies Adopted and Cybersecurity Decision-Making (A and A1)

The implementation established practical access rules for the remote-access environment. These are the operating requirements embodied in the technical configuration; this report does not imply that a separate executive-approved policy document was signed.

- Identity rule: users must authenticate with an organizational identity synchronized to or provisioned in the Entra tenant.
- MFA rule: access covered by the custom Conditional Access policy requires multifactor authentication using the configured authentication method.

- Remote-access rule: external users must use the approved Global Secure Access client and may reach only the private resources configured and assigned to them.
- Device rule: applicable access scenarios require the endpoint to meet the Intune compliance conditions and satisfy the enforced device-based access policy.
- Least-privilege rule: users receive access through the role groups associated with their job responsibilities; membership in one group does not imply access to all departments' resources.
- Resource authorization rule: application-native credentials, application roles, Windows share permissions, and NTFS ACLs remain in effect.
- Change-control rule: policy changes must distinguish report-only evaluation from enforcement and must be validated with both allowed and denied access tests.

The solution improves cybersecurity decision-making by replacing a broad "inside versus outside" assumption with multiple decision inputs. Administrators can consider the identity attempting access, whether MFA was completed, whether the endpoint is managed and compliant, whether the user is assigned to the requested private application, and whether the target resource accepts the user's native credentials and permissions. This separation is important because a user can be authenticated but still lack authorization to a particular application or file share.

The test evidence illustrates this distinction. TC-04 shows a Private Access application denial for Priya Patel because the account was not directly assigned or a member of a group assigned to Docmost. The message explicitly identifies the assignment requirement. TC-06 shows a successful network-drive access scenario and role membership evidence. These examples demonstrate that role membership is not merely an administrative label; it affects which private resources are reachable.

5. Cybersecurity Assurance, Automation, and Modernization (B)

5.1 Automation and repeatability

The project uses platform-managed services to make identity and device information available to access decisions. Entra Connect synchronizes directory identities, Intune evaluates device compliance, and Conditional Access evaluates sign-in conditions. Private Access application assignments use security groups so that administrators can grant or remove access through membership and assignment changes rather than configuring each remote session individually.

These capabilities improve consistency and reduce reliance on ad hoc decisions. The project did not measure time saved, support-ticket reduction, or changes in incident frequency, so no quantitative efficiency claim is made. The operational benefit is the creation of a repeatable process: identity and device state are evaluated by centralized services, while role groups provide a structured authorization mechanism.

5.2 Modernization

The modernization was targeted. The organization retained its on-premises domain, file server, OPNsense gateway, Coolify host, and applications, but added a cloud-mediated identity-aware access layer. This allowed remote access to be introduced without redesigning the LAN or

replacing the applications. It is a practical hybrid approach: existing resources remain in place while cloud identity and access services provide an additional control plane.

5.3 Assurance limits

The solution's assurance is limited by the scope of the lab. One connector is installed on the domain controller, and the supplied environment documentation does not establish connector redundancy or a tested failover path. The internal network remains flat. The lab uses trial licensing with expiry/renewal dates documented as November 27 and November 28, 2026; production licensing must be validated before operational deployment. The project demonstrates working access scenarios, but it does not establish high availability, production-scale capacity, or comprehensive security coverage.

6. Data Collection, Digital Evidence, and CIA (C)

6.1 Evidence collected

The evidence archive contains several complementary evidence types:

- Identity and directory exports: domain.txt, forest.txt, users.csv, groups.csv, ous.csv, gpos.csv, and role-memberships.txt.
- File-service evidence: shares.csv, share-permissions.txt, and ClinicFiles-full-acl.txt.
- Network evidence: nmap-discovery.txt and nmap-services.txt.
- Cloud configuration evidence: Entra tenant, users, synchronization, MFA, Conditional Access, licensing, device enrollment, and compliance screenshots.
- Authentication and activity evidence: EV-10-Sign-in-Logs.csv, containing ten exported sign-in records.
- Test evidence: screenshots for successful external access, device restrictions, MFA workflow, role-based denials, and permitted file-share access.
- Environment documentation: the nested Docmost export, including network addressing, firewall, Active Directory, Entra synchronization, access matrix, licensing, Coolify services, and OrangeHRM documentation.

The sign-in CSV includes fields for event time, user display name, UPN, application, IP address, client app, status, Conditional Access status, and device details. The first entries show Microsoft Graph Command Line Tools activity for the Information Technology account on November 5, 2026, with Conditional Access status recorded as notApplied. This is useful context for the collection activity but should not be confused with evidence that the MFA policy was evaluated for an unrelated application session.

The Nmap discovery file records a scan of 10.0.10.0/24 on November 4, 2026. The service scan records three hosts up, including the gateway, application host, and domain controller. It identifies exposed services such as DNS, SMB, and RDP on the domain controller and SSH and web-related services on the application host. Nmap service identification is useful for asset and service inventory; it is not proof that a host is vulnerable or that a vulnerability assessment was completed.

6.2 Digital evidence handling

The evidence set is useful because it connects multiple parts of an access decision: the user and group, the endpoint's enrollment and compliance state, the Conditional Access configuration, the requested private resource, and the observed allow or block result. For a formal forensic process, evidence should be preserved in original form, with collection time and time zone, source system, collector, query or export method, and cryptographic hash recorded. Presentation copies should be redacted where they expose personal or sensitive information. The supplied archive contains the original screenshots and exports, but does not include a documented hash manifest or full chain-of-custody record.

6.3 Confidentiality, integrity, and availability

Confidentiality is supported by MFA, device-based conditions, Private Access assignments, role groups, and resource permissions. The denied Docmost test demonstrates that a user without the required application assignment is blocked. The device restriction evidence shows a remote access attempt blocked because the device or client did not meet the organization's compliance requirement. These controls reduce unnecessary exposure, but do not prove that every application account, local administrative path, or file permission is correctly configured.

Integrity is supported indirectly by limiting who can reach and modify systems and by retaining audit and configuration evidence. The Intune policy includes platform-security and encryption requirements, while Windows file-share ACLs and application roles restrict who can modify resources. The project did not conduct a comprehensive integrity assessment of application data or validate all backup and recovery processes.

Availability is supported by successful authorized-access tests, including an external-network scenario. However, the single connector placement on NORTHWEST-DC creates a dependency that should be evaluated. No connector failover, disaster recovery, or application recovery test is documented. A future production design should assess connector redundancy, server maintenance impact, application dependencies, and recovery objectives.

7. Incident Investigation and Mitigation (D)

No actual security incident is documented in the supplied project evidence. The project's contribution to incident response is the additional identity, device, policy, and access context that can be used when investigating a suspected unauthorized access attempt. The following procedure is an operational recommendation, not a description of an incident that occurred.

7. Triage and preserve: record the affected account, device, resource, source network, event time, user-reported symptoms, and any correlation or request identifiers. Preserve the relevant Entra sign-in record, Conditional Access result, Intune device state, and application or Windows logs.
8. Establish the access path: determine whether the Global Secure Access client was connected, whether the Private Access profile applied, whether the target application was configured, and whether the connector was available.
9. Evaluate identity and policy: review the user's authentication and MFA result, the policy mode and scope at the time, exclusions, device compliance status, and group assignments.

10. Evaluate resource authorization: review application-native account status and role, Windows share permissions, NTFS ACLs, and the user's current AD/Entra group membership.
11. Contain: if compromise is suspected, use approved administrative procedures to disable or secure the identity, revoke sessions where supported, remove inappropriate application assignments, and isolate a suspected endpoint when justified.
12. Remediate and recover: reset credentials or re-register MFA as appropriate, remediate device noncompliance, correct group and resource permissions, validate legitimate access, and document the final state.
13. Review and improve: preserve the incident timeline, identify whether the control failed or was misconfigured, and update policies, procedures, monitoring, and test cases.

The project does not establish a SIEM deployment, continuous alerting program, formal log-retention schedule, or exercised incident-response playbook. These are recommended next steps. The sign-in export is a useful starting point, but its existence alone does not establish ongoing monitoring.

8. Plans, Standards, Procedures, and Compliance Alignment (E and E1)

8.1 Operational plans and procedures

The implementation requires documented lifecycle procedures so that access remains aligned with job responsibilities.

Joiner, mover, and leaver process

- Joiner: confirm the approved identity; verify AD-to-Entra synchronization; place the user in the correct department and role groups; assign the appropriate Private Access applications; register MFA; provision native application accounts and file permissions; and validate access.
- Mover: remove obsolete role-group membership and application assignments before granting new access; review old file permissions and native application roles; test both newly granted and removed access.
- Leaver: disable the organizational identity through the approved identity process; review sessions, Private Access assignments, group memberships, endpoint association, native application accounts, and file permissions; retain records according to policy.

Endpoint and remote-access onboarding

For an approved endpoint, IT should verify device identity and hybrid-join state, enroll the endpoint in Intune, install the Global Secure Access client, confirm the Private Access profile is received, and review the Basic Windows Compliance - Lab evaluation. The endpoint should meet applicable encryption, BitLocker, Secure Boot, and password requirements. IT should then verify the applicable Conditional Access policy mode and test access to an authorized resource from an external network. A denied scenario should also be tested to confirm that an unauthorized user or noncompliant endpoint cannot reach the resource.

Helpdesk workflow

When a user reports that an internal application is unavailable remotely, the helpdesk should capture the username, device, destination resource, time, network context, client status, and error message. Troubleshooting should proceed through client connectivity, identity sign-in, MFA, device enrollment/compliance, Conditional Access evaluation, Private Access application assignment, and resource-level permissions. Users should not be instructed to bypass MFA or device requirements to restore access. An unexpected MFA prompt should be treated as suspicious and escalated.

8.2 NIST CSF 2.0 alignment

NIST Cybersecurity Framework 2.0 provides a risk-management taxonomy organized around Govern, Identify, Protect, Detect, Respond, and Recover (Pascoe et al., 2024). The project supports selected outcomes within these functions:

CSF 2.0 function	Project contribution	Remaining work
Govern	Defines the scope and operating rules for controlled remote access and role assignment.	Formal policy approval, risk ownership, and periodic governance review.
Identify	Uses AD, Entra, Intune, network, application, and permission inventories.	Maintain a complete asset and data inventory; identify data owners and criticality.
Protect	Implements MFA, Conditional Access, device compliance, Private Access, and role-based authorization.	Review all policies, segment the LAN, harden apps, and validate production licensing.
Detect	Provides sign-in and device-compliance information for review.	Implement alerting, retention, centralized monitoring, and review ownership.
Respond	Provides evidence sources and a proposed investigation/containment workflow.	Approve and exercise an incident-response procedure.
Recover	Identifies the need to restore access after policy or connector failures.	Test connector resilience, backup/restore, and controlled rollback.

This is an alignment assessment, not a certification or assertion that every NIST CSF outcome has been achieved. The project makes the strongest contribution to Protect and selected Identify and Detect outcomes. Respond and Recover are primarily addressed through recommended procedures and future validation.

8.3 HIPAA Security Rule alignment

Because Northwest Health Center is a healthcare-oriented environment, the design should be evaluated against relevant HIPAA Security Rule safeguards. The HHS summary identifies technical safeguard areas including access control, audit controls, integrity, person or entity authentication, and transmission security (HHS, n.d.). The implemented MFA and role-based access model support authentication and access-control objectives. The Private Access path supports controlled access to internal resources over an external network. Intune compliance and resource permissions add further access conditions.

The implementation does not establish HIPAA compliance. A compliance determination would require a broader assessment of administrative, physical, and technical safeguards; risk analysis; workforce training; emergency access; audit review; data integrity; transmission protections; business associate obligations; incident procedures; and evidence of ongoing operation. The project is a technical improvement aligned with selected safeguard objectives, not a certification or complete Security Rule assessment.

9. Applications, Tools, Installation, and User Guidance (E2)

The environment uses Microsoft Entra ID, Entra Connect, Microsoft Entra Private Access / Global Secure Access, the Global Secure Access client, Microsoft Authenticator, Conditional Access, Intune, Windows Server Active Directory, OPNsense, Coolify, and the internal applications. The supplied environment documentation records the application host and service endpoints: Coolify on port 8000, Docmost on 3000, OpenEMR on 3001, Zammad on 3002, OrangeHRM on 3003, and Invoice Ninja on 3004.

The Private Access deployment requires a registered connector on a Windows Server that can reach the private resources and the Global Secure Access service. Microsoft documents the connector as an agent that establishes outbound connectivity from the private network and recommends additional connector servers when high availability is required (Microsoft, 2026e). In this lab, the connector was installed on NORTHWEST-DC. This is functional for the project but creates a dependency on the domain controller and is not a high-availability design.

The user workflow is: connect to the approved endpoint; sign in with the organizational account; complete Microsoft Authenticator MFA when prompted; confirm the Global Secure Access client is connected; open the assigned internal application or file share; and sign in using that application's native credentials where required. If access fails, the user should report the exact resource, timestamp, device, and error to IT rather than repeatedly retrying or bypassing security controls.

The supplied Docmost environment export contains the network, identity, service, licensing, and access-matrix documentation. Those documents should be retained as operational references. The JML (usejml.com).md entry contains a URL, but the supplied content does not establish that a joiner/mover/leaver automation platform was implemented; no such capability is claimed.

10. Post-Implementation Environment and Architecture (F)

After implementation, the core on-premises topology remained intact. OPNsense remained at 10.0.10.1, NORTHWEST-DC remained at 10.0.10.10, NORTHWEST-SS remained at 10.0.10.20, and the LAN remained 10.0.10.0/24 without VLANs. The principal architectural change was the addition of the Entra Private Access control and connectivity path. The connector was installed on NORTHWEST-DC, and Global Secure Access clients were installed on endpoint machines.

Figures 1 and 2 show the network before and after implementation. The post-implementation diagram distinguishes identity and policy evaluation from the private traffic path: Conditional Access evaluates access conditions, the Global Secure Access service brokers configured private traffic, the connector reaches the private network, and each target application or file server applies its own authorization.

10.1 Security posture and efficiency (F1)

The implemented design improves the security posture for remote access by requiring a defined path and evaluating more than the user's password. It introduces identity synchronization, MFA, device compliance, role-based application assignments, and resource-level permissions. It also allows selected internal resources to be reached without making the entire LAN remotely accessible. The successful external-access test demonstrates that the path worked for an authorized user in the lab.

The implementation adds operational dependencies. IT must maintain the connector and endpoint client, resolve MFA registration issues, remediate noncompliant devices, maintain group assignments, and support native application accounts. The project did not measure the time required for these activities or compare helpdesk workload before and after deployment. The expected efficiency gain is therefore procedural consistency rather than a quantified reduction in labor.

10.2 New data and business-process impact (F2)

The solution introduces or makes more operationally important several data points: synchronized cloud identity, hybrid-join state, Intune enrollment and compliance status, MFA registration and sign-in outcome, Conditional Access evaluation, Private Access application assignment, and role-group membership. These signals help administrators determine why an access request was granted or denied. The business process changes because remote users must use the approved client, satisfy authentication and device conditions, and hold the required role before reaching the resource. They then continue to authenticate to the application itself.

For staff, the primary benefit is the ability to access approved internal resources from outside the office without broad network exposure. The trade-off is initial setup and possible remediation when a device is not compliant or MFA is not configured. The access matrix provides a basis for mapping business responsibilities to application and file-share access. The project did not include formal user interviews or a measured user-satisfaction survey.

11. Test Results and Summative Evaluation (F3)

All six acceptance tests passed their expected outcomes. The test set covers authorized access, device compliance, MFA completion, role assignment, unmanaged-device restrictions, and successful resource access with the correct permissions.

Test	Precondition / scenario	Expected result	Reported actual result	Evidence
TC-01	Compliant endpoint; MFA satisfied; authorized role; external network	Allow access	PASS — authorized external access succeeded	EV-TC01-Allow-Priya-Success.png; EV-TC01-Priya-External-Network-Success.png
TC-02	Noncompliant device	Block access	PASS — access blocked	EV-TC02-TC05-Unmanaged-Device-Blocked.png
TC-03	MFA not satisfied / not completed	Block access	PASS — access path denied until authentication requirements were met	EV-TC03-MFA-Setup-Prompt.png; EV-TC03-MFA-Not-Setup-Blocked.png; EV-TC03-Work-Account-Sign-in-Prompt.png
TC-04	User is not assigned to the requested application / role	Block access	PASS — Docmost denied access; file-share denial also recorded	EV-TC04-Role-Blocked-Docmost.png; EV-TC04-Network-Drive-Blocked.png
TC-05	Unmanaged endpoint	Block access	PASS — access blocked by device/compliance requirement	EV-TC02-TC05-Unmanaged-Device-Blocked.png
TC-06	Compliant endpoint; MFA satisfied; authorized role	Allow access with correct permissions	PASS — network-drive access allowed	EV-TC06-Network-Drive-Allow.png; EV-TC06-Priya-Role-

				Membership.png

11.1 Interpretation of test outcomes

TC-01 is the positive control for the remote-access path. The Global Secure Access client screenshot shows the connection state, and the external-network screenshot shows successful reachability to the internal application sign-in page. This demonstrates that the project did not merely configure policies that block everyone; an authorized user could reach an assigned resource from outside the internal network.

TC-02 and TC-05 are negative device-state tests. The shared screenshot displays a Microsoft access message stating that the application contains sensitive information and can only be accessed from devices or client applications that meet the Northwest Health Center management compliance policy. It therefore supports the device-based block. Because one screenshot is referenced for both cases, the evidence package should preserve the distinct test setup for the noncompliant and unmanaged conditions if separate records exist.

TC-03 tests the MFA requirement. The evidence set includes an MFA setup prompt, a Global Secure Access client status showing the Private channel disconnected, and a work-account sign-in prompt. The test outcome was denial when MFA was not satisfied. The artifacts document the authentication sequence; the setup prompt alone does not establish the denial.

TC-04 provides a particularly clear authorization result. The Docmost error explicitly states that Priya Patel was blocked because the user was not a direct member of a group with access and had not been directly assigned by an administrator. This is direct evidence that the Private Access application assignment was evaluated. The separate network-drive denial supports the role-based file-share boundary.

TC-06 is the positive authorization test for the file share. The evidence includes the successful network-drive access and a screenshot of Priya's group membership. Together, these show that a user with the appropriate role could reach the authorized resource. Application-native authentication and file permissions remain additional checks.

11.2 Evaluation against project objective

The objective was to enable secure remote access to selected internal resources. The successful external access scenario demonstrates that the connectivity objective was achieved in the lab. The negative tests demonstrate that access was not granted solely because a user could authenticate: MFA, device state, and role assignment affected the outcome. The final test demonstrates that an authorized user could reach the relevant file resource.

The project met its stated lab acceptance scenarios. It did not prove that all possible application paths, ports, devices, user types, policy combinations, or production conditions were tested. Broader testing should include every published application, multiple device states, policy exclusions, privileged accounts, session revocation, connector failure, and recovery. The current results are meaningful evidence of a functioning implementation, but not a substitute for production readiness testing.

12. Stakeholder Needs and Outcomes (F5)

The environment access matrix identifies executive, IT, billing, scheduling, clinical, and administrative stakeholders. The table below relates those documented responsibilities to the implemented access model. It does not claim that stakeholder interviews or satisfaction surveys were conducted.

Stakeholder / role	Documented need	How the implementation addresses it
Jennifer Walsh — CEO	Email and productivity access without routine administrative privileges.	The project preserves the M365 role and does not grant executive administrative rights. Remote access to internal resources is restricted by application assignment.
Erick Pacheco — IT Administrator	Administrative control across identity, applications, and file services.	IT-Admins and administrative assignments support operational access; centralized identity and policy controls provide common administration. Privileged access review remains important.
Alex Rivera — IT Helpdesk	Support and user administration without unrestricted system administration.	User Administrator and helpdesk duties are documented; the layered troubleshooting process helps separate client, identity, device, policy, and resource-permission failures.
Maria Gonzalez and James Carter — Billing	Invoice Ninja and Billing share access.	Role-Billing and resource permissions provide a basis for limiting billing access to the required resources.
Priya Patel — Scheduling	OpenEMR scheduling access and Scheduling share.	Role-Scheduling and application assignments support the intended access; TC-01 and TC-06 include Priya-related evidence.
David Nguyen — Administrative	OpenEMR and general administrative tools; Admin	Role-Admin and resource-specific assignments support

	share.	the documented administrative workflow.
Sarah Mitchell — Clinical Support	OpenEMR and Clinical share access.	Role-Clinical and file-share permissions provide a departmental access boundary.

The implementation supports stakeholder needs by enabling remote reachability to selected resources while retaining the existing business application permissions. It does not eliminate the need for access reviews. Role groups must remain aligned with current job responsibilities, and native application accounts must be maintained separately.

13. Remaining Risks and Future Work (F4)

The project deliberately left several security improvements outside its scope. The following qualitative ratings are planning judgments based on the current architecture, not measured probabilities. Likelihood and impact should be reassessed after the organization performs a formal risk analysis.

Risk / gap	Likelihood	Impact	Recommended mitigation
Flat network with no VLAN segmentation	High	High	Design VLANs and network access controls to reduce lateral movement; define inter-VLAN rules and validate required service flows.
Incomplete review of Conditional Access policies	Medium	High	Inventory all policies, modes, assignments, exclusions, grant controls, and interactions; test with representative users and emergency accounts.
Security defaults disabled	Medium	High	Validate the custom controls replacing relevant defaults; review break-glass accounts, exclusions, authentication

			strength, logging, and recovery.
Production licensing not validated	Unassessed	High	Confirm licensing for Private Access, Conditional Access, Intune, and any required Entra features before deployment beyond the lab.
Single connector hosted on domain controller	Medium	High	Assess separation of duties and server risk; deploy and test additional connector capacity if availability requirements justify it.
Native application authentication remains	Medium	High	Review password policy, MFA support, session security, application patching, account lifecycle, and role permissions for each application.
File-share and group-membership drift	Medium	High	Conduct scheduled access reviews; compare role membership, Private Access assignments, share permissions, and NTFS ACLs.
Insufficient central monitoring and retention	Medium	High	Define audit coverage, log retention, alert routing, review ownership, and evidence preservation; consider centralized SIEM integration.
Endpoint compliance gaps or client failures	Medium	Medium	Maintain enrollment, policy assignment,

			client health, remediation guidance, and test coverage for supported endpoint types.
Limited negative and resilience test coverage	Medium	High	Expand tests to all applications, alternate access paths, privileged accounts, connector outages, session revocation, and rollback.

The highest-priority future work is to review the complete Conditional Access policy set and the replacement controls for security defaults, then address the flat network and connector dependency. Production licensing is a gating item because the environment documentation identifies trial subscriptions with November 2026 expiry or renewal dates. The project should not be moved into production until licensing and operational support are confirmed.

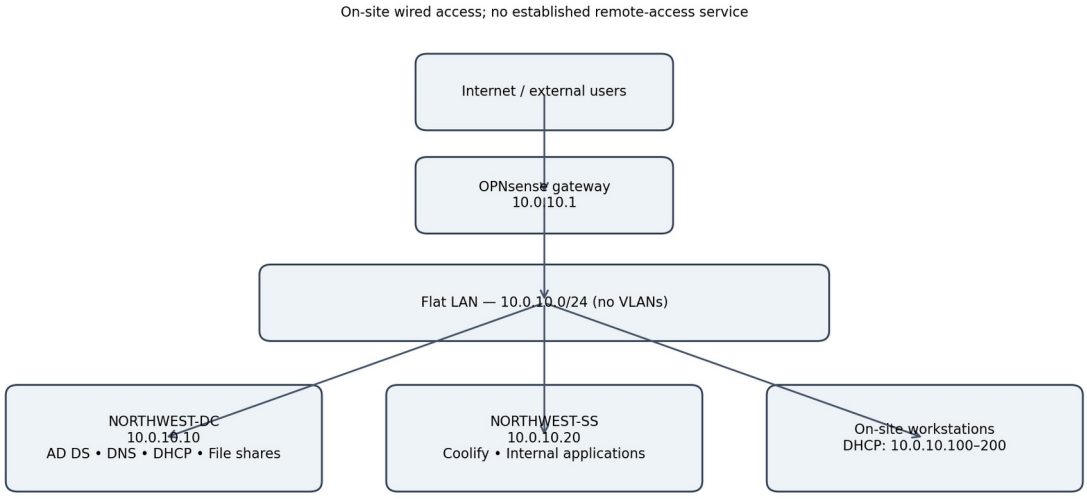
14. Maintenance Plan (G)

The following maintenance schedule defines recommended review frequencies, responsible roles, and operational activities.

Frequency	Responsible role	Activities and records
Daily / continuous	IT administration; helpdesk triage	Review available sign-in and access failures, suspicious MFA activity, connector/client health, and device-compliance alerts. Record escalations and response actions.
Monthly	IT administration	Review Entra Connect/Cloud Sync health, Intune enrollment and compliance, endpoint client health, connector updates, licensing status, and Conditional Access changes.
Quarterly	IT administration with department owners	Review role-group membership, Private Access assignments, file-share and

		NTFS permissions, native application accounts, privileged access, and leaver records. Retest representative allow and deny scenarios.
Annually and after material change	Executive risk owner and IT administration	Review remote-access architecture, all Conditional Access policies, security-defaults replacement controls, emergency access, HIPAA-related risk objectives, log retention, incident response, and recovery.
Before production deployment	IT administration and executive risk owner	Validate production licensing, complete broader security testing, assess connector resilience, confirm support procedures, and document acceptance of residual risk.

Figure 1. Pre-implementation network



Maintenance evidence should include dated review records, policy exports, group-membership snapshots, compliance reports, connector health checks, test results, and documented remediation. Changes to access policies should follow a controlled process: capture the current state, define the intended change, test with representative allowed and denied scenarios, verify the final mode, and retain the change record.

15. Conclusion

Northwest Health Center implemented a controlled remote-access capability using Microsoft Entra Private Access / Global Secure Access. The project connected the existing on-premises identity environment to Entra ID, configured hybrid join, deployed a Private Access connector on NORTHWEST-DC and clients on endpoint machines, introduced MFA through custom Conditional Access, enabled Intune enrollment and device compliance, and used role groups to restrict access to selected private applications and file shares.

The architecture adds a security layer without replacing the existing application authentication model. Remote users must pass the identity, MFA, device, and application-assignment checks before reaching an internal resource. They must then authenticate to the application itself or satisfy the Windows file-share permissions. This layered model improves remote-access control while preserving the existing on-premises applications and services.

All six acceptance tests passed. The evidence includes successful external access, device-based denials, MFA workflow artifacts, a role-based Docmost denial, and successful authorized file-share access. The implementation achieved its focused objective in the lab. It did not implement network segmentation, NAC, application-wide SSO, a complete Conditional Access review, or a comprehensive monitoring and incident-response program. Those remain future priorities.

The project's central outcome is a practical move away from implicit trust based on physical network location toward controlled, identity-aware access to selected internal resources. Continued policy review, licensing validation, connector resilience, network segmentation, application hardening, and operational monitoring are necessary before treating the lab configuration as a production-ready security architecture.

References

Microsoft. (2026a). Tutorial: Enable Private Access traffic forwarding. Microsoft Learn. https://learn.microsoft.com/en-us/entra/global-secure-access/tutorial-private-access-enable-traffic-forwarding

Microsoft. (2026b). How to configure per-app access using Global Secure Access applications. Microsoft Learn. https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-per-app-access

Microsoft. (2026c). Microsoft Entra Conditional Access documentation. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/conditional-access/

Microsoft. (2026d). Use compliance policies to set rules for devices you manage with Intune. Microsoft Learn. https://learn.microsoft.com/en-us/intune/device-security/compliance/overview

Microsoft. (2026e). How to configure connectors for Microsoft Entra Private Access and Microsoft Entra application proxy. Microsoft Learn. https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-connectors

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

U.S. Department of Health and Human Services. (n.d.). Summary of the HIPAA Security Rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Appendix A. Evidence Register

The accompanying supporting evidence appendix contains selected screenshots from the project archive. This register identifies each evidence group and its relevance to the report.

Evidence group	Files	Use in report
Entra tenant and identity	EV-03-M365-Licenses.png; EV-04-Entra-Overview.png; EV-05-Entra-Users.png; EV-06-Entra-Connect-Status.png	Tenant, users, licensing context, and synchronization.
MFA and Conditional Access	EV-08-MFA-Baseline.png; EV-09-CA-Policies.png; EV-09-CA-Require-MFA.png	Authentication methods and custom MFA policy. The supplied policy screenshot records report-only state at capture.
Device enrollment/compliance	EV-11-Entra-Baseline-Devices.png; EV-11-Intune-Baseline-Devices.png; EV-12-Intune-Enrollment-Config.png; EV-13-Intune-Device-Compliant-NORTHWEST-L-LAB.png; EV-14-Compliance-Policy.png	Enrollment configuration, device inventory, and compliant endpoint.
Device policy state	EV-09-CA-Require-Compliant-Device-ReportOnly.png; EV-14-Intune-Compliance-Remediation-BitLocker-Prompt.png	Report-only policy snapshot and compliance remediation. Enabled for acceptance testing; screenshot is report-only at capture.
Security defaults chronology	EV-10-Security-Defaults-Note.txt; EV-10-Security-Defaults-Reenabled.png	Collection note and enabled-state screenshot; these show an enabled state at capture; security defaults were disabled at project completion.
Sign-in logs	EV-10-Sign-in-Logs.csv	Ten exported sign-in records with identity, application, IP,

		client, status, Conditional Access, and device fields.
TC-01	EV-TC01-Allow-Priya-Success.png; EV-TC01-Priya-External-Network-Success.png	Successful Global Secure Access connection and external application reachability.
TC-02 / TC-05	EV-TC02-TC05-Unmanaged-Device-Blocked.png	Access blocked because endpoint/client did not meet management compliance requirements; retain separate test preconditions.
TC-03	EV-TC03-MFA-Setup-Prompt.png; EV-TC03-MFA-Not-Setup-Blocked.png; EV-TC03-Work-Account-Sign-in-Prompt.png	MFA registration and sign-in workflow evidence.
TC-04	EV-TC04-Role-Blocked-Docmost.png; EV-TC04-Network-Drive-Blocked.png; EV-TC04-Role-Prompt.png; EV-TC04-Unresolved-Then-Signin.png	Application assignment denial and file-share access denial.
TC-06	EV-TC06-Network-Drive-Allow.png; EV-TC06-Priya-Role-Membership.png	Successful authorized file-share access and role membership.
AD / FileShares / Network	domain.txt; forest.txt; gpos.csv; groups.csv; ous.csv; role-memberships.txt; users.csv; shares.csv; share-permissions.txt; ClinicFiles-full-acl.txt; nmap-discovery.txt; nmap-services.txt	Directory structure, group membership, file-share permissions, and baseline network/service inventory.

Figure 2. Post-implementation remote-access architecture

