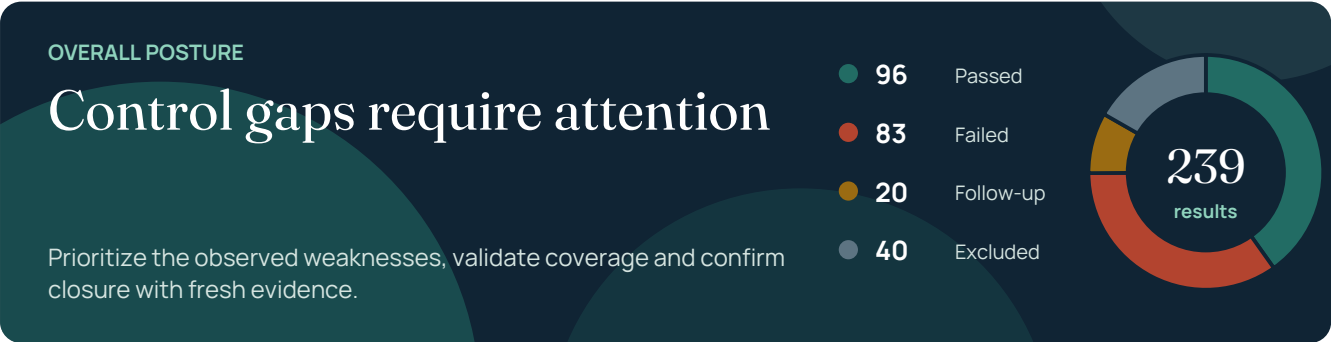


SECURITY ASSESSMENT

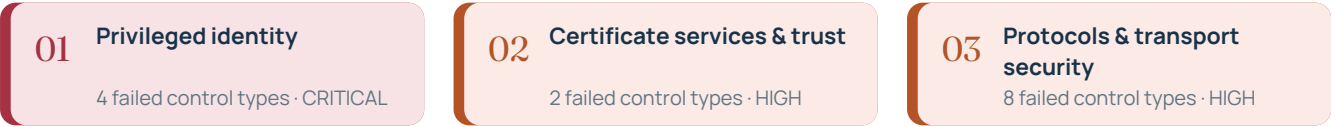
Executive summary

northwind.example | 29 September 2026 | Internal assessment



The leading areas for review are privileged identity, certificate services & trust, protocols & transport security. The scan recorded 83 failed and 96 passing results. Repeated host checks are counted separately; these totals are not unique vulnerabilities. The report does not establish active compromise, business impact or an organization-wide security score.

WHERE TO FOCUS



FAILED RESULTS BY SEVERITY



ASSESSMENT SNAPSHOT

REMOTE COLLECTION 6 of 6 targets returned; 7 of 63 discovered hosts selected DC 1/2 · server 5/9 · workstation 1/52	HUMAN REVIEW 1 review required Collected evidence to assess	EXPLICIT CONFIGURATION 11 not configured Validate effective defaults	COVERAGE LIMITS 1 unavailable / 7 inconclusive Collect or validate evidence	ERRORS / EXCLUSIONS 0 errors / 40 not applicable Errors never count as passes
--	--	---	--	--

THE MANAGEMENT DECISION

Assign owners, agree a staged rollout and resolve each evidence limitation before accepting closure. Manual reviews and absent explicit settings are separate from failed collection.

REPORT NAVIGATION

Contents

Sample excerpt. Page 1 is the executive summary. Each section below keeps its summary and shows at most 2 controls in full; the last page says what the full report adds.

Scope & interpretation	3
Essentials summary	5
Findings & next actions	6
Directory / northwind.example	7
nwt-dc01.northwind.example	8
Microsoft 365 / northwind.onmicrosoft.com	9
About this excerpt	10

READ THIS FIRST

Scope & interpretation

Domain: northwind.example

Selected controller: nwt-dc01.northwind.example

Collected UTC: 2026-09-29T09:30:00+00:00

Collector: 0.14.2 | Technical format: 3.0

Microsoft 365 tenant: northwind.onmicrosoft.com (Northwind Traders)

Exchange Online organization: Northwind Traders | module 3.7.1 | Exchange session connected | Security & Compliance session connected

Workload tracks: SharePoint ok | Defender ok | Teams ok

Selection and coverage: 6 of 6 remote targets returned evidence; 7 of 63 discovered hosts were selected (domain controllers 1 of 2, servers 5 of 9, workstations 1 of 52). Selection strategy: operator-selected hosts. Hosts that were discovered but not selected were not assessed; no result is inferred for them.

Sample report: fictional organization

336

Passed

217

Needs attention

77

Not applicable

70

Review required

48

Not explicitly configured

7

Evidence unavailable

9

Inconclusive

0

Collection error

PASS

Passed. Observed baseline met.

FAIL

Needs attention. Observed baseline not met.

N/A

Not applicable. Evidence established this check was inapplicable.

REVIEW

Review required. Evidence was collected; this control requires a contextual review.

UNSET

Not explicitly configured. The queried explicit configuration was absent. This does not establish effective runtime state.

NO DATA

Evidence unavailable. Required evidence was not returned or the provider could not establish the state.

PARTIAL

Inconclusive. Some evidence was collected, but it is insufficient for a complete conclusion.

ERROR

Collection error. An attempted collection operation failed.

NO RESULT marks an absent matrix intersection; scope or missing evidence must be reviewed. It is not an N/A determination and is excluded from result counts. Repeated local/remote observations are retained and counted separately, including conflicting statuses. Directory results apply to the selected-controller scope, not every host.

Review this explicit lab configuration against the applicable Microsoft baseline and application dependencies. The collector makes no changes; missing settings do not imply a safe default.

Collection is read-only. Configuration observations do not attest runtime enforcement or endpoint integrity. Account and membership queries are capped at 200 entries per query. Privileged scope covers Domain, Enterprise and Schema Admins, including the collected nested/primary-group relationships; other groups and effective fine-grained user policies are outside scope. Host inventory is bounded and marked when truncated. AD CS results identify candidates, not proven attack paths. Microsoft 365 coverage is limited to the Entra ID controls read through Microsoft Graph with delegated read-only permissions, the Exchange Online and Purview controls read through Get-* cmdlets of the Exchange Online PowerShell module and the SharePoint, Defender, Teams controls of the collected workload tracks, all listed under the tenant scope; on-premises Exchange application configuration and effective share/NTFS access are not assessed. Hotfix dates and software registrations do not establish vulnerability or patch applicability.

REPORTING PROFILE

Essentials summary

The Essentials profile covers 71 of the 194 evaluated control types (239 of 764 results). The executive brief is computed from these rows only; every control is evaluated on every run.

96

Passed

83

Needs attention

40

Not applicable

1

Review required

11

Not explicitly configured

1

Evidence unavailable

7

Inconclusive

0

Collection error

This section continues with 71 more controls in the full report.

SHARED GUIDANCE / HOST-SPECIFIC EVIDENCE

Findings & next actions

In the full report every failed and unresolved control is explained here once, with its guidance, next action and every affected scope. Severity is separate from outcome.

AD-007**Enabled privileged users with service principal names****GUIDANCE**

An SPN on a privileged user creates Kerberos service-ticket exposure; no ticket requests or password cracking were performed. Review privilege separation and managed service accounts.

Directory /
northwind.example

1 matching objects observed. Examples: svc-backup.

FAIL

Severity: critical | Rule 2

AD-001**krbtgt password age****GUIDANCE**

If confirmed, plan a controlled krbtgt rotation using Microsoft guidance; verify replication and effective ticket lifetimes before scheduling resets. No directory changes were performed.

Directory /
northwind.example

Password age exceeds 180 days. Password last set: 2023-08-29T09:30:00+00:00.
Threshold: greater than 180 days.

FAIL

Severity: high | Rule 1

This section continues with 138 more controls in the full report.

SCOPE SUMMARY / EXCERPT

Directory / northwind.example



Failed-result severity: 1 critical, 4 high, 7 medium, 1 low, 0 unrated.

AD-002	Privileged users with non-expiring passwords
GUIDANCE	Review service-account ownership and managed-account alternatives before changing expiration.
Directory / northwind.example	2 matching objects observed. Examples: Administrator, svc-backup.
FAIL	
Severity: high Rule 2	

CHECK / OUTCOME	OBSERVATION
AD-009	Unconstrained delegation on enabled non-DC objects
PASS	No matching objects found in collected scope. Rule: 2.

This section continues with 21 more controls in the full report.

SCOPE SUMMARY / EXCERPT

nwt-dc01.northwind.example

47 Passed	22 Needs attention	11 Not applicable	7 Review required
8 Not explicitly configured	0 Evidence unavailable	0 Inconclusive	0 Collection error

Failed-result severity: 0 critical, 4 high, 18 medium, 0 low, 0 unrated.

HOST - 013	Print Spooler on domain controllers
GUIDANCE	Disable the Spooler on domain controllers after reviewing printing dependencies. Non-DC hosts are not applicable.
nwt-dc01	Domain controller: True; Spooler running: True.
FAIL Severity: high Rule 2	

CHECK / OUTCOME	OBSERVATION
HOST-001	Windows OS support lifecycle
PASS	Microsoft Windows Server 2022 Standard. Extended support ends 2031-10-14. Lifecycle table reviewed 2026-09-22; ESU not verified. Rule: 1.

This section continues with 93 more controls in the full report.

The full report includes a volume for each of the 7 hosts assessed.

SCOPE SUMMARY / EXCERPT

Microsoft 365 / northwind.onmicrosoft.com

36

Passed

26

Needs attention

0

Not applicable

14

Review required

0

Not explicitly configured

0

Evidence unavailable

0

Inconclusive

0

Collection error

Failed-result severity: 0 critical, 12 high, 14 medium, 0 low, 0 unrated.

DEF-003

Alerts unresolved for more than 7 days

GUIDANCE

Triage every Defender alert open for more than seven days, starting with the high-severity ones, and record the resolution or the accepted risk.

FIX

Triage the alerts older than seven days in the Defender portal: resolve, classify as false positive, or escalate. Assign an owner for the alert queue.

Microsoft 365 / northwind.onmicrosoft.com

2 of 5 unresolved alerts have been open for more than 7 days; 1 high severity.

FAIL

Severity: high | Rule 1

CHECK / OUTCOME

OBSERVATION

ENT-001

PASS

MFA required for all users

Security defaults are disabled; 1 enabled Conditional Access policy requires MFA for all users (Require MFA for all users); 0 excluded users and 0 excluded groups. Rule: 1.

This section continues with 74 more controls in the full report.

SAMPLE EXCERPT

About this excerpt

This is an excerpt. The full technical report for this environment has 126 pages covering 194 controls across 22 sections.

What the full report adds

Executive brief: the priority and supporting workstreams and a 30/60/90-day delivery plan (pages 2 to 4).

Cross-host check matrices: every evaluated control against every scope, grouped by workstream and by Microsoft 365 workload.

Essentials matrices: each Essentials control against every scope.

Findings & next actions: every failed and unresolved control with its guidance, next action and affected scopes.

Scope sections: one per host, the directory and the tenant, each with a findings index and its passed and inapplicable evidence.

Host inventories: operating system, local administrators, shares, hotfixes, ASR rule modes and software registrations of each host.

Tenant inventory: tenant identity, licensing, granted scopes, workload collection status and collection diagnostics.

Methodology references: the Microsoft documentation the assessment refers to.

Your own report covers every control for your environment. The sample is built from a fictional organization by the same rules and renderer.

About this report

This report describes the configuration collected from the hosts and workloads listed in it, at the time shown, within the limits in its coverage section. It is a point-in-time review, not a penetration test, an audit opinion, a certification or a guarantee of security or compliance. Findings and guidance are informational; test any change first. Settings that could not be read are reported as missing, not passing. Microsoft and Windows behavior can change after the collection date. Prepared by GlacierPoint Technologies LLC under the GlacierPoint Scan Terms of Service.