



northwind-components.example

LAST SCANNED

SEP 25 2026

FIRST SCANNED

SEP 25 2026

SCAN DURATION

6m 52s

680 / 950

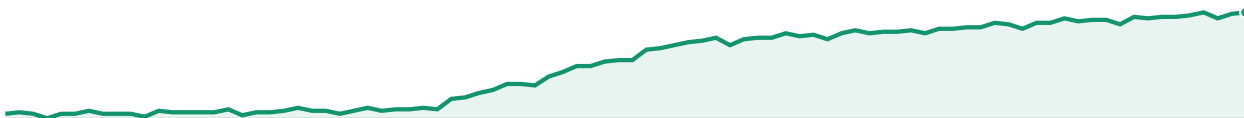
Grade B- · Fair

6 / 21 checks failed · 7 informational · 8 passed

● Critical 0 ● High 2 ● Medium 4 ● Low 0

Scan ran from 2026-09-25 02:14 UTC to 2026-09-25 02:21 UTC Duration: 6m 52s

NINETY-DAY TREND



612 → 680 over the last 90 days ▲ 68 points — posture has improved.

What we scanned

12,266

total checks run

9

assets monitored

6

issues discovered

What this report covers

12,266 automated checks were executed against 9 monitored assets. Every check that ran is listed in this report with its result — there are no categories assessed but omitted.

Issue summary

Severity	Issue	Count	First detected
High	Object storage bucket is publicly readable	1	2026-08-02
High	Administrative interface reachable from the public internet	1	2026-08-02
Medium	TLS certificate expires within 30 days	1	2026-09-16
Medium	Web server discloses version in response headers	1	2026-08-02
Medium	Access key older than 365 days	1	2026-08-02
Medium	Security group permits unrestricted egress	1	2026-08-02

6 / 21 checks failed

Object storage bucket is publicly readable

High

A storage bucket holding production export files permits anonymous list and read access. Anyone who learns or guesses the bucket name can enumerate and download its contents; no authentication is required and no access log distinguishes an attacker from a legitimate reader.

Enable the account-level public access block, remove the allow-all bucket policy, and serve the objects that must remain public through a signed URL or a CDN origin identity instead.

[CIS AWS Foundations 2.1.5](#)
[ISO/IEC 27001:2022 A.5.10](#)

	exports.northwind-components.example:443 public-read
First detected	2026-08-02
1 Known	

Administrative interface reachable from the public internet

High

A management interface answers on TCP/3389 from any source address. Exposed administrative services are subject to continuous automated credential attacks, and a single reused password is sufficient for initial access.

Restrict the security group to the corporate egress ranges or a bastion, and require the VPN for administrative access. Where remote administration must remain available, put it behind an identity-aware proxy with MFA.

[NIS2 Article 21\(2\)\(d\)](#)
[CIS Controls v8 4.6](#)

	203.0.113.47:3389 0.0.0.0/0
First detected	2026-08-02
1 Known	

TLS certificate expires within 30 days

Medium

The certificate presented on the customer portal expires in 22 days. Expiry on a customer-facing service is a self-inflicted outage, and the browser warning that precedes it trains users to click through exactly the dialog that protects them.

Renew and automate renewal, and alert at 30 days rather than at expiry.

[ISO/IEC 27001:2022 A.8.24](#)

	portal.northwind-components.example:443 expires in 22 days
First detected	2026-09-16
1 Known	

Web server discloses version in response headers

Medium

The Server header names the product and exact version. It does not create a vulnerability, but it lets an attacker select a working exploit without probing, which removes the noisy step defenders are most likely to detect.

Suppress version tokens in the server configuration.

[OWASP ASVS 14.3.3](#)

	portal.northwind-components.example:443
	203.0.113.19:443
First detected	2026-08-02

2 Known

Access key older than 365 days

Medium

A programmatic credential has not been rotated in over a year. Long-lived keys accumulate copies — in CI configuration, on laptops, in a former employee's password manager — and none of those copies are revoked when someone leaves.

Rotate the key and move the workload to a short-lived assumed role. Where a static key is unavoidable, set a rotation reminder at 90 days.

[CIS AWS Foundations 1.14](#)

[DORA Article 9\(4\)\(c\)](#)

	iam:: service-account (build pipeline) key age 418 days
First detected	2026-08-02

1 Known

Security group permits unrestricted egress

Medium

Instances in one subnet may open outbound connections to any destination on any port. Unrestricted egress is what turns an initial foothold into data exfiltration and command-and-control, and it is rarely required.

Restrict egress to the destinations the workload needs, then alert on denials.

[NIS2 Article 21\(2\)\(a\)](#)

[CIS Controls v8 13.4](#)

	203.0.113.0/24 egress 0.0.0.0/0 all ports
First detected	2026-08-02

1 Known

7 informational findings

HTTP Strict-Transport-Security header present

Info

HSTS is set with a one-year max-age on all customer-facing hosts.

	portal.northwind-components.example
First detected	2026-08-02

1 Known

No plaintext HTTP listener on customer-facing hosts

Info

All public web endpoints redirect to TLS; no service answers unencrypted.

	portal.northwind-components.example
First detected	2026-08-02

1 Known

Database services are not internet-reachable

Info

No database port answered from outside the estate during the scan window.

	203.0.113.0/24
First detected	2026-08-02

1 Known

Root account has no active access keys

Info

The account root principal holds no programmatic credentials.

	iam:: root
First detected	2026-08-02

1 Known

Storage encryption at rest enabled across all volumes

Info

Every attached volume and managed database reports encryption enabled.

	all monitored assets
First detected	2026-08-02

1 Known

No indicators of compromise matched threat intelligence

Info

No observed address, domain or hash matched the threat-intelligence corpus.

	all monitored assets
First detected	2026-09-16

1 Known

Audit logging enabled in all active regions

Info

Management-plane logging is on in every region with running resources.

	3 regions
First detected	2026-08-02

1 Known

8 / 21 checks passed

No reports of botnet activity in the last 30 days



This IP/domain has not been reported as a source of botnet activity in the last 30 days.

Expected	Botnet Activity: false
----------	------------------------

No reports of brute force login attempts in the last 30 days



This IP/domain did not appear on any list of IPs and domains known to perform brute force login attempts in the last 30 days.

Expected	Unsolicited Communication > Brute Force Login Attempt: false
----------	--

No reports of malware distribution in the last 30 days



This IP/domain has not been reported for distributing malware in the last 30 days.

Expected	Malware Server: false
----------	-----------------------

No reports of phishing activity in the last 30 days



This IP/domain has not been reported as a phishing site in the last 30 days.

Expected	Phishing Site: false
----------	----------------------

No reports of botnet activity in the last 90 days



This IP/domain has not been reported as a source of botnet activity in the last 90 days.

Expected	Botnet Activity: false
----------	------------------------

No reports of brute force login attempts in the last 90 days

This IP/domain did not appear on any list of IPs and domains known to perform brute force login attempts in the last 90 days.

Expected	Unsolicited Communication > Brute Force Login Attempt: false
----------	--

No reports of malware distribution in the last 90 days

This IP/domain has not been reported for distributing malware in the last 90 days.

Expected	Malware Server: false
----------	-----------------------

No reports of phishing activity in the last 90 days

This IP/domain has not been reported as a phishing site in the last 90 days.

Expected	Phishing Site: false
----------	----------------------

About Telaris

Platform

Telaris is a continuous attack surface intelligence platform that actively scans internet-facing infrastructure, cloud environments, and containers for vulnerabilities, misconfigurations, and exposed secrets.

Scanning methodology

All scans use read-only network probes executed inside ephemeral, isolated containers. No data is modified on target systems. Credentials are never stored after scan completion.

Severity definitions

Critical	Immediate breach risk. Exploit requires minimal skill. Remediate within 24 h.
High	Likely to be exploited. Could lead to significant data compromise. Remediate within 30 days.
Medium	Unlikely in isolation. Requires attacker skill or vulnerability chain. Remediate within 90 days.
Low	Minor weakness or informational finding. Address in next maintenance cycle.