

Northwind Logistics (demo)

Sept 1–30, 2026 · 9 monitored assets



Good, up 3 points from August.
2 high risks remain open; 11 alerts were resolved.

16

Alerts

11

Resolved

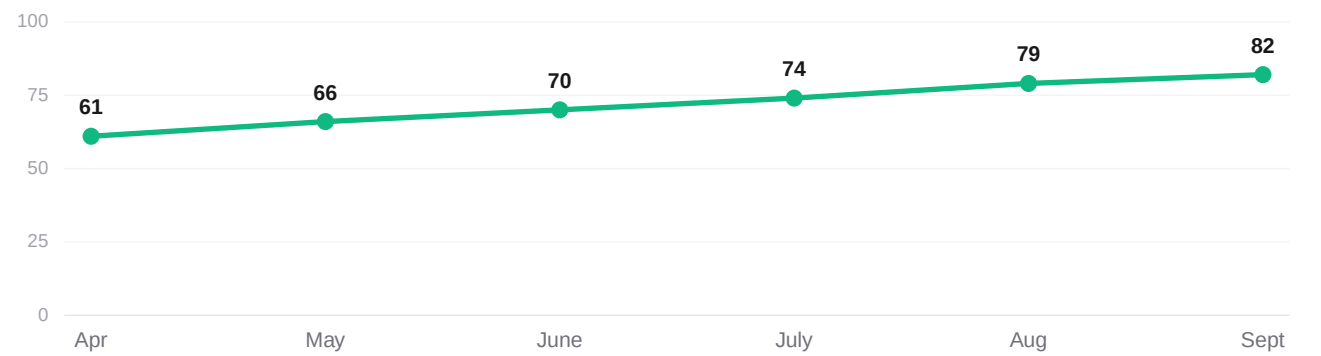
2

Open high+

6.5h

Median fix

Score, last 6 months



Top open risks

- HIGH

OpenSSH 7.4 with known CVEs exposed on vpn.northwind-logistics.example
vpn.northwind-logistics.example · since Sep 21, 2026
- HIGH

Anonymous FTP login allowed on legacy-ftp.northwind-logistics.example
legacy-ftp.northwind-logistics.example · since Sep 26, 2026
- MEDIUM

DMARC policy is p=none — mail.northwind-logistics.example
mail.northwind-logistics.example · since Sep 9, 2026

Assets

ASSET	TYPE	RISK SCORE	LAST CHECKED
vpn.northwind-logistics.example	DOMAIN	64	Sep 30, 2026
legacy-ftp.northwind-logistics.example	DOMAIN	58	Sep 30, 2026
198.51.100.24	IP	41	Sep 30, 2026
mail.northwind-logistics.example	DOMAIN	33	Sep 30, 2026
northwind-logistics.example	DOMAIN	18	Sep 30, 2026
portal.northwind-logistics.example	DOMAIN	12	Sep 30, 2026
tracking.northwind-logistics.example	DOMAIN	9	Sep 30, 2026
203.0.113.17	IP	6	Sep 30, 2026
status.northwind-logistics.example	DOMAIN	0	Sep 30, 2026

Resolved this period

ALERT	SEVERITY	RESOLVED
TLS certificate expires in 7 days — portal.northwind-logistics.example	HIGH	Sep 2, 2026
Open port 3389 (RDP) on 198.51.100.24	CRITICAL	Sep 3, 2026
Missing HSTS header — tracking.northwind-logistics.example	LOW	Sep 5, 2026
SPF record allows too many lookups — northwind-logistics.example	MEDIUM	Sep 8, 2026
Weak TLS 1.0 enabled — mail.northwind-logistics.example	MEDIUM	Sep 10, 2026
Domain registration expires in 21 days — northwind-logistics.example	MEDIUM	Sep 12, 2026
Staff credentials found in a public breach (2 accounts)	HIGH	Sep 14, 2026
Open port 9200 (Elasticsearch) on 203.0.113.17	CRITICAL	Sep 17, 2026
Missing Content-Security-Policy — status.northwind-logistics.example	LOW	Sep 20, 2026
New subdomain discovered: staging.northwind-logistics.example	INFO	Sep 23, 2026
Certificate name mismatch — legacy-ftp.northwind-logistics.example	MEDIUM	Sep 27, 2026

Recommendations

Strengthen email security

Email security score 68 · 1 open alert · DMARC policy is p=none on 1 domain

- Publish SPF and DKIM for every domain that sends mail.
- Move DMARC to p=quarantine or p=reject once aggregate reports look clean.
- Reset passwords and enforce MFA for accounts found in breaches.

Reduce internet exposure

Exposure score 71 · 2 open alerts · SSH open on 1 host; 1 service with a known CVE

- Close or firewall ports that do not need to be public (databases, RDP, SSH, admin panels).
- Patch or upgrade services that have known CVEs in the exposure scan.
- Add missing security headers and renew domain registrations early, with auto-renew on.

Work down open alerts

Open alerts score 80 · 3 open alerts · 2 high alerts open

- Triage critical and high alerts first and give each one an owner.
- Resolve fixed issues and mark false positives so the score reflects real risk.
- Tune rules that fire repeatedly without leading to action.

Generated by TLINK PRO on Oct 23, 2026 · pro.threatgrid.tech