SAMPLE

SURVEIL-X

northstarcommerce-demo.com Cyber Risk Report

Diagnosing Company:	Northstar Commerce Ltd.
Diagnosed Domain:	northstarcommerce-demo.com
Submission Date:	30 June 2026

Scan Results

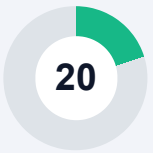
Cyber Risk Report

30 June 2026

northstarcommerce-demo.com

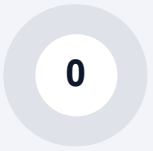
Surface Exposure

Risk Level: Low



IP Reputation

Risk Level: Low

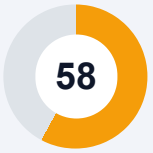


Domain Health

Risk Level: High

Asset Risk

Risk Level: Medium



Report Summary

Overall, this sample organization shows moderate external cyber risk. The most important areas needing attention are domain health and visible public assets, while IP reputation remains stable and surface exposure is comparatively controlled. The next steps should focus on DNS hardening, legacy asset cleanup, and tightening administrative access to externally reachable services.

Credential Check

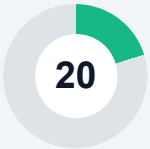
No leaked passwords were identified in this sample review. That said, account security still depends on strong credential hygiene across registrar, DNS, hosting, CDN, and shared mailbox access.

Recommended baseline controls: use unique passwords, enforce MFA on critical accounts, and maintain named ownership for every public-facing service.

Disclaimer

- This sample cyber risk report is provided for informational purposes only and does not constitute legal, financial, or cybersecurity advice.
- Findings are based on public signals and outside-in observations available at the time of the scan, so they may not reflect every internal control or compensating safeguard.
- Any remediation decisions should be reviewed by the organization’s security, IT, compliance, or leadership teams before implementation.

Surface Exposure



Risk Level: Low

This reflects how visible or accessible your systems are on the public internet. In this sample, the public footprint is relatively controlled, but a few discoverable services still warrant periodic review.

Summary

The exposure surface score reflects the number of externally visible entry points. A lower score indicates fewer public attack paths and a stronger default posture.

Action

- Continue regular reviews of externally reachable ports, services, and staging endpoints.
- Restrict access to administrative interfaces and remove any public assets no longer in use.

Key Insight

The current exposure is manageable, but disciplined inventory and access review keep it that way.

Risk Level	Explanation
Low	Only essential public services are visible. Safer and more controlled.
Medium	A few extra systems or ports are externally discoverable and should be reviewed.
High	Multiple visible services or weak access paths increase the likelihood of external targeting.
Critical	Sensitive systems appear overly exposed, creating serious breach risk.

Domain Health

Risk Level: High

Domain health covers the settings and trust signals that protect email, DNS, and the external identity of the business. In this sample, weak DMARC enforcement, incomplete sender alignment, and legacy subdomain hygiene are the main concerns.

Summary

The domain score indicates a meaningful risk of spoofing, phishing, or loss of trust if DNS and email controls are not tightened.

Recommended Actions

- Move DMARC toward quarantine or reject after validating approved senders.
- Review SPF and DKIM alignment across business-critical email flows.
- Inventory subdomains and retire any legacy or unowned records still resolving publicly.
- Protect registrar and DNS administration with MFA and named ownership.

Visible Signals

- SPF record present
- DKIM alignment partial
- DMARC policy monitor-only
- Security headers incomplete
- Legacy subdomains observed

This sample is intentionally formatted to mirror the structure and page rhythm of the provided reference reports while using neutral Surveil-X branding and placeholder organization data.