EXECUTIVE SUMMARY

# Acme Logistics Exposure Score: 58/100

**High Exposure** — Multiple critical gaps in email authentication and identity controls. Acme is at elevated risk of Business Email Compromise (BEC) and credential-based account takeover. The fixes are straightforward and require no new tool purchases; Northwind IT Services can complete the prioritized roadmap in approximately 6 weeks.

## Category Breakdown

| Category | Grade | Score | Notes |
|---|---|---|---|
| Email Authentication (SPF + DMARC) | **F** | 28 | DMARC missing entirely · SPF has +all (open) |
| TLS / SSL & Certificate Health | **B** | 78 | TLS 1.2 · cert valid 96 days · HSTS missing |
| HTTP Security Headers | **C** | 64 | 5 of 11 headers present · no CSP, no COOP |

PRIORITIZED FINDINGS

## What to fix first

This list is ordered by impact. Items marked **HIGH** represent realistic attack paths into Acme's environment. Northwind IT Services recommends prioritizing all HIGH items in the first two weeks of remediation.

| Sev | Area | Finding |
|---|---|---|
| HIGH | Email | **No DMARC record published**<br>Acme's domain can be spoofed by attackers. Publish a starting record at p=none with reporting, then escalate to p=quarantine after 2 weeks and p=reject after another 2 weeks. Most BEC attacks against SMBs depend on this gap. |
| HIGH | Email | **SPF record uses +all (allows any sender)**<br>Replace +all with -all in the SPF record after confirming every legitimate sender is listed in the includes. +all defeats SPF entirely. |
| HIGH | Email | **No MFA enforcement detected on M365 admin**<br>Audit confirms admin accounts on Acme's tenant have MFA disabled. Enable MFA enforcement under Defender → Identity → Authentication methods. Highest-impact single change. |
| MED | TLS | **HSTS header missing on apex domain**<br>Add Strict-Transport-Security with max-age=15552000; includeSubDomains; preload to all HTTP responses. Once in place for 60+ days, submit to the HSTS preload list. |

| Sev | Area | Finding |
|---|---|---|
| MED | Headers | **No Content-Security-Policy header**<br>Set a starting CSP of default-src 'self' on all HTML responses, then iterate. Blocks a wide class of XSS attacks. |
| MED | Headers | **Missing Cross-Origin-Opener-Policy**<br>Add COOP: same-origin-allow-popups for protection against cross-origin attacks. |
| LOW | TLS | **Certificate renewal window approaching**<br>Cert expires in 96 days. If using Let's Encrypt, ensure auto-renewal is working. Otherwise, calendar the renewal at day 60. |

REMEDIATION ROADMAP

## Northwind's recommended 6-week plan

This roadmap balances impact against effort. Northwind IT Services can execute most items under your existing managed services agreement; the DMARC and MFA work specifically requires admin access to your M365 tenant.

| When | Focus | Tasks |
|---|---|---|
| **Week 1** | Email authentication | Publish DMARC at p=none + verify SPF/DKIM. Engage Acme's M365 admin to enable MFA on all admin accounts. |
| **Week 2-3** | Email + monitoring | Review DMARC reports for unauthorized senders. Add missing legitimate senders to SPF. Begin MFA rollout for all user accounts. |
| **Week 4-5** | TLS + Headers | Add HSTS, CSP, COOP headers. Schedule a re-scan to verify. |
| **Week 6** | Escalate DMARC | Move DMARC to p=quarantine pct=25, then 100, then p=reject over 2 weeks. |
| **Quarterly** | Continuous monitoring | Re-scan client domains monthly. Track exposure-score drift. Raise concerns at QBR. |

**Northwind IT Services** can review these findings and the roadmap with you on a 30-minute call. Reply to alex.chen@northwind-it.example or call your account manager directly.

*This report is a white-label sample from the Breach Horizon for MSPs platform. The data is illustrative; Acme Logistics and Northwind IT Services are fictional companies. The methodology, score formula, and category weights are identical to production scans.*