VAIXUS
Technologies

VAIXUS-CS-001

Revenue Deliverability Infrastructure Assessment

A Laboratory-Engineered Consulting Simulation — Outbound Sales Infrastructure

Prepared for: Northlane Software, Inc. (Synthetic Engagement)
Prepared by: Vaixus Technologies
Publication Date: June 10, 2026
Document Version: 1.0
Classification: Laboratory Simulation — Public Portfolio Use

LABORATORY-ENGINEERED CONSULTING SIMULATION

This report is a fictional, laboratory-generated case study prepared for portfolio and methodology-demonstration purposes. It does not describe a real client, a real organization, or an actual engagement.

Confidentiality Notice

This document is a laboratory-engineered consulting simulation produced by Vaixus Technologies for portfolio, training, and methodology-demonstration purposes. All organization names, personnel, domains, IP addresses, DNS records, SMTP transcripts, authentication results, and engineering findings contained within this document are entirely synthetic and were constructed within a controlled laboratory environment. No portion of this report describes, references, or was derived from any real organization's infrastructure, personnel, or confidential information.

This report does not represent an actual client engagement. Vaixus Technologies has not been retained by, and has no business relationship with, any organization resembling the fictional entity described herein. Any resemblance to an actual organization, domain, or individual is coincidental and unintended.

Where this document is distributed for evaluative purposes (e.g., prospective client discovery, recruiting, or partner review), it should be treated as a demonstration of Vaixus Technologies' consulting methodology, technical documentation standard, and analytical approach — not as evidence of prior client work or measured business outcomes.

If adapted as a template for an actual client engagement, all synthetic evidence contained in this document must be replaced in its entirety with verified production evidence before delivery, and this notice must be revised to reflect the real engagement's confidentiality requirements.

Document Control

Field	Value
Document Title	VAIXUS-CS-001 — Revenue Deliverability Infrastructure Assessment
Document Version	1.0
Publication Date	June 10, 2026
Prepared By	Vaixus Technologies
Review Status	Final — Approved for Portfolio Publication
Classification	Laboratory Simulation — Public Portfolio Use
Engagement Type	Laboratory-Engineered Consulting Simulation

Revision History

Version	Date	Author	Summary of Changes
0.1	May 18, 2026	Soorya S V	Initial discovery findings drafted following environment reconnaissance.
0.6	May 29, 2026	Soorya S V	Technical findings and remediation roadmap completed; internal engineering review.
1.0	June 10, 2026	Soorya S V	Final release following documentation and executive review.

Table of Contents

1. Executive Summary

Northlane Software, Inc. (“Northlane”) engaged Vaixus Technologies to assess the infrastructure supporting its outbound sales email program following a sustained decline in outbound reply and meeting-booked rates across its North American and EMEA sales development pods. Northlane treats outbound email as a revenue-critical system: it is the primary top-of-funnel channel for its Revenue Intelligence platform and supports prospecting, demonstration scheduling, and account management across a combined sales development and account executive organization of 54 representatives.

The assessment examined DNS infrastructure, authentication configuration (SPF, DKIM, DMARC), domain segmentation strategy, and the integration quality of Northlane's outbound technology stack, which spans Google Workspace, Apollo, Instantly, Smartlead, and SendGrid across one primary corporate domain, one transactional subdomain, and three secondary outbound domains.

Vaixus identified thirteen findings spanning DNS configuration, authentication posture, domain architecture, and vendor operations. Two findings are rated Critical: the primary corporate domain's SPF record exceeds the RFC 7208 ten-lookup limit and is intermittently evaluated as a hard failure by strict receiving systems, and one of Northlane's secondary outbound domains was provisioned inside the same Google Workspace tenant as corporate mail, causing it to share the corporate MX destination and trust boundary rather than remaining operationally isolated. Both conditions directly undermine the domain segmentation strategy Northlane believes it has in place and represent the most probable drivers of the deliverability decline that prompted this engagement.

Overall, Northlane's outbound infrastructure reflects an organization that adopted modern outbound tooling faster than it formalized DNS governance. No finding in this report indicates malicious compromise; all findings are configuration and architectural in nature and are remediable without interrupting active sending campaigns. Vaixus recommends a three-phase remediation program beginning with the two critical findings, followed by authentication hardening and a DMARC enforcement ramp, and concluding with operational controls that prevent recurrence. Full remediation is estimated at 10–12 weeks and does not require a change of vendor.

Infrastructure Maturity Snapshot

Dimension	Current State	Target State
Authentication Coverage	SPF, DKIM configured on all domains; DMARC unenforced (p=none)	SPF valid on all domains; DMARC enforced (p=reject) with monitoring
Domain Segmentation	1 of 3 secondary domains improperly shares corporate trust boundary	All secondary domains fully isolated from corporate mail cluster
Deliverability Governance	No DMARC reporting visibility on 2 of 3 secondary domains	Aggregate reporting active on all sending domains
Sender Reputation Controls	Shared-IP sending without formal warm-up governance	Documented warm-up and ramp policy for all new sending identities

2. Environment Overview

Northlane Software is a business-to-business SaaS provider headquartered in Austin, Texas, with a secondary office in Dublin, Ireland supporting EMEA revenue operations. The company employs approximately 340 people, including a 38-person Platform Engineering organization, a 54-person combined Sales Development and Account Executive organization operating across six regional pods, a 22-person Demand Generation marketing team, and a 6-person Corporate IT/Systems function reporting to the CTO.

Northlane's revenue organization relies on a modern outbound technology stack layered on top of Google Workspace, which serves as the corporate mail platform for the primary domain. Sales development representatives use Apollo for prospect enrichment and initial sequence construction, with Salesforce serving as the system of record for account and opportunity data. Outbound sending is distributed across two dedicated sending platforms — Instantly and Smartlead — which route mail through secondary domains kept operationally separate from the corporate domain to protect primary-domain sender reputation. SendGrid handles transactional mail (product notifications, password resets, and invoicing) through a dedicated subdomain.

Infrastructure Inventory

Component	Platform / Vendor	Function
Primary Corporate Domain	northlanesoftware.com	Corporate mail, marketing site, brand identity
Corporate Mail Platform	Google Workspace	Employee mailboxes; system of record for corporate mail
Transactional Subdomain	mail.northlanesoftware.com (SendGrid)	Product notifications, password resets, billing
Secondary Domain — EMEA Outbound	northlane-connect.com (Instantly)	EMEA SDR pod cold outbound
Secondary Domain — NA Outbound	northlanehq.io (Smartlead)	North America SDR pod cold outbound
Secondary Domain — Scheduling	meetnorthlane.com (Instantly)	Account Executive demo-scheduling sequences
DNS Provider	Cloudflare (Authoritative DNS)	Zone hosting for all five domains
Enrichment & Sequencing	Apollo	Prospect data enrichment, initial sequence design
CRM / System of Record	Salesforce	Account, contact, and opportunity data

Domain segmentation — the practice of isolating cold outbound sending onto domains separate from the primary corporate domain — is a deliberate strategy Northlane's Revenue Operations team adopted eighteen months ago to protect the corporate domain's sender reputation from the higher bounce and spam-complaint rates inherent to cold prospecting. As documented in Section 11 (Detailed Technical Findings), this strategy is only partially realized in the current environment.

3. Assessment Scope

In Scope

- DNS infrastructure for northlanesoftware.com and all secondary sending domains
- SPF, DKIM, and DMARC configuration and alignment across all sending identities
- MX configuration and inbound mail routing architecture
- Domain architecture and sending-domain segmentation strategy
- Third-party sending service configuration (Apollo, Instantly, Smartlead, SendGrid)
- Vendor dependency mapping and operational ownership
- Deliverability architecture, including shared-IP and warm-up practices
- Authentication alignment between sending platforms and published DNS policy

Out of Scope

- Endpoint security of employee workstations
- Web application security of the Northlane product or marketing site
- Source code review of any Northlane-owned system
- Internal network security and corporate firewall configuration
- Employee security awareness training
- Mail content, copywriting, or sequence messaging review

This assessment is architectural and configuration-focused. It does not constitute a penetration test, a phishing simulation, or a content/compliance review of outbound messaging.

4. Infrastructure Architecture

Northlane's outbound ecosystem is organized around five domains sharing a single Cloudflare-hosted DNS account. The intended architecture routes corporate correspondence exclusively through Google Workspace on the primary domain, transactional mail through a SendGrid-authenticated subdomain, and all cold outbound prospecting through three secondary domains dedicated to specific sales pods. Figure 1 illustrates the intended high-level relationship between these platforms.

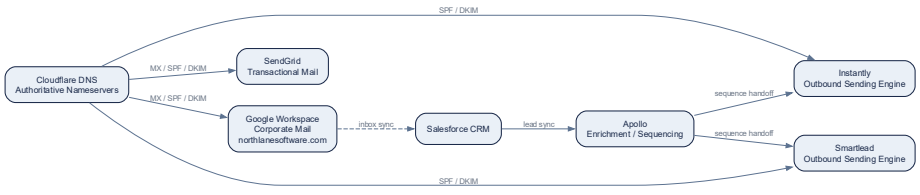

Figure 1 — High-Level Infrastructure Overview

Domain Inventory

Domain	Sending Platform	MX Destination	Isolation Status
northlanesoftware.com	Google Workspace	Google Workspace MX cluster	N/A (corporate domain)
mail.northlanesoftware.com	SendGrid	N/A (send-only subdomain)	Isolated — no inbound MX
northlane-connect.com	Instantly	Vendor-hosted relay (redundant)	Isolated
northlanehq.io	Smartlead	Google Workspace MX cluster (shared)	Not isolated — see Finding CS001-01
meetnorthlane.com	Instantly	Vendor-hosted relay (single record)	Isolated — single point of failure, see CS001-08

Figure 2 maps the vendor relationships underlying this architecture, including the systems that are dependent on Cloudflare DNS as the single source of authentication-record truth for the entire outbound program.

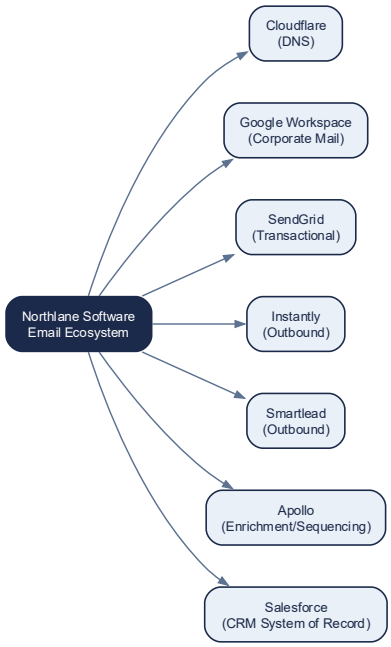

Figure 2 — Third-Party Vendor Relationships

5. Assessment Methodology

Vaixus conducted this assessment using a five-stage methodology consistent with its standard email infrastructure engagement model.

- Discovery Workshop — structured interviews with Revenue Operations, Marketing, and IT stakeholders to document intended architecture, ownership, and prior incidents.
- Passive DNS Reconnaissance — authoritative-record enumeration (dig, nslookup, host) across all in-scope domains and subdomains to establish the as-built configuration.
- Authentication Trace Testing — controlled test messages sent through each sending platform to independent receiving mailboxes, with full header capture and Authentication-Results inspection.
- Vendor Configuration Review — direct review of Google Workspace, SendGrid, Instantly, Smartlead, and Apollo administrative consoles to confirm published DNS records match platform-side configuration.
- Findings Synthesis and Executive Readout — consolidation of findings into severity-rated, business-impact-aligned recommendations, presented to Northlane's CTO and VP of Revenue Operations.

All engineering evidence referenced in this report — DNS records, SMTP transcripts, and Authentication-Results headers — was captured during the reconnaissance and trace-testing stages and is reproduced in the Technical Appendix.

6. Executive Findings Summary

Vaixus identified thirteen findings. Two are rated Critical, four High, five Medium, one Low, and one Informational. The table below summarizes all findings; full technical detail is provided in Section 11.

ID	Finding	Category	Severity
CS001-01	Secondary domain shares corporate MX trust boundary	Domain Architecture	Critical
CS001-02	Primary domain SPF exceeds 10-lookup limit	DNS / Authentication	Critical
CS001-03	DMARC unenforced on primary domain (p=none)	Authentication	High
CS001-04	Shared-IP sending without warm-up governance	Deliverability	High
CS001-05	Duplicate SPF-formatted TXT records on primary domain	DNS	High
CS001-06	Legacy vendor include retained in SPF chain	Vendor Configuration	High
CS001-07	Google Workspace DKIM key still 1024-bit	Authentication	Medium
CS001-08	Single MX record on meetnorthlane.com	Domain Architecture	Medium
CS001-09	Missing DMARC aggregate reporting on 2 domains	Operational Risk	Medium
CS001-10	DKIM selector naming collision across vendors	Authentication	Medium

ID	Finding	Category	Severity
CS001-11	No standardized sending-mailbox ramp policy	Operational Risk	Medium
CS001-12	Inconsistent Reply-To breaks thread continuity	Vendor Configuration	Low
CS001-13	No BIMI record present (blocked by CS001-03)	Security Best Practices	Informational

7. Detailed Technical Findings

Findings are presented in descending order of severity. Each finding follows the evidence → analysis → business impact → recommendation → verification structure applied consistently throughout this report.

CS001-01 — Secondary Outbound Domain Shares Corporate MX Trust Boundary

Severity	**Critical**
Category	Domain Architecture
Reference	Google Workspace Admin — Domain Management; RFC 5321 §5

Evidence.

DNS reconnaissance shows that northlanehq.io, the secondary domain used by Smartlead for North America outbound sending, resolves an MX record set identical to the corporate domain's Google Workspace MX cluster, rather than pointing to Smartlead's reply-handling infrastructure or a domain-specific relay.

```
$ dig MX northlanehq.io +short
1 aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
5 alt2.aspmx.l.google.com.
10 alt3.aspmx.l.google.com.
10 alt4.aspmx.l.google.com.

$ dig MX northlanesoftware.com +short
1 aspmx.l.google.com.
5 alt1.aspmx.l.google.com.
5 alt2.aspmx.l.google.com.
10 alt3.aspmx.l.google.com.
10 alt4.aspmx.l.google.com.
```

Technical Analysis.

Google Workspace administrative records confirm that northlanehq.io was added as a “secondary domain” inside the same Workspace tenant as northlanesoftware.com approximately eighteen months ago, when Northlane's IT team provisioned reply-monitoring aliases for the domain. Adding a domain as a Workspace secondary domain automatically applies the tenant's shared MX configuration to that domain, which is the correct behavior for a domain intended to receive corporate mail — but is

inconsistent with northlanehq.io's intended role as an isolated cold-outbound identity. As a result, any mail addressed to northlanehq.io, including bounce traffic, backscatter, or a spoofed message crafted by a third party, is delivered into the same mail cluster as corporate email rather than being contained within Smartlead's infrastructure.

Business Impact.

This finding directly undermines the domain segmentation strategy that Revenue Operations believes protects the corporate domain's sender reputation. A reputation event on northlanehq.io — for example, a spam-complaint spike from an aggressive prospecting sequence — has a credible path to affect the shared Google Workspace mail cluster, and by extension, corporate deliverability. It also means a spoofed message impersonating northlanehq.io, a domain external recipients have limited familiarity with, would land inside infrastructure trusted by the corporate domain rather than being isolated to vendor-side infrastructure.

Recommendation.

Remove northlanehq.io as a Google Workspace secondary domain and re-provision it as a fully external domain with its own DNS-only MX configuration pointed at Smartlead's dedicated reply-handling relay (consistent with the configuration already in place for northlane-connect.com and meetnorthlane.com). Any reply-monitoring functionality currently dependent on Workspace aliasing should be re-implemented using Smartlead's native unified-inbox reply tracking, which does not require shared MX placement.

Verification Method.

Following remediation, confirm via `dig MX northlanehq.io` that the MX record set no longer matches the corporate domain, and confirm via Google Workspace Admin Console that northlanehq.io no longer appears under Domains → Manage Domains. Send a controlled test message to a northlanehq.io alias and confirm it is received and processed by Smartlead's infrastructure, not a Workspace mailbox.

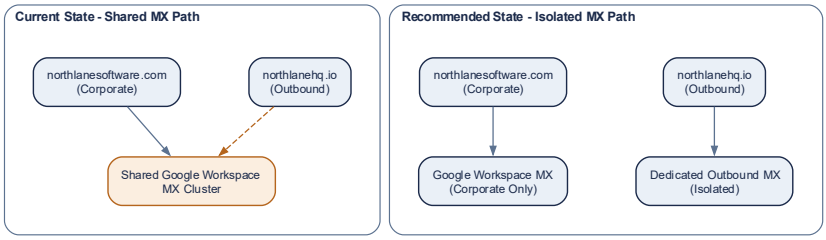

Figure 3 — Domain Segmentation Strategy: Current vs. Recommended State

CS001-02 — Primary Domain SPF Record Exceeds RFC 7208 Ten-Lookup Limit

Severity	**Critical**
Category	DNS / Authentication
Reference	RFC 7208 §4.6.4

Evidence.

The SPF record published for northlanesoftware.com resolves to eleven DNS lookups once all nested includes are expanded, one over the limit defined in RFC 7208 §4.6.4.

```
$ dig TXT northlanesoftware.com +short | grep spf1
"v=spf1 include:_spf.google.com include:sendgrid.net include:mail.reply.io
include:apollo.io ~all"

Lookup expansion:
  _spf.google.com        -> 4 nested lookups
  sendgrid.net            -> 2 nested lookups
  mail.reply.io           -> 2 nested lookups (legacy vendor, see CS001-09)
  apollo.io                -> 2 nested lookups
  TOTAL                    = 10 nested + 1 base lookup = 11
```

Technical Analysis.

RFC 7208 caps SPF evaluation at ten DNS-mechanism lookups; any record requiring more must be evaluated as PERMERROR by a compliant validator. In practice, receiving systems vary: many major consumer mailbox providers apply lenient fallback behavior, but a meaningful subset of enterprise gateways and stricter validators treat PERMERROR as equivalent to a hard fail. Northlane's SDR teams report intermittent bounces and spam-foldering specifically when prospecting into enterprise-gateway-protected domains, which is consistent with this failure mode.

Business Impact.

Corporate correspondence and sales prospecting sent from the primary domain is at risk of unpredictable rejection by exactly the class of enterprise recipients Northlane's SaaS platform targets — mid-market and enterprise buyers with mature email security gateways. This is a plausible direct contributor to the declining outbound performance that prompted this engagement.

Recommendation.

Remove the legacy mail.reply.io include (see CS001-06, Reply.io is no longer in active use) to bring the total lookup count to nine. If future vendor additions are required, flatten static includes where the vendor publishes a fixed IP range, or migrate to SPF macros only where the sending platform explicitly supports them.

Verification Method.

Re-run lookup-count validation using an SPF lint tool (e.g., an RFC 7208-compliant validator) and confirm a result of ten or fewer lookups with no PERMERROR. Send authentication trace tests to a strict enterprise-gateway test mailbox and confirm an explicit SPF Pass result in the Authentication-Results header.

CS001-03 — DMARC Published at p=none With No Path to Enforcement

Severity	**High**
Category	Authentication
Reference	RFC 7489 §6.3

Evidence.

The DMARC record at _dmarc.northlanesoftware.com specifies a monitoring-only policy.

```
$ dig TXT _dmarc.northlanesoftware.com +short
"v=DMARC1; p=none; rua=mailto:dmarc-reports@northlanesoftware.com; fo=1"
```

Technical Analysis.

A DMARC policy of p=none instructs receiving mail systems to take no enforcement action on messages that fail alignment; it provides visibility only. Northlane's Marketing team has requested BIMI (Brand Indicators for Message Identification) to display the corporate logo in supporting inboxes, but BIMI's VMC/logo-display requirements are contingent on DMARC enforcement at p=quarantine or p=reject with a high percentage applied — a prerequisite the current record does not satisfy.

Business Impact.

Beyond blocking the BIMI initiative, p=none provides no protection against spoofing of the corporate domain in phishing attempts directed at customers or prospects, which carries brand-trust and customer-communication risk independent of the BIMI objective.

Recommendation.

Begin a staged DMARC enforcement ramp: move to p=quarantine at pct=25 once aggregate reports confirm all legitimate sending sources (Google Workspace, SendGrid) are correctly aligned, increase to pct=100 over 2–4 weeks, then advance to p=reject following a further monitoring period. This staged approach is addressed in the Remediation Strategy (Section 14).

Verification Method.

Review DMARC aggregate (rua) reports at each ramp stage to confirm zero unexpected alignment failures from legitimate sources before advancing enforcement percentage. Confirm final state via `dig TXT _dmarc.northlanesoftware.com` showing p=reject.

CS001-04 — Shared-IP Outbound Sending Without Formal Warm-Up Governance

Severity	**High**
Category	Deliverability
Reference	M3AAWG Sender Best Common Practices

Evidence.

Smartlead's administrative console confirms northlanehq.io mailboxes are provisioned on Smartlead's shared sending-IP pool rather than dedicated IPs, and Northlane has no documented warm-up schedule governing how sending volume ramps for newly added mailboxes.

Technical Analysis.

Shared-IP sending pools carry reputation influenced by the aggregate behavior of all tenants using the pool, not solely Northlane's own sending practices. Without a warm-up governance policy, individual SDR onboarding has resulted in inconsistent initial send volumes — interview evidence indicates at least two recently onboarded representatives were sending at full sequence volume (60+ messages/day) within their first week, well above commonly recommended warm-up ramps for new sending identities.

Business Impact.

Reputation volatility on the shared pool, compounded by unmanaged internal ramp practices, produces deliverability swings that are difficult to diagnose and are likely contributing to the inconsistent reply-rate patterns Revenue Operations has observed across SDR pods.

Recommendation.

Adopt a documented warm-up policy for all newly provisioned sending mailboxes (recommended: 14-day ramp from 10 to 50 messages/day), and evaluate migrating northlanehq.io to a dedicated IP allocation within Smartlead once monthly send volume justifies the cost, removing exposure to shared-pool reputation events entirely.

Verification Method.

Confirm ramp policy adoption via Smartlead's per-mailbox sending-limit configuration. Track domain-level reputation metrics (Google Postmaster Tools reputation category, where corporate-adjacent) for 30 days post-implementation to confirm reduced volatility.

CS001-05 — Duplicate SPF-Formatted TXT Records on Primary Domain

Severity	High
Category	DNS
Reference	RFC 7208 §3.2

Evidence.

Two separate TXT records beginning with “v=spf1” are published at the root of northlanesoftware.com — the current record referenced in CS001-02, and a legacy record apparently left in place from a prior migration.

```
$ dig TXT northlanesoftware.com +short
"v=spf1 include:_spf.google.com include:sendgrid.net include:mail.reply.io
include:apollo.io ~all"
"v=spf1 include:_spf.google.com ~all"  ; legacy record, pre-dates current vendor stack
```

Technical Analysis.

RFC 7208 §3.2 requires exactly one SPF-formatted TXT record per domain; publishing multiple records is itself a PERMERROR condition independent of the lookup-count issue in CS001-02. The two failure modes compound: even after CS001-02 is remediated, this duplicate-record condition would continue to produce authentication failures until resolved.

Business Impact.

Identical to CS001-02 — unpredictable rejection or spam-foldering of legitimate corporate mail, with the added risk that some validators may select an unpredictable one of the two records, making failures inconsistent and difficult to reproduce during troubleshooting.

Recommendation.

Remove the legacy TXT record entirely, retaining only the current, corrected SPF record produced as part of CS001-02 remediation. Both changes should be deployed together in the same maintenance window.

Verification Method.

Confirm via `dig TXT northlanesoftware.com` that exactly one v=spf1 record is present, and re-validate lookup count per CS001-02.

CS001-06 — Legacy Vendor Include Retained in Primary SPF Chain

Severity	**High**
Category	Vendor Configuration
Reference	RFC 7208 §5.2

Evidence.

The primary domain's SPF record includes mail.reply.io, a sending platform Northlane's Revenue Operations team confirms was fully decommissioned fourteen months ago when the team consolidated onto Apollo, Instantly, and Smartlead.

Technical Analysis.

The include remains authorized to send on behalf of northlanesoftware.com despite no longer being an active vendor relationship, which is both an unnecessary lookup contributor to CS001-02 and an unmanaged trust grant — if Reply.io's published SPF range were ever reassigned or compromised at the vendor level, it would retain the ability to send authenticated mail as Northlane.

Business Impact.

Directly contributes to the Critical SPF lookup-limit finding (CS001-02) and represents an avoidable, unreviewed authentication grant to a vendor no longer under active contract.

Recommendation.

Remove the mail.reply.io include as part of the CS001-02 remediation change. Establish a quarterly SPF include review as part of ongoing vendor offboarding procedure to prevent recurrence.

Verification Method.

Confirm removal via updated SPF record inspection (see CS001-02 verification). Add SPF review as a standing checklist item in Northlane's vendor offboarding runbook.

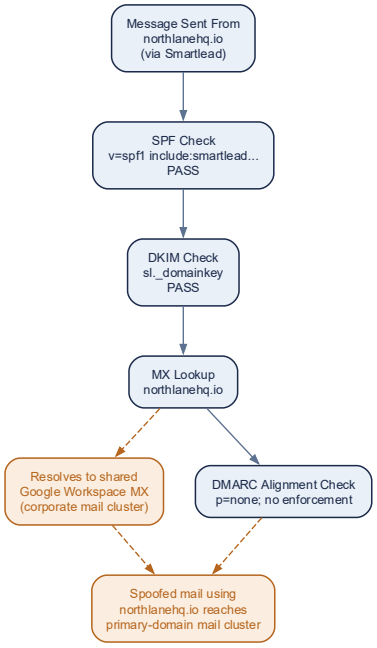

Figure 4 — DNS Authentication Flow — northlanehq.io

CS001-07 — Google Workspace DKIM Signing Key Remains 1024-Bit

Severity	Medium
Category	Authentication
Reference	RFC 6376 §3.3.3

Evidence.

The active DKIM selector for the primary domain publishes a 1024-bit RSA key, despite Google Workspace having supported 2048-bit key generation for corporate domains for several years.

```
$ dig TXT google._domainkey.northlanesoftware.com +short
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..." (1024-bit modulus)
```

Technical Analysis.

1024-bit RSA keys remain technically functional but fall below current best-practice guidance, which recommends 2048-bit as the minimum for new DKIM deployments given advances in factorization capability over the key's originally intended service life.

Business Impact.

No immediate deliverability impact was observed; this is a forward-looking hardening item rather than an active failure. Some receiving systems are beginning to deprecate trust in sub-2048-bit keys, which could become an authentication risk without remediation.

Recommendation.

Generate a new 2048-bit DKIM key pair within Google Workspace Admin Console, publish the new selector, confirm propagation, and rotate signing to the new selector before revoking the legacy 1024-bit key.

Verification Method.

Confirm new key length via `dig TXT` on the new selector, then confirm DKIM Pass with the new selector referenced in the Authentication-Results header of a controlled test message before decommissioning the old selector.

CS001-08 — Single MX Record on meetnorthlane.com

Severity	Medium
Category	Domain Architecture
Reference	RFC 5321 §5.1

Evidence.

meetnorthlane.com publishes a single MX record with no secondary/backup preference value.

```
$ dig MX meetnorthlane.com +short
10 mx1.instantly-mail.net.
```

Technical Analysis.

A single MX record creates a single point of failure for inbound reply handling on this domain: any outage or maintenance event at the vendor's sole relay results in inbound reply mail (including out-of-office and bounce traffic from AE demo-scheduling sequences) being undeliverable rather than queued to an alternate path.

Business Impact.

Account Executive demo-scheduling sequences are time-sensitive; an inbound outage during an active scheduling window risks lost prospect replies at a late, high-value stage of the sales funnel.

Recommendation.

Confirm with Instantly whether a secondary relay endpoint is available for redundant MX configuration; if not natively offered, evaluate a low-cost backup MX service that queues mail during primary relay unavailability.

Verification Method.

Confirm via `dig MX meetnorthlane.com` that two MX records with distinct preference values are present, and perform a controlled failover test if a backup relay is implemented.

CS001-09 — Missing DMARC Aggregate Reporting on Two Secondary Domains

Severity	Medium
Category	Operational Risk
Reference	RFC 7489 §6.2

Evidence.

northlane-connect.com and meetnorthlane.com both publish DMARC records without a rua (aggregate reporting) address.

```
$ dig TXT _dmarc.northlane-connect.com +short
"v=DMARC1; p=none;"
$ dig TXT _dmarc.meetnorthlane.com +short
"v=DMARC1; p=none;"
```

Technical Analysis.

Without rua reporting, Northlane has no visibility into authentication pass/fail rates or unauthorized use of these domains — the same class of blind spot noted for the primary domain in CS001-03, but with no reporting whatsoever rather than unenforced-but-visible reporting.

Business Impact.

Reduces Northlane's ability to detect domain spoofing or misconfiguration on these lower-visibility secondary domains, and removes the data needed to safely plan a future enforcement ramp on them.

Recommendation.

Add a rua reporting address to both domains' DMARC records, directed to the same reporting mailbox used for the primary domain, to consolidate monitoring.

Verification Method.

Confirm updated records via `dig TXT` and confirm receipt of aggregate reports within 24–48 hours of the first reporting-period boundary following the change.

CS001-10 — DKIM Selector Naming Collision Across Independent Vendors

Severity	Medium
Category	Authentication
Reference	RFC 6376 §3.1

Evidence.

Smartlead's default DKIM selector for northlanehq.io and Instantly's default selector for northlane-connect.com are both published as “s1”, despite being entirely independent keys managed by unrelated vendors.

Technical Analysis.

This is not a security flaw — selectors are scoped per-domain and the keys themselves are distinct — but it creates operational ambiguity for anyone reviewing DNS records or automated monitoring tooling across Northlane's domain portfolio, increasing the risk of a rotation or troubleshooting error where a selector reference is applied to the wrong domain.

Business Impact.

Primarily an operational maintainability concern rather than a direct deliverability or security risk; the impact is increased time-to-diagnose during any future authentication incident and elevated risk during key rotation.

Recommendation.

Where platform configuration allows custom selector naming, standardize on a vendor-prefixed convention (e.g., sl1._domainkey for Smartlead, inst1._domainkey for Instantly) across all secondary domains to eliminate ambiguity.

Verification Method.

Confirm updated selector names via `dig TXT` against each domain and update internal documentation to reference the new selector naming convention.

CS001-11 — No Standardized Ramp Policy for Newly Provisioned Sending Mailboxes

Severity	**Medium**
Category	Operational Risk
Reference	M3AAWG Sender Best Common Practices

Evidence.

Interviews with Revenue Operations confirm that initial sending-volume limits for new SDR mailboxes are set manually and vary by whoever performs the onboarding, with no written policy.

Technical Analysis.

This finding is closely related to CS001-04 but is distinct in scope: CS001-04 addresses shared-IP pool risk, while this finding addresses the absence of a repeatable internal process regardless of IP allocation strategy.

Business Impact.

Inconsistent onboarding practice makes deliverability outcomes difficult to attribute and complicates root-cause analysis when a specific pod or representative experiences a reputation event.

Recommendation.

Formalize the warm-up ramp defined in CS001-04 as a written onboarding checklist item owned by Revenue Operations, with Smartlead and Instantly per-mailbox send-limit settings configured as part of new-hire IT provisioning rather than left to manual SDR judgment.

Verification Method.

Confirm checklist adoption via Revenue Operations onboarding documentation review; spot-check three most-recently onboarded mailboxes' configured send limits against the documented ramp schedule.

CS001-12 — Inconsistent Reply-To Configuration Breaks Thread Continuity

Severity	Low
Category	Vendor Configuration
Reference	RFC 5322 §3.6.2

Evidence.

A sample of Instantly sequences reviewed during this engagement shows outbound messages sent from northlane-connect.com domains while the Reply-To header routes back to personal @northlanesoftware.com accounts, tracking back to a subset of representatives migrating from a legacy manual prospecting process.

Technical Analysis.

When a prospect replies, the message routes to the representative's personal corporate inbox rather than remaining inside Instantly's tracked conversation view, breaking analytics attribution and creating a risk that replies are missed if the representative does not separately monitor that inbox.

Business Impact.

Reduces the reliability of reply-rate reporting used by Revenue Operations for pipeline forecasting, and creates a minor but real risk of missed prospect replies at pods still using the legacy Reply-To habit.

Recommendation.

Standardize Reply-To configuration across all Instantly and Smartlead sequences to match the From domain, consistent with platform default behavior, and communicate the change to affected representatives.

Verification Method.

Sample five sequences per pod post-remediation and confirm Reply-To matches From domain in each case.

CS001-13 — No BIMI Record Present

Severity	Informational
Category	Security Best Practices
Reference	BIMI Group Specification

Evidence.

No BIMI (Brand Indicators for Message Identification) TXT record exists at default._bimi .northlanesoftware.com.

Technical Analysis.

This is expected given the current DMARC posture documented in CS001-03; BIMI publication is contingent on DMARC enforcement and is not actionable until that prerequisite is satisfied.

Business Impact.

No current impact. Recorded for visibility as a future-state marketing objective once CS001-03 is remediated.

Recommendation.

Revisit BIMI implementation once DMARC reaches p=quarantine at pct=100 or higher, in coordination with Northlane's Marketing team and a Verified Mark Certificate (VMC) provider if logo display in Gmail is desired.

Verification Method.

No verification required at this time; re-assess as part of the Phase 3 remediation review defined in Section 14.

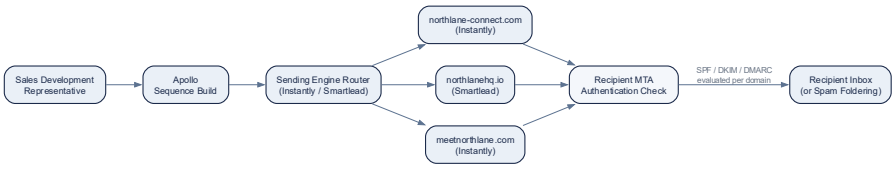

Figure 5 — Outbound Mail Flow

8. Risk Prioritization

Findings are prioritized below by a combination of severity and remediation effort, establishing the sequencing basis for the Remediation Strategy in Section 14.

Priority	Finding ID	Severity	Effort	Rationale
1	CS001-01	Critical	Low	Single Workspace admin change; removes shared trust boundary immediately
2	CS001-05	High	Low	Deploy alongside CS001-02 in same DNS change window
3	CS001-02	Critical	Low	Single DNS record edit; highest deliverability impact per unit effort
4	CS001-06	High	Low	Bundled with CS001-02 change
5	CS001-03	High	Medium	Requires staged ramp over several weeks; cannot be rushed safely
6	CS001-04	High	Medium	Requires warm-up policy authoring and possible dedicated-IP evaluation

Priority	Finding ID	Severity	Effort	Rationale
7	CS001-07	Medium	Low	Key generation and rotation is low-effort but requires a cutover window
8	CS001-09	Medium	Low	Single DNS record edit per domain
9	CS001-11	Medium	Medium	Requires new process documentation and IT provisioning change
10	CS001-08	Medium	Medium	Dependent on vendor-side redundant relay availability
11	CS001-10	Medium	Low	Cosmetic/operational; scheduled with other DNS work
12	CS001-12	Low	Low	Sequence-level configuration change per representative
13	CS001-13	Informational	N/A	Deferred until CS001-03 reaches sufficient enforcement

9. Business Impact Analysis

The findings in this report collectively translate into three business-level consequences for Northlane's revenue organization.

Revenue Pipeline Risk

CS001-02 and CS001-05 create intermittent, hard-to-diagnose delivery failures against exactly the enterprise-gateway-protected recipients that represent Northlane's target buyer profile. Given that outbound email is the primary top-of-funnel motion for a 54-person revenue organization, even a partial delivery failure rate against enterprise domains represents a direct and likely material drag on pipeline generation — consistent with the decline that prompted this engagement.

Brand Trust and Spoofing Exposure

CS001-01 and CS001-03 together mean the corporate domain and one secondary domain both lack a hardened trust boundary: the corporate domain has no enforcement policy against spoofing, and the secondary domain's inbound path is not isolated from corporate infrastructure. Neither condition indicates an active incident, but both leave Northlane's brand more exposed to impersonation than its Revenue Operations team currently believes, given its stated segmentation strategy.

Operational Maintainability

CS001-08, CS001-10, CS001-11, and CS001-12 do not individually threaten deliverability but collectively represent the kind of unmanaged operational drift that produces future incidents. Absent reporting visibility, inconsistent naming, and ad hoc onboarding practice compound over time as the sales organization continues to scale, and are most efficiently addressed now, while the vendor footprint remains at its current size.

10. Remediation Strategy

Remediation is organized into three phases sequenced by urgency and dependency.

Phase 1 — Immediate (Weeks 1–2)

Action	Addresses	Expected Result	Operational Considerations
Remove northlanehq.io as Workspace secondary domain; re-provision isolated MX	CS001-01	Secondary domain fully isolated from corporate mail cluster	Requires brief reply-monitoring cutover; coordinate with Smartlead admin
Correct primary domain SPF record: remove legacy TXT, remove Reply.io include	CS001-02, CS001-05, CS001-06	SPF resolves to ≤ 9 lookups; single valid record	Single DNS change window; no sending downtime required
Begin staged DMARC enforcement ramp on primary domain	CS001-03	DMARC reaches p=quarantine, pct=100	Requires weekly aggregate-report review; do not rush pct increases
Author and adopt sending-mailbox warm-up policy; evaluate dedicated IP for northlanehq.io	CS001-04, CS001-11	Consistent, documented ramp for all new mailboxes	Coordinate with Smartlead account team on dedicated IP pricing
Rotate Google Workspace DKIM key to 2048-bit	CS001-07	DKIM signing on hardened key length	Brief dual-key overlap period recommended during cutover
Add DMARC rua reporting to remaining secondary domains	CS001-09	Full reporting visibility across all domains	No sending impact; DNS-only change

Phase 3 — Operational Hardening (Weeks 7–12)

Action	Addresses	Expected Result	Operational Considerations
Standardize DKIM selector naming across vendors	CS001-10	Unambiguous selector-to-vendor mapping	Coordinate rollout with next scheduled key rotation
Evaluate/implement backup MX for meetnorthlane.com	CS001-08	Redundant inbound path for AE scheduling domain	Contingent on vendor-offered redundancy options
Standardize Reply-To across all active sequences	CS001-12	Reply thread continuity restored	Representative communication and brief retraining
Advance primary domain DMARC to p=reject; revisit BIMI	CS001-03, CS001-13	Full enforcement; BIMI prerequisite satisfied	Contingent on clean aggregate reports through Phase 2

11. Verification Plan

Each remediation action is paired with a specific verification procedure to confirm successful implementation before the associated finding is considered closed.

Finding	Verification Method	Success Criterion
CS001-01	DNS MX lookup + Workspace Admin Console review	MX no longer matches corporate cluster; domain absent from Workspace domain list
CS001-02 / CS001-05	SPF lint validation + trace test to strict gateway	≤ 10 lookups; single record; explicit SPF Pass in Authentication-Results
CS001-03	Weekly DMARC aggregate report review	Zero unexpected alignment failures at each ramp stage
CS001-04	Smartlead per-mailbox send-limit audit	All active mailboxes conform to documented ramp schedule
CS001-06	SPF record inspection	mail.reply.io include absent
CS001-07	DKIM selector trace test	New 2048-bit selector referenced in Authentication-Results with Pass result
CS001-08	Controlled failover test (if backup MX implemented)	Inbound mail continues during primary relay simulated outage
CS001-09	DMARC aggregate report receipt confirmation	Reports received within 48 hours of first reporting boundary
CS001-10	DNS selector inspection across all secondary domains	Vendor-prefixed selector naming applied consistently
CS001-11	Onboarding documentation + mailbox spot-check	3 most recent mailboxes conform to ramp policy
CS001-12	Sequence sampling (5 per pod)	Reply-To matches From domain in all sampled sequences

12. Final Assessment

Northlane's outbound infrastructure reflects a revenue organization that scaled its sending stack faster than it formalized DNS and authentication governance — a common and fully remediable pattern in fast-growing B2B SaaS environments. Vaixus rates Northlane's current infrastructure maturity as Developing (Level 2 of 5 on Vaixus's internal maturity scale), with a clear and achievable path to Managed (Level 4) within the twelve-week remediation window defined in this report.

The two Critical findings — CS001-01 and CS001-02 — are both low-effort, single-change remediations and should be treated as immediate priorities independent of the broader roadmap. Their resolution alone is likely to produce a measurable improvement in the enterprise-domain deliverability that Revenue Operations flagged as the original trigger for this engagement.

No finding in this report indicates an active security compromise. All findings are configuration, architectural, or process gaps consistent with organic infrastructure growth, and all are remediable without a change of vendor or an interruption to active sending campaigns.

13. References

- RFC 5321 — Simple Mail Transfer Protocol
- RFC 5322 — Internet Message Format
- RFC 6376 — DomainKeys Identified Mail (DKIM) Signatures
- RFC 7208 — Sender Policy Framework (SPF) for Authorizing Use of Domains in Email
- RFC 7489 — Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- M3AAWG Sender Best Common Practices, Messaging, Malware and Mobile Anti-Abuse Working Group
- BIMI Group — Brand Indicators for Message Identification Specification
- Google Workspace Admin Help — Domain Management and Email Authentication

14. Technical Appendix

A. Full DNS Record Set (Synthetic Laboratory Environment)

northlanesoftware.com

Record Type	Name	Value
A	@	76.223.105.230
MX	@	1 aspmx.l.google.com / 5 alt1 / 5 alt2 / 10 alt3 / 10 alt4
TXT (SPF, current)	@	v=spf1 include:_spf.google.com include:sendgrid.net include:mail.reply.io include:apollo.io ~all
TXT (SPF, legacy — duplicate)	@	v=spf1 include:_spf.google.com ~all
TXT (DKIM)	google._domainkey	v=DKIM1; k=rsa; p=(1024-bit key, truncated)
TXT (DMARC)	_dmarc	v=DMARC1; p=none; rua=mailto:dmarc-reports@northlanesoftware.com; fo=1
NS	@	elle.ns.cloudflare.com / hank.ns.cloudflare.com
SOA	@	elle.ns.cloudflare.com admin.northlanesoftware.com (serial auto)

northlanehq.io (Pre-Remediation)

Record Type	Name	Value
MX	@	1 aspmx.l.google.com / 5 alt1 / 5 alt2 / 10 alt3 / 10 alt4 (shared — see CS001-01)
TXT (SPF)	@	v=spf1 include:_spf.google.com include:smartlead.ai ~all
TXT (DKIM)	s1._domainkey	v=DKIM1; k=rsa; p=(2048-bit key, truncated)
TXT (DMARC)	_dmarc	v=DMARC1; p=none;

northlane-connect.com / meetnorthlane.com

Record Type	Domain	Value
MX	northlane-connect.com	10 mx1.instantly-mail.net / 20 mx2.instantly-mail.net
MX	meetnorthlane.com	10 mx1.instantly-mail.net (single record — see CS001-08)
TXT (SPF)	both domains	v=spf1 include:instantly.ai ~all
TXT (DKIM)	both domains	s1._domainkey — v=DKIM1; k=rsa; p=(2048-bit key, truncated)
TXT (DMARC)	both domains	v=DMARC1; p=none; (rua absent — see CS001-09)

B. Sample Authentication-Results Header (northlanehq.io Trace Test)

```
Authentication-Results: mx.receivingtest.example;
  spf=pass (sending domain northlanehq.io designates 168.245.x.x as permitted sender)
    smtp.mailfrom=bounce.smartlead.ai;
  dkim=pass header.i=@northlanehq.io header.s=s1 header.b=7fA1qD9m;
  dmarc=none (p=NONE sp=NONE dis=NONE) header.from=northlanehq.io
```

C. Command Output — SPF Lint (Post-Remediation, Simulated)

```
$ spf-lint northlanesoftware.com
Record: v=spf1 include:_spf.google.com include:sendgrid.net include:apollo.io ~all
Total DNS lookups: 9
Result: VALID (within RFC 7208 limit)
```

D. Vendor Configuration Inventory

Vendor	Role	Domains Serviced	Admin Owner
Google Workspace	Corporate mail	northlanesoftware.com	IT / Corporate Systems
SendGrid	Transactional mail	mail.northlanesoftware.com	Platform Engineering
Apollo	Enrichment & sequencing	N/A (upstream of sending platforms)	Revenue Operations
Instantly	Outbound sending	northlane-connect.com, meetnorthlane.com	Revenue Operations
Smartlead	Outbound sending	northlanehq.io	Revenue Operations
Salesforce	CRM system of record	N/A	Revenue Operations
Cloudflare	Authoritative DNS	All domains	IT / Corporate Systems