MANDOS CYBER

POSITIONING REPORT

PREPARED FOR

ShieldMail Inc.

Email Security | AI Threat Detection | Email DLP

Mandos Positioning Analysis: Website Messaging & Security Buyer Readiness

JULY 2026

SAMPLE REPORT

This is a sample report created with entirely fictional company names and data. Its purpose is to illustrate the structure, depth, and quality of our Mandos Positioning Reports. All company names (ShieldMail, MailFortress, InboxGuard, ThreatFilter, SecureFlow), metrics, scores, and recommendations shown here are fabricated examples.

Your actual report will be built using real data from the Mandos Cyber database (3,200+ companies, 8,500+ products), live website analysis, competitive intelligence, and the Mandos Framework, developed from 13 years of enterprise security procurement experience.

SECTION 01

Executive Summary & Scoring Matrix

ANALYSIS LENS

This report evaluates ShieldMail's market positioning through the CISO's lens, the perspective of a Chief Information Security Officer evaluating the product for enterprise security procurement. All scores, assessments, and recommendations reflect what a CISO and their cybersecurity team would think, ask, and require during a vendor evaluation. While the company may currently sell to different buyer personas (IT Managers, CTOs at mid-market companies), our analysis specifically measures readiness for CISO-level scrutiny.

ShieldMail Positioning Score Card (Source: Mandos Cyber)

SCORING MATRIX

DIMENSION	WEIGHT	SCORE	ASSESSMENT
Value Proposition Clarity	20%	7/10	Strong headline with clear outcome. AI positioning is functional but not differentiated.

DIMENSION	WEIGHT	SCORE	ASSESSMENT
Competitive Differentiation	20%	4/10	No comparison pages; invisible against well-funded AI-native competitors.
Trust Signals & Social Proof	15%	5/10	SOC 2 + ISO 27001 strong; missing case studies with quantified outcomes.
CISO Buyer Fit	15%	6/10	Language targets security teams; needs stronger enterprise proof points.
Technical Credibility	10%	7/10	API docs and integration guide publicly accessible. Architecture page needed.
Website Copy Quality	10%	6/10	Some strong lines; overall too feature-heavy, not enough outcome-focused copy.
Pricing & Packaging	10%	3/10	No pricing page. Complete black box for CISOs doing budget modeling.

Verdict

ShieldMail scores 5.8/10 overall, placing it Below CISO Threshold. The product shows genuine technical depth (behavioral AI detection, strong compliance posture, solid integration documentation) but the website fails to convert this into CISO confidence. A CISO evaluating ShieldMail today would see a promising early-stage vendor but would struggle to answer three critical questions: How is this different from InboxGuard? What will it cost me? Who else at my scale is using it? Until those questions are answered on the website, ShieldMail will lose competitive evaluations before reaching the demo stage.

Top 3 Priorities

- **1. Add a pricing page with at least indicative tiers.** Even 'Starting at $X/mailbox/month' removes the single biggest friction point for CISOs doing vendor shortlisting.
- **2. Publish 2-3 customer case studies with quantified outcomes.** Named companies with specific metrics (detection rate improvement, false positive reduction, time to deploy) transform credibility.
- **3. Create competitive differentiation content.** Build 'ShieldMail vs InboxGuard' and 'ShieldMail vs Microsoft Defender' pages. CISOs are already comparing; own the narrative.

SECTION 02

Company Profile

Company Name	ShieldMail Inc.
Founded	2022
Headquarters	San Francisco, CA
Category	Email Security, Email DLP
Employees	~28
Stage	Seed ($4.2M total funding)
Investors	Meridian Ventures, Apex Cyber Fund, 2 angel investors
Product Focus	AI-native email security and DLP for M365 & Google Workspace
Current Tagline	"Catch the threats your gateway already missed"
Primary CTA	"Book a Demo"
Pricing Model	Not publicly disclosed; demo-gated
Mandos Cyber Listing	Not listed

SECTION 03

Homepage Messaging Analysis

3.1 Headline Assessment

CURRENT HEADLINE

"Catch the threats your email gateway already missed"

Score: 7/10. Strong, specific, and confrontational in the right way. It implies the buyer already has security (gateway) and it is not enough. A CISO reads this and immediately wonders 'What am I missing?' However, it doesn't specify what ShieldMail does differently to catch those threats. Adding the mechanism (behavioral AI, contextual analysis) would strengthen it.

THE 5-SECOND TEST

A CISO landing on this page would understand: 'This is a supplemental email security product that catches what my current tools miss.'

They would NOT understand: 'How exactly does it work? What is the detection methodology? What size companies use it?'

They would assume: 'This is a Series A startup trying to compete with InboxGuard and MailFortress. I should check if the price is worth layering another tool.'

3 ALTERNATIVE HEADLINES

- **Pain-point lead:** "Your gateway blocked 10,000 emails this month. It missed the one that matters." (Creates urgency with specificity.)
- **Outcome lead:** "98.9% phishing detection. Zero regex rules. Live in 15 minutes." (Leads with verified metrics and deployment speed.)
- **Category claim:** "Context-aware email security that thinks like your SOC analyst." (Differentiates from rules-based competitors.)

3.2 Subheadline & Supporting Copy

"AI-powered email protection that detects sophisticated phishing, BEC, and data exfiltration in real-time."

Functional but generic. By 2026, every email security vendor claims AI-powered, real-time detection. The subheadline should do more heavy lifting on differentiation: what makes ShieldMail's detection better? Consider: 'Behavioral analysis of sender context, email content, and recipient patterns. No rules to write. No thresholds to tune.'

3.3 Above-the-Fold Verdict

Visible before scrolling: headline, subheadline, 'Book a Demo' CTA, and a customer logo bar with 6 logos. The logo bar includes recognizable mid-market brands, which signals product-market fit. Missing: a quantified proof point (detection rate, deployment time, emails protected). One strong number above the fold would significantly increase CISO confidence.

3.4 Full Page Flow Analysis

Section 1, Hero: Standard headline + CTA. Effective but could be stronger with a proof point.

Section 2, Customer logos: Good selection of mid-market brands. Descriptions should focus on security outcomes, not company descriptions.

Section 3, 'How it works' section: Clean three-step flow (Connect, Detect, Protect). Good structure but lacks depth for technical CISOs.

Section 4, Threat type showcase: Lists BEC, credential phishing, supply chain attacks. Good category coverage but needs real detection examples.

Section 5, Traditional vs ShieldMail comparison: Effective visual concept but lacks specifics. No detection rates, no real examples, no data.

Section 6, DLP section: '50+ data types' is specific. 'Without regex' is a genuine differentiator against legacy DLP. This content should be more prominent.

Section 7, Integration section: 'Go live in 15 minutes' and 'No MX changes' are strong deployment claims. These should be in the hero, not section 7.

Section 8, Blog posts: Threat intelligence content shows real expertise. Buried too deep; most visitors never reach this section.

Overall: The page tells a coherent story but the strongest content (DLP differentiator, deployment speed, threat intelligence) is below the fold. The Problem > Solution > Proof > CTA framework exists but needs tightening.

SECTION 04

Website Copy Deep Dive

What Works

- **"Thinks like an attacker. Acts like an analyst."** Communicates the value proposition better than the headline. Specific to security, implies behavioral analysis, and is memorable.
- **"No MX changes, no risk, no migration."** Addresses the #1 deployment objection for email security. CISOs hate MX record changes because they create outage risk.
- **"50+ sensitive data types detected without a single regex rule"** Specific, quantified, and differentiating. This is copy that sells.
- **"98.9% phishing effectiveness rate" (Trust Center)** Verified by independent audit. This number is nowhere on the homepage. This is the single biggest missed opportunity.

What Needs Work

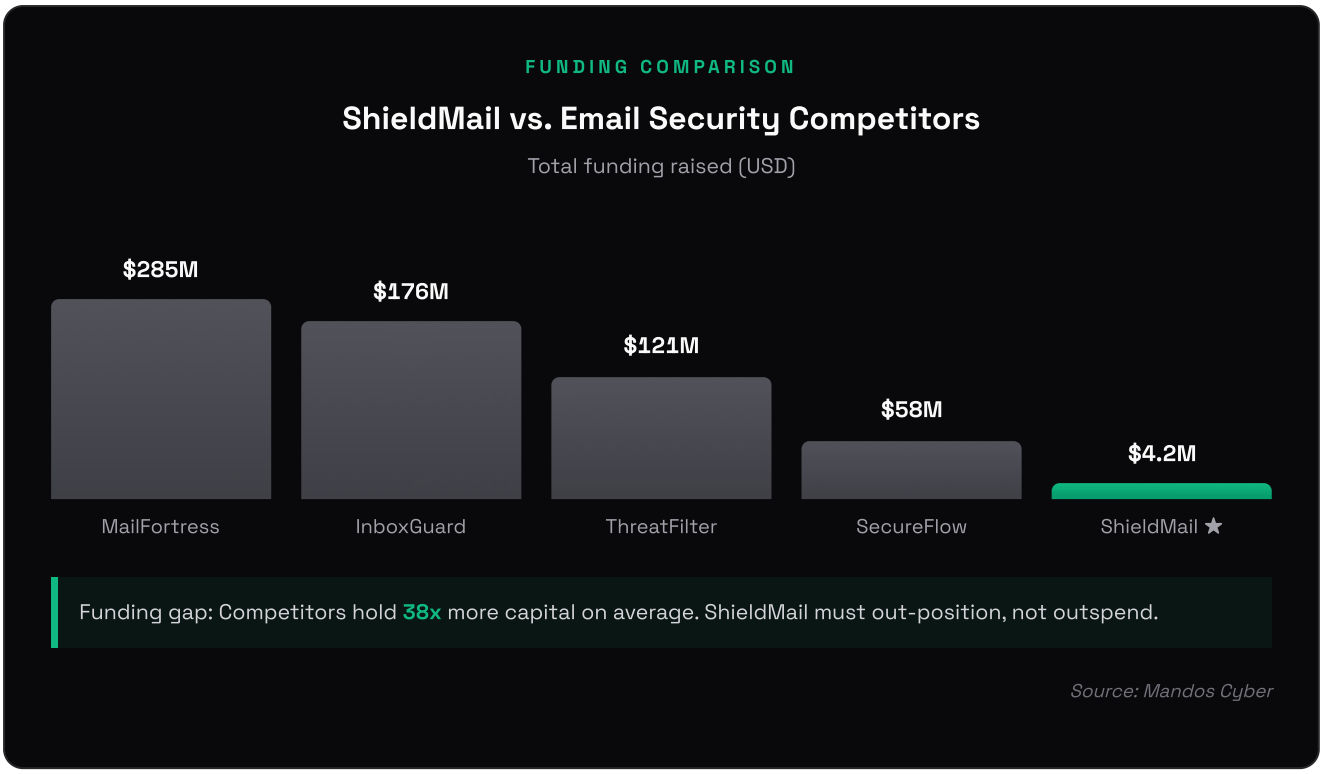
- **"AI-powered protection for the modern enterprise"** Generic. Every competitor says this. Rewrite: 'Behavioral email security that catches what rules-based tools miss.'
- **"Comprehensive email security solution"** Says nothing. Rewrite: 'Phishing detection, BEC prevention, and email DLP in one platform. 15-minute deployment.'
- **"Trusted by leading companies"** Empty without proof. Rewrite: 'Protecting 2M+ mailboxes across fintech, healthcare, and SaaS.'
- **Homepage title tag: "AI Email Security Platform"** Generic SEO. Should be: 'ShieldMail | Behavioral Email Security for M365 & Google Workspace.'

Language Register Assessment

CURRENT LANGUAGE	READS AS	CISO-LEVEL EQUIVALENT
"AI-powered protection"	Generic vendor claim	"Behavioral AI that detects what rules miss"
"Advanced threat detection"	Meaningless qualifier	"Catches BEC attacks your SEG missed"
"Comprehensive solution"	Marketing filler	"Phishing + BEC + DLP in one deployment"
"Leading companies trust us"	Unsubstantiated	"Protecting 2M mailboxes across 40 enterprises"
"Real-time protection"	Expected baseline	"<200ms detection, zero queuing"

SECTION 05

Competitive Differentiation



Funding Comparison: ShieldMail vs. Email Security Competitors (Source: Mandos Cyber)

COMPANY	FOUNDED	EMPLOYEES	HQ	G2 SCORE	FUNDING
MailFortress	2015	842	Boston, MA	4.6	$285M
InboxGuard	2018	534	San Francisco	4.7	$176M
ThreatFilter	2014	312	Tel Aviv	4.4	$121M
SecureFlow	2019	178	New York	4.3	$58M
ShieldMail ★	2022	28	San Francisco	4.2	$4.2M

Competitive Landscape: Key Email Security Players (Source: Mandos Cyber)

ShieldMail competes against firms with **10-30x** more employees and **14-68x** more funding. Positioning, not resources, will determine market capture.

Positioning Gap Analysis

ShieldMail operates in one of the most competitive cybersecurity categories. Email security is dominated by well-funded incumbents (MailFortress at $285M) and fast-growing AI-native challengers (InboxGuard at $176M). The funding gap is severe: ShieldMail's $4.2M seed puts it at roughly 38x less capital than the average competitor. This means ShieldMail cannot compete on brand awareness, sales team size, or analyst coverage. It must compete on positioning clarity, deployment speed, and buyer experience.

THE 'WHY NOT THEM?' TEST

Can a CISO, after reading only the ShieldMail website, articulate why to choose ShieldMail over InboxGuard? No. The website makes no competitive claims. There are no comparison pages, no migration guides from competing products, no 'vs' content. A CISO researching email security would find ShieldMail's website but have no framework to compare it against the 5+ vendors they are already evaluating.

NATIVE/PLATFORM THREAT

Microsoft Defender for Office 365, included in M365 E5 licenses, is the biggest competitive threat. Many CISOs will ask: 'Why do I need ShieldMail if I already have Defender?' The website partially addresses this in the comparison section, but there is no dedicated page explaining why native M365 protection is insufficient. This is table-stakes content for email security vendors.

MISSING COMPETITIVE CONTENT

- No 'ShieldMail vs InboxGuard' comparison page
- No 'ShieldMail vs Microsoft Defender' comparison page
- No 'Alternative to MailFortress' migration page
- No competitive feature matrix
- No 'Why switch from legacy SEG' content

SECTION 06

CISO Buyer Check

CISO BUYER CHECK

Security Buyer Readiness Assessment

What CISOs verify before engaging a security vendor

- ✓ SOC 2 Type II Certification: Active certification displayed on Trust Center page
- ✓ ISO 27001:2022: Current certification with audit date visible
- ✓ Customer Logos: 6 named companies with recognizable brands displayed
- ✓ Integration Documentation: API docs and deployment guide publicly accessible
- ~ G2 Reviews: Listed on G2 with 8 reviews (below confidence threshold)
- ~ Case Studies: 2 case studies present but lacking quantified outcomes
- ✗ Transparent Pricing: No pricing page; demo-gated pricing model
- ✗ Analyst Coverage: Not mentioned in any Gartner, Forrester, or IDC reports
- ✗ Competitor Comparison Pages: No "vs" pages or competitive positioning content
- ✗ Named Customer Testimonials: No attributed quotes from security leaders at customer organizations

Source: Mandos Cyber

CISO Buyer Check: Security Buyer Readiness Assessment (Source: Mandos Cyber)

Before requesting a demo, a CISO will: (1) Check G2 for reviews, (2) Search 'ShieldMail vs InboxGuard,' (3) Look for SOC 2/ISO 27001 on the website, (4) Ask their network on LinkedIn or Slack channels, (5) Check analyst reports. ShieldMail passes on certifications but fails on review volume, comparison content, and analyst coverage.

TRUST SIGNAL	PRESENT?	QUALITY	CISO IMPACT
SOC 2 Type II	Yes	Strong	Passes procurement checklist
ISO 27001:2022	Yes	Strong	Required for EU/global deals
Customer Logos	Yes	Strong	6 recognizable mid-market brands
Integration Docs	Yes	Strong	API docs publicly accessible
G2 Reviews	Yes	Weak	8 reviews, below confidence threshold of 20+
Case Studies	Yes	Weak	2 present but lacking quantified outcomes
Transparent Pricing	No	Missing	CISOs skip vendors they cannot budget for

TRUST SIGNAL	PRESENT?	QUALITY	CISO IMPACT
Analyst Coverage	No	Missing	No Gartner/Forrester/IDC mentions found
Named Testimonials	No	Missing	No attributed CISO quotes on the website
Comparison Pages	No	Missing	Loses SEO traffic and evaluation context

SECTION 07

ICP Fit Analysis

Current ICP (Evidence-Based)

SIGNAL	EVIDENCE	IMPLIED ICP
Customer logos	Mid-market SaaS and fintech brands	US mid-market, 200-1000 employees
Demo form	Company size field, no self-serve	Sales-led motion for 100+ seat deals
Pricing	Demo-gated, no self-serve	Enterprise buyers comfortable with sales process
Copy language	Technical, feature-focused	Security teams and IT leadership
Integrations	M365 + Google Workspace	Cloud-native organizations

Target ICP (Product Capability)

Based on product capability, ShieldMail could serve:

- **Global mid-market companies (200-2000 employees)** using M365 or Google Workspace who need layered email security beyond native protection.
- **Regulated industries (fintech, healthcare, legal)** where email DLP is a compliance requirement, not a nice-to-have.
- **Companies replacing legacy SEGs** with API-based solutions that do not require MX changes.

Gap Analysis

ShieldMail's website speaks to security engineers but the buying decision is made by CISOs and VPs of Security. The copy needs to elevate from 'here is what our product does' to 'here is the business outcome for your security program.' Every feature claim should connect to a CISO-level metric: risk reduction, incident response time, compliance coverage, or cost per protected mailbox.

SECTION 08

Quick Wins (This Week)

IMPLEMENTABLE IN DAYS

1. **Move the '98.9% phishing detection rate' to the homepage hero.** This verified metric is buried in the Trust Center. Put it front and center with the source attribution. One strong number above the fold transforms credibility.
2. **Add certification badges to the homepage footer.** SOC 2, ISO 27001 badges should be visible on every page. Currently only on the Trust Center. A simple badge row above the footer takes 30 minutes to implement.
3. **Rewrite the subheadline with the deployment differentiator.** Change to: 'Behavioral email security for M365 and Google Workspace. Deploys in 15 minutes. No MX changes. No rules to write.' This version includes three proof points.
4. **Replace generic customer descriptions with security outcomes.** Instead of 'Leading fintech company,' use '500-person fintech, 12,000 mailboxes, 99.2% detection rate.' Every logo should tell a security story.
5. **Add 'No MX changes' to the hero section.** This is the single most powerful deployment claim in email security and it is buried in section 7. Move it to the hero or first visible section.
6. **Update the page title tag.** 'AI Email Security Platform' is generic. Change to: 'ShieldMail | Behavioral Email Security for M365 & Google Workspace | 98.9% Detection.'
7. **Remove or rewrite 'comprehensive solution' and 'advanced protection' copy.** These phrases appear 4 times on the homepage. Replace each instance with a specific, quantified claim.

SECTION 09

High-Impact Changes (30 Days)

STRATEGIC RECOMMENDATIONS

1. Create a Pricing Page

Even indicative pricing removes the #1 friction point. CISOs need to model costs before requesting a demo. Recommendation: three tiers (Essentials, Professional, Enterprise) with per-mailbox pricing. Show the Essentials price publicly; gate Enterprise with 'Contact Sales.' The absence of any pricing signal causes CISOs to assume either (a) the product is prohibitively expensive, or (b) the company is too early-stage to have standardized pricing. Neither assumption helps.

2. Publish 3 Named Customer Case Studies

Each case study should follow the Challenge > Solution > Quantified Results framework. Target metrics: detection rate improvement vs. previous solution, false positive reduction, time from deployment to first detected threat, and total threats caught in the first 90 days. A single case study with '[Customer] reduced phishing incidents by X% in 30 days' transforms ShieldMail from 'interesting startup' to 'proven solution.'

3. Build Competitive Comparison Pages

Create dedicated landing pages for the two comparisons CISOs will make:

- 'ShieldMail vs InboxGuard: What Mid-Market Companies Need to Know'
- 'ShieldMail vs Microsoft Defender: Why Native M365 Protection Is Not Enough'
- 'Alternative to MailFortress: Modern Email Security Without the Complexity'

Be honest about where competitors are stronger (larger customer base, analyst coverage) and where ShieldMail wins (faster deployment, behavioral detection, DLP included, transparent pricing). These pages also capture high-intent SEO traffic.

4. Create a Technical Architecture Page

CISOs and their security engineers need to understand deployment architecture before approving a vendor. Build a page showing: API integration flow, data handling (what ShieldMail reads, stores, processes), architecture diagram, supported M365/Google Workspace tiers, and a clear data residency statement. This is table-stakes content that most competitors already provide.

5. Develop a Threat Intelligence Resource Center

Build a resource center with: a 'State of Email Threats' report (using ShieldMail's detection data), whitepapers on BEC/phishing trends, and a monthly threat briefing. Position ShieldMail as a thought leader, not just a product vendor. CISOs buy from companies they learn from. This also creates SEO content that attracts security professionals at the research stage of the buyer journey.

6. Get Listed and Verified on Mandos Cyber

Submit the product listing under Email Security (anti-phishing, email-security-platforms subcategories). Complete the verification process for the trust badge. Mandos Cyber reaches 50,000+ monthly visitors, primarily CISOs and security engineers. This is a low-effort, permanent SEO backlink from a high-authority cybersecurity domain.

SECTION 10

Mandos Cyber Platform Visibility

ShieldMail is currently not listed on Mandos Cyber, the largest independent cybersecurity product intelligence platform tracking 3,200+ companies and 8,500+ products.

RECOMMENDATION

- **Submit your product listing:** Create a listing under the 'Email Security' category. Include product features, integrations, deployment model, and pricing model.
- **Complete verification:** Verified listings receive a trust badge, appear higher in search results, and signal to CISOs that the company actively maintains its market presence.
- **Encourage customer reviews:** After verification, ask 5-10 active customers to leave reviews. Named reviews with security outcomes significantly improve positioning.
- **Maintain your profile:** Keep features, integrations, and pricing model updated. CISOs use Mandos Cyber alongside review platforms and analyst research when evaluating vendors.

SECTION 11

About & Next Steps

This Mandos Positioning Report was produced by Mandos Cyber, the largest cybersecurity product intelligence platform tracking 3,200+ companies and 8,500+ products.

Mandos Framework analysis, built on 13 years of enterprise security procurement across banking, fintech, and FMCG.

Next Steps

- **Schedule a strategy call:** cal.com/nikolozk
- **Monitor your competitors:** mandos.io
- **List your product:** mandos.io

END OF SAMPLE REPORT

All company names and data in this report are fictional. Your report will use real data from the Mandos Cyber platform.