Health Score calculation logic

Ensuring cold emails land in the inbox (not spam) requires monitoring multiple metrics. We propose a composite Health Score (0–100) based on key deliverability factors. This score can flag problems early, so senders can adjust tactics before campaigns suffer. In email terms, “delivery” means the message was sent; “deliverability” means where it lands (inbox vs spam) . Thus, a good health score emphasizes true inbox placement via factors like reputation, engagement, bounces, etc.

Key factors influencing deliverability include:

- **Domain/IP Reputation:** Trust level of your sending domain and IP, based on past behavior (engagement, complaints, bounces) .
- **Technical Setup (SPF/DKIM/DMARC/rDNS):** Email authentication and DNS records that confirm sender identity .
- **Bounce Rate:** Percentage of emails that bounce back (undelivered addresses), which directly harms reputation .
- ~~**Spam Complaint Rate:** Percentage of recipients marking the email as spam. ISPs consider high complaint rates a major red flag .~~ (Not using this as it involves postmaster tools setup which would be hard to implement for each domain)
- **Engagement (Open/Reply Rates):** Recipient interaction metrics. High open/reply rates signal healthy inbox placement; extremely low rates (given a comparable send volume) can indicate deliverability or content issues . (Note: open-tracking is now less reliable due to privacy features , so reply/click rates become more important.)
- **Sending Volume & Consistency:** How many emails you send and how steadily you send them. Gradual ramp-up and steady volumes build reputation; sudden spikes can trigger spam filters .

Below we detail each factor, suggest how to weight it, and recommend monitoring practices and tools.

Domain & IP Reputation

Domain reputation is the overall “health” of your email domain/IP, rating its trustworthiness . A sender with a strong reputation is more likely to reach inboxes. Reputation is influenced by historical engagement (opens/replies), complaint rates, bounce rates and spamtrap hits . For example, Validity’s SenderScore (0–100) quantifies IP reputation; scores above ~80 are good . In the chart below, a very high SenderScore (98) is shown for a well-established sender:

Figure: Example SenderScore (0–100) for a high-volume sender (score = 98). Higher scores indicate strong reputation.

- Importance: A poor domain or IP reputation causes ISPs (like Gmail, Yahoo) to filter or block mail. Maintaining a good reputation is foundational: senders with a history of spam or abuse will see their messages shunted to spam no matter what else they do .

- Monitoring: Use reputation-check tools and ISP dashboards. Google Postmaster Tools, Microsoft SNDS (Smart Network Data Services), Cisco Talos, SenderScore.org, and BarracudaCentral can report your domain/IP rating and blacklist status . Regularly scan common DNSBL lists (via MXToolbox, for example) to ensure you’re not listed. If any major provider shows a low score or blacklisting, investigate immediately.

- Weight: High (e.g. ~20%). Domain/IP reputation underpins all email sending; we recommend allocating a large weight since even great content won’t reach inboxes if reputation is poor.

Technical Setup (SPF, DKIM, DMARC, rDNS)

Proper email authentication and DNS configuration are critical prerequisites for deliverability. SPF, DKIM, and DMARC are protocols that prove an email is legitimately from your domain . A correctly set up SPF record lists authorized sending IPs; DKIM provides a cryptographic signature; DMARC tells receivers what to do with messages that fail SPF/DKIM. Reverse DNS (PTR record) links your sending IP to your domain.

- Why It Matters: ISPs reject or spam-flag emails that fail authentication. As Cloudflare notes, domains lacking correct SPF/DKIM/DMARC “may find their emails get quarantined as spam, or are not delivered” . Likewise, without proper rDNS, receiving servers often refuse delivery . In effect, any failure in this setup can immediately degrade your score.

- Checklist & Tools:

    - SPF: Confirm your DNS has an SPF TXT record listing all sending IPs. MXToolbox and SPF record checkers can verify correct syntax.
    - DKIM: Ensure your ESP or mail server is signing outgoing mail and publish the matching public key in DNS. Test with MXToolbox DKIM lookup.
    - DMARC: Publish a DMARC record (e.g. p=reject or p=quarantine) to enforce authentication. Start with p=none to gather reports, then tighten policy. Tools like dmarcian or DMARC Analyzer simplify DMARC deployment and reporting.
    - rDNS: Verify via a DNS lookup that your sending IP has a PTR record pointing to your domain (or a subdomain you control). This is often done through your hosting/ISP.
    - Use email testing tools (e.g. MXToolbox's DNS check, Mail-Tester) to catch any gaps.

- Weight: High (e.g. ~20%). This is essentially a gating factor: if authentication fails, other metrics become moot. A fully authenticated setup should get full points; any failure should deduct substantially.

Bounce Rate (List Hygiene)

Bounce rate is the percentage of sent emails that never reach the inbox because the address is invalid (hard bounce) or temporarily unavailable (soft bounce). Hard bounces in particular signal bad list hygiene. ISPs penalize senders with high bounce rates as it suggests purchased or stale lists.

- Thresholds: Aim for <2% hard-bounce rate . Many sources say 2–5% is a cautionary range and anything above ~5% is critical . For example, one guide advises "an overall bounce rate below 2% is considered healthy" ; above 5% often triggers warnings or blocks.
- Mitigation: Keep your lists clean. Before sending, validate addresses with list-cleaning tools (e.g. NeverBounce, Kickbox). Remove hard bounces immediately. Track bounce logs daily: if a campaign's bounce rate spikes, pause sending and correct the issue.
- Effects: High bounce rates directly harm your sender reputation . Each hard bounce is like a vote against you in the ISP's eyes, reducing your score. Over time, ISPs may throttle or blacklist your IP/domain if bounces remain elevated.
- Weight: Moderate-high (15%). Because bounces can quickly degrade reputation, allocate significant weight. Score less than ~10–15 points (out of 100) for bounce component if

bounces are ≤2%; if bounce exceeds the threshold, deduct accordingly.

~~Spam Complaint Rate~~

~~This is the fraction of delivered emails marked as spam by recipients. Even a few complaints can severely hurt deliverability. Major ISPs use this as a top signal for spam.~~

- ~~Benchmark: Aim for <0.1% complaint rate (fewer than 1 complaint per 1,000 sends) . Google and Yahoo explicitly recommend staying under this level . Crossing ~0.3% is dangerous and can lead ISPs to throttle or block your mail . In practice, any sustained rate above ~0.1% should trigger corrective action.~~

- ~~Prevention: Always include a clear unsubscribe link and honor opt-outs promptly. Segment your list to avoid sending unwanted content. Educate recipients to whitelist you, especially in cold outreach.~~

- ~~Monitoring: Use ISP feedback loops (where available) to receive complaint notifications. Google Postmaster Tools and similar services report spam rate and abuse complaint data for your domain/IP. If you see complaints rising, investigate content or targeting issues immediately.~~

- ~~Weight: Moderate-high (15%). Spam complaints are one of the quickest ways to tank a reputation. Factor any spike heavily into the score. For example, a complaint rate of 0.0–0.1% might score full points, whereas >0.3% should score near zero.~~

Engagement: Open and Reply Rates

Engagement signals inbox placement and relevance. If recipients are opening and replying, it generally means your mail is getting through and interesting. Conversely, very low opens or replies (given normal send patterns) can indicate deliverability or content problems.

- Open Rate: Historically, a high open rate (>50%) was taken to imply good deliverability . (Emails landing in spam often see open rates below ~40% .) However, email client privacy features (e.g. Apple Mail Privacy Protection) mean open rates are now noisy – pixels may auto-load or block entirely . As Lemlist notes, open pixels can be “preloaded without the recipient opening the email,” making open rates unreliable . Still, extremely low open rates (e.g. <30%) usually reflect a real issue.

- Reply Rate: The percentage of recipients who reply. Cold email benchmarks are low – typically 1–5% . Even small increases in reply rate can greatly improve ROI. Because open

tracking may be disabled, reply or click rates become more meaningful proxies for engagement. If your opens are high but replies near zero, it often means the content isn't resonating (or possibly that mails went to a "read-only" inbox).

- Tools: Email platforms (Outreach, Mailshake, etc.) track opens and replies. Even if open tracking is off, reply tracking is reliable (a response proves delivery). Use UTM-tagged links to measure clicks, or "reply" as a key success metric.

- Weight: Moderate (10% each for opens and replies, or 20% combined). Engagement should contribute to the score but not override core factors. For scoring, you might scale engagement: e.g. >50% open and >2% reply (cold) yields full engagement points; dropping below these affects score.

Sending Volume & Consistency

Cold-email accounts (especially new domains/IPs) must be "warmed up" with gradually increasing volume. Consistency over time is vital; erratic sending (sudden spikes or long pauses) harms reputation.

- Warm-up Guidelines: For a brand-new domain, start with small batches (e.g. 10–20 emails/day) and double roughly every week if engagement is good . For example, one schedule suggests ramping from 20→50→100 daily over 2–3 weeks . Even for established senders, avoid one-day surges. As Inboxroad warns, "large surges of emails can often be seen as spam by ISPs," so follow a measured schedule .

- Consistency: Maintain a steady cadence. If you normally send 20/day and suddenly send 1,000, filters may flag it. Spreading sends evenly and slowly scaling up builds a positive sending history .

- Monitoring: Track daily/weekly send volumes and compare to historical averages. Use warm-up services (Lemwarm, WarmupInbox) that automate sending patterns. If you use multiple accounts, distribute volume across them as advised by ESP limits.

- Weight: Moderate (10%). Volume itself isn't as direct a signal as reputation or complaints, but erratic volume can negate a good reputation. Penalize big deviations: e.g. if current volume >200% of normal, deduct some score. Reward steady, properly warmed-up accounts.

Continuous Monitoring & Scoring

Implementing this health score means tracking each factor over time and recomputing the score regularly (e.g. daily or weekly). For example, SparkPost's "Health Score" runs daily and predicts your engagement based on recent bounces, complaints, etc. – scores >80 are considered good . Similarly, you can create a dashboard that ingests your ESP stats (bounces, complaints, opens/replies), ISP data (Google Postmaster/ SNDS), and external checks.

- Adjusting Over Time: Use sliding-window metrics (e.g. last 7-30 days) to smooth out anomalies. If any metric worsens (e.g. bounce rate climbs), the score should drop accordingly, prompting investigation. Conversely, improvements (clean list, better content) should raise the score.

- Alerts & Trends: Set thresholds on each metric (e.g. bounce >2%, spam >0.1%) to trigger alerts. Watch trends: a steadily declining score indicates a systemic issue.

- Tools & Services: Key tools include: Google Postmaster Tools (Gmail metrics: spam rate, reputation, delivery errors), Microsoft SNDS (Outlook/Hotmail data), MXToolbox (DNS and blacklist checks), mailbox testers like GlockApps or Mail-Tester (simulate delivery to multiple inboxes), and DMARC monitoring services (for auth reports). Most ESPs also provide analytics dashboards with these metrics. Use these to diagnose problems.

Overall, each factor contributes a weighted portion of the 100-point health score. For example, one might allocate ~20% each to Reputation and Technical setup, ~15% each to Bounce and Spam Complaints, and the remaining ~30% split among Open Rate, Reply Rate, and Volume (10% each) – though exact weights can be adjusted based on your priorities. The table below summarizes each factor, its weight, ideal thresholds, and monitoring tools.

Factor	Weight	Healthy Threshold / Guideline	Monitoring & Tools
Domain/IP Reputation	20%	High SenderScore/IP score (e.g. >80) ; no blacklists; Gmail "high" reputation.	SenderScore.org, Cisco Talos, BarracudaCentral, Google Postmaster (spam rate, reputation), MXToolbox (DNSBL).
Technical Setup (SPF/DKIM/DMARC/rDNS)	20%	All checks PASS: valid SPF record; DKIM-signing enabled; DMARC policy (preferably quarantine/reject with monitoring); PTR (reverse DNS) set .	MXToolbox DNS lookup (SPF, DKIM, DMARC, PTR); DMARC analyzers (e.g. DMARCIan); mailbox tester (GlockApps, Mail-Tester).
Bounce Rate	15%	<2% overall bounce . (2–5% is cautionary; >5% is critical.)	ESP bounce reports; list hygiene tools (Kickbox, NeverBounce) to clean lists; pause sends if bounces spike.

Email Deliverability Score	15%	<0.1% (≤1 complaint per 1,000 emails) . (Above ~0.3% is dangerous.)	Gmail Postmaster (spam rate), ISP feedback loops (Yahoo/AOL FBL), ESP complaint stats; ensure clear unsubscribe.
Open Rate	10%	Cold-email >50% is ideal ; <40% usually indicates deliverability issues .	ESP analytics (open logs); note tracking pixels may be blocked . Use subject tests and warm-up to improve.
Reply/Response Rate	10%	Typically 1–5% for cold campaigns . (Higher means better engagement.)	Track replies via CRM or sales platform. Compare to historical averages; a sudden drop may signal inboxing problems.
Volume & Consistency	10%	Steady ramp-up and volume. Example warm-up: 10–20→50→100 emails/day over weeks . No sudden spikes .	Warm-up tools (Lemwarm, WarmupInbox); sending logs/dashboards. Alert if current volume >200% of norm or big daily swings.

Revision #1
Created 9 June 2025 13:01:33 by Vivek Yadav
Updated 9 June 2025 13:42:50 by Vivek Yadav