missioninbox

ENTERPRISE BRIEF · FOR OUTBOUND AT SCALE

You can run cold email at scale without putting your domain at risk.

Most enterprise teams stop sending cold from their root domain the first time a campaign tanks their transactional deliverability. The usual reaction, buying lookalike domains, solves the wrong problem. There is a cleaner architecture.

THE ARCHITECTURE IN ONE LINE

Subdomains of your root, on dedicated IPs. They inherit your domain's age and trust, keep cold reputation isolated from transactional, and scale horizontally without brand dilution.

THE ENTERPRISE QUESTION 01 / 03

Cold email keeps tanking the domain your business runs on.

Most enterprise teams stop sending cold from their root domain the first time a campaign tanks their transactional deliverability. The usual reaction is to buy lookalike domains: trycompany.com, companysales.com, company-team.com. That move solves the wrong problem. It dilutes your brand, signals spoofing to recipients, and starts you from zero reputation with Microsoft.

MISSION INBOX		STATUS QUO
Subdomains of your root Inherit age and trust · Reputation isolated · Dedicated IPs	VS	**Root domain or lookalikes** Shared reputation · Brand dilution · Cold volume on transactional rails

THE PROBLEM

Three ways your current setup leaks deliverability.

ROOT RISK

Cold volume on the root domain

One bad campaign blacklists the domain your CFO uses for wire confirmations and your CEO uses to talk to the board. Recovery takes weeks. The damage is measured in lost deals, not lost emails.

BRAND DILUTION

Lookalike domains dilute trust

Recipients see trycompany.com and either delete or report. Microsoft sees a brand new domain with no history and throttles it. You bought forty domains that inherit nothing and start from zero with every filter.

WRONG RAILS

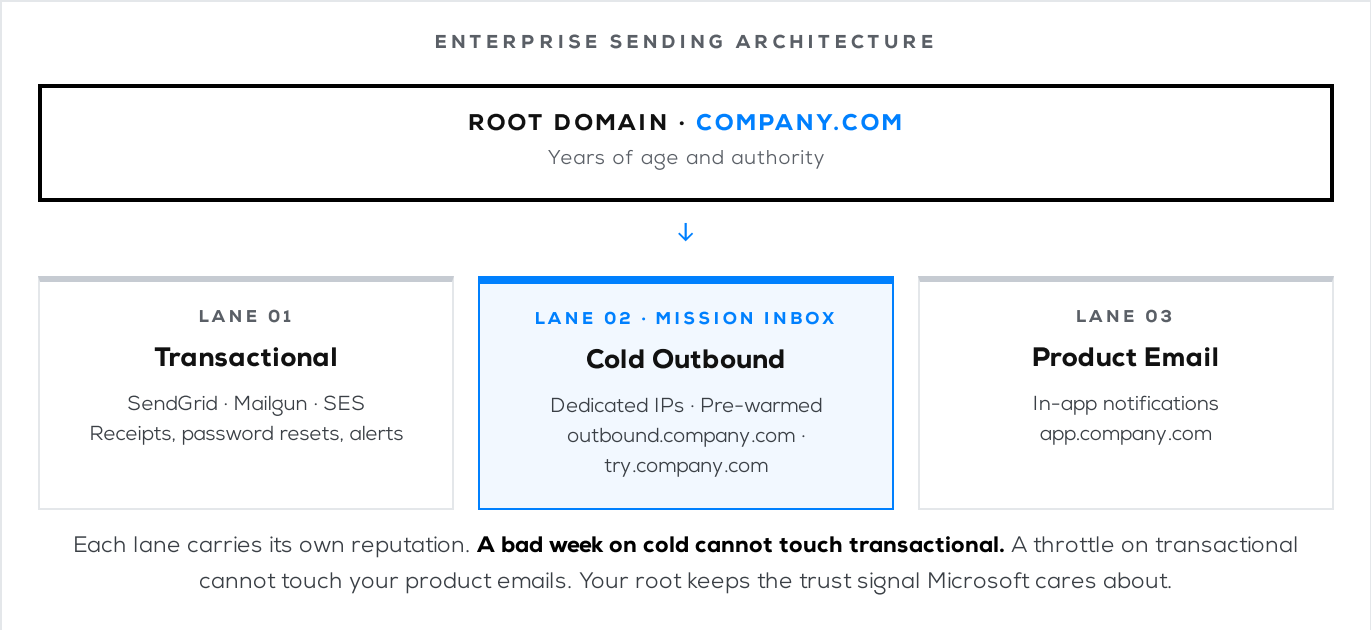
Transactional ESPs were not built for cold

SendGrid, Mailgun, Postmark, SES, Resend. These are shared pools optimized for receipts and password resets. Push cold volume through them and you trigger abuse teams, and risk losing the rails your product runs on.

THE ARCHITECTURE 02 / 03

Three lanes. One brand. Reputations that do not touch.

Mission Inbox runs your cold outbound on subdomains of your root, on dedicated IPs we own. Your transactional sending stays on its existing ESP. Your product emails stay on their own rails. Three separate reputations, all under your brand, none of them able to take the others down.



Each lane carries its own reputation. **A bad week on cold cannot touch transactional.** A throttle on transactional cannot touch your product emails. Your root keeps the trust signal Microsoft cares about.

HEAD TO HEAD

Where the architectures actually differ.

CAPABILITY	MISSION INBOX SUBDOMAINS (WINNER)	ROOT DOMAIN SENDING	LOOKALIKE DOMAINS
Brand trust signal	Recipient sees your real brand	Real brand, but cold volume puts it at risk	Reads as spoofing, gets reported
Domain age inherited	Full age of root carried into Microsoft filter	Yes, but exposes the root to cold risk	Zero. Starts from a brand new domain
Reputation isolation	Cold reputation cannot touch transactional	None. One bad campaign blacklists everything	Isolated, but with no reputation to inherit
IP allocation	Dedicated, pre-warmed, 1.5M/day capacity	Shared ESP pool, pool average reputation	Shared ESP pool, no domain to anchor it
IT and security posture	No API access to your DNS. TXT file upload	Cold campaigns running on production infrastructure	Forty new domains for IT to monitor and renew
Time to first send	3 weeks warmup. Scales horizontally	Immediate, but every send puts the root at risk	8 to 12 weeks per domain. Manual warmup each

WHY THIS MATTERS FOR ENTERPRISE 03 / 03

OUTLOOK DECIDES WHO REACHES THE ENTERPRISE INBOX

Microsoft's spam filter weighs two signals above almost everything else: **IP reputation** and **domain age**. On shared ESP infrastructure, IP reputation is a pool average. It is not yours, and you cannot improve past it. On a brand new lookalike domain, you have neither. With Mission Inbox subdomains, you get both. The age and authority of your root domain carries forward, and the IP reputation is yours alone to build. That is why enterprise teams targeting Outlook see Mission Inbox outperform both shared ESP rails and lookalike domain strategies, often by a meaningful margin.

WHAT THIS LOOKS LIKE IN PRACTICE

Cold email, saved without the rest of the infrastructure ever feeling it.

Your transactional ESP keeps doing what it was built for. Your product emails keep firing. Outbound runs on subdomains that look like part of your brand because they are part of your brand. If a campaign goes sideways, the only thing affected is the subdomain it ran on. The blast radius stops at the subdomain wall. The CFO's wire confirmations still land in the inbox.

CONTAINMENT

Blast radius stops at the subdomain

A burned subdomain affects only the mailboxes on that subdomain. Route to the next, retire the old, keep sending. The root and the other lanes never know it happened.

SPEED

Scale horizontally, not vertically

Need more capacity? Spin up more subdomains. No per-domain fees. No new infrastructure procurement. No IT ticket queue. The architecture grows with the pipeline.

COMPLIANCE

Built for the IT review

No API access to your DNS. No write access to your domain registrar. We hand you a TXT file. Your team uploads it. SOC 2 in progress. Architecture documentation available on request.

Stop sending cold from the wrong rails.

Talk to our team about migrating outbound to dedicated infrastructure.

BOOK A CALL

TRUSTED BY

15+ YC startups
Y COMBINATOR

a16z & Sequoia portfolio
COMPANIES

Enterprise
450M+ EMAILS/MO