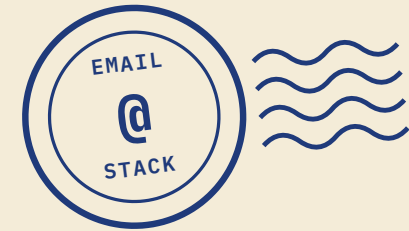


PAR AVION
BY AIR MAIL



THREAT TAXONOMY • THE REFERENCE FOR ELEVATION OF EMAIL FLOW

The Unmodeled Attack Surface

A Threat Taxonomy for Email Infrastructure

This is the reference for the Elevation of Email Flow card game: 117 threats across nine layers of the email stack, plus eight structural hazards. Each entry states the threat as a property of a component or a design decision, the principle a sound design follows, design measures, and mappings to STRIDE, CAPEC and CWE. The game and the taxonomy share one set of references.

© 2026 Jonathan Brett Crawley. CC BY-NC-ND 4.0, with additional permissions.

Licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0): you may share the whole taxonomy, unchanged and with credit, for non-commercial purposes. In addition, whether or not the use is commercial, you may use it to threat model systems, including for paying clients; use it internally and for training inside any organisation; and quote individual entries, with credit, in paid courses, reports and talks. Shipping it in a product, such as a tool's built-in library, a printed deck or a reprint for sale, needs written permission.



Brett Crawley

ostering.com • Version 1.0, October 2026

How to use it

Every entry has a reference, a name, a threat, a mitigation principle and two to four design measures. The principle says what must be true; the measures show what that looks like in practice, and are examples of what works rather than the only acceptable answers.

The taxonomy is the reference for the card game Elevation of Email Flow: each entry is one of its cards, and the two share one set of references. The reference is the layer prefix plus a playing-card rank, from Ace down to 2, or T1 to T8 for the structural hazards. It is a stable identifier, not a severity: in the card game the ranks follow severity because play is trick-based, but in the taxonomy a reference only names an entry, and it stays the same as the taxonomy grows.

1. Draw the mail flow: every hop, scanner, store and client a message touches, with the trust boundaries marked.
2. Take one layer and walk every entry in it against each element it applies to.
3. For each entry, ask whether the design satisfies the principle. Write down a finding, or "no exposure" and the design decision that defeats it.
4. Where there is a finding, start from the measures given and adapt them to your architecture. They are the shape of a fix, not a prescription.
5. Finish with the structural hazards, played against the design as a whole.

Scope. The taxonomy covers the infrastructure: the components, protocols and sequencing contracts that deliver the message. It does not cover social engineering, phishing lures or the human decisions that make email such a successful attack vector.

Which side of the line

Some layers touch, and it helps to know which side of the line an entry sits on:

- **Authentication and DNS:** DNS covers who can control or falsify an answer. Authentication covers what a genuine answer can be made to mean.
- **SMTP and delivery pipeline:** SMTP is a single hop's conversation. The pipeline is the composition of hops.
- **MIME and delivery pipeline:** MIME is how a message is interpreted. The pipeline is whether and when it is inspected.
- **Delivery pipeline and content scanners:** the pipeline decides what to do with a scanner's limits and verdicts. The scanner layer asks whether the inspection itself holds up.
- **Tenancy:** Tenant Confusion (DP·7), Cross-Tenant Identity (AU·K) and Shared Reputation Poisoning (SM·8) each cover a different face of shared infrastructure (configuration, identity, reputation). Shared Infrastructure, Shared Fate (T2) is the structural hazard behind all three.
- **Operations and the other layers:** delivery pipeline, client protocols and DNS each cover a corner of operations (admin routing changes in DP·2, mailbox state in CP·10, dangling records in DN·K). Operations and storage covers the stores and tooling around the message path: the copies, the credentials and the people with access.

The layers

LAYER	NAME	PREFIX	ENTRIES	SCOPE
01	Delivery pipeline	DP	13	The composition of hops between sending MTA and mailbox: sequencing, fracture, remediation
02	Authentication protocols	AU	13	SPF, DKIM, DMARC and ARC as trust signals that can be weaponised
03	Client protocols	CP	13	IMAP, POP, submission, and the API protocols clients use to reach the mailbox
04	SMTP	SM	13	The MTA-to-MTA conversation: identity, relay, transport security, parsing
05	MIME and S/MIME	MI	13	How content is parsed, decoded, rendered, signed and encrypted
06	DNS layer	DN	13	The records and resolvers that say where mail goes and who may send it
07	Content scanners	CS	13	URL, malware, sandbox, ML and LLM inspection engines
08	Human-facing layer	HF	13	What the client and platform present to the person reading or sending
09	Operations and storage	OP	13	The operational plane: archive, backup, search, logs, support access, configuration, offboarding
T	Structural hazards	T	8	Hazards of email itself

The mapping line under each threat. Every entry is mapped to STRIDE, to CAPEC 3.9 attack patterns and to CWE 4.20 weaknesses, for example STRIDE E (Loose) · CAPEC Partial: CAPEC-554, CAPEC-36 · CWE Direct: CWE-420, CWE-424. **STRIDE** gives the categories, best fit first; *Clean* means a STRIDE prompt would plausibly find the threat, *Loose* that STRIDE gives a label but not the question. For **CAPEC** and **CWE**, the rating applies to the list as a whole, and the IDs are in best-fit order: *Direct* means the first ID names the flaw, and any others cover further aspects of it; *Partial* means the IDs cover only part of the flaw, or a broader version of it; *None* means there is no matching pattern or weakness. Look an ID up at capec.mitre.org/data/definitions/<number>.html or cwe.mitre.org/data/definitions/<number>.html. The Excel, SKOS and STIX downloads carry the names as well as the IDs.

Licence

© 2026 Jonathan Brett Crawley. This taxonomy is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (CC BY-NC-ND 4.0), with the additional permissions below.

Licence text: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

USE	PERMISSION NEEDED?
Sharing the whole taxonomy non-commercially (OWASP, universities, conferences, individuals)	No
Threat modeling with it, including for paying clients	No
Internal use and training inside any organisation	No
Quoting entries, with credit, in paid courses, reports and talks	No
Shipping the taxonomy in a product: a tool's built-in library, a printed deck, a reprint for sale	Yes, ask me

Additional permissions. In addition to the rights the licence gives, and whether or not the use is commercial, the copyright holder grants you permission to:

- use the taxonomy to threat model systems you build, operate or assess, including for paying clients;
- use it internally, and for training, inside any organisation;
- quote individual entries, with credit, in paid courses, reports, findings and talks.

Any other commercial use, including shipping the taxonomy or a substantial part of it in a product (a tool's built-in library, a printed deck, a reprint for sale), needs written permission. Ask me on LinkedIn.

Credit. “The Unmodeled Attack Surface: A Threat Taxonomy for Email Infrastructure” by Jonathan Brett Crawley, ostering.com, licensed under CC BY-NC-ND 4.0.

These additional permissions are given alongside the licence. They add to what the licence allows and do not take anything away from it.



Delivery pipeline (DP)

Every message should pass every control, in the intended order, and each control should see what the recipient will see. These entries cover sequencing, fracture and remediation across the hops between the sending MTA and the mailbox.

ID	THREAT	MITIGATION
DP-A	<p>Ingress Bypass</p> <p>The platform exposes an endpoint that accepts mail for a recipient without it having passed the upstream controls the design assumes.</p> <p>STRIDE E (Loose) · CAPEC Partial: CAPEC-554, CAPEC-36 · CWE Direct: CWE-420, CWE-424, CWE-291</p>	<p>Every ingress path enforces the same controls, bound to a verified identity rather than a network location.</p> <ol style="list-style-type: none">(1) Authenticate hybrid and partner ingress with mutual TLS or a per-connector client certificate, and reject sessions that present neither.(2) Route all ingress endpoints through one policy enforcement point, so an endpoint added later cannot skip a control by construction.(3) Inventory ingress endpoints from the network and load-balancer configuration, not from documentation, and alert when a listener appears that is not registered with the enforcement point.
DP-K	<p>Inherited Verdict</p> <p>A hop trusts a verdict, authentication result or classification written upstream that it cannot verify, including headers an external sender can forge.</p> <p>STRIDE S, T (Clean) · CAPEC Partial: CAPEC-194, CAPEC-21 · CWE Direct: CWE-807, CWE-349</p>	<p>A hop acts only on verdicts and authentication results it produced or can cryptographically verify.</p> <ol style="list-style-type: none">(1) Strip Authentication-Results, verdict and other platform headers at every ingress boundary before any inbound mail is processed.(2) Carry verdicts in out-of-band metadata keyed to the message (a queue envelope or database row), never in headers that travel with the message.
DP-Q	<p>Mutating Hop</p> <p>A hop rewrites the message (URLs, banners, footers, re-encoding), so downstream hops verify or scan something different from what was sent or what will be displayed.</p> <p>STRIDE T (Loose) · CAPEC None · CWE Partial: CWE-179</p>	<p>A control inspects or verifies the exact bytes the recipient will receive, and any mutation is recorded with what it invalidated.</p> <ol style="list-style-type: none">(1) Verify DKIM and S/MIME signatures before any rewriting, and record the result in metadata the later hops and the client read.(2) Run content inspection on the post-mutation message, or make the mutating hop the last one before delivery.(3) Keep an immutable copy of the message as received, so that any later verification or investigation can be run against the original bytes.

ID	THREAT	MITIGATION
DP-J	Fail-Open Scanning A scanner reaches a size, depth, time or decryption limit and the pipeline delivers the message anyway. STRIDE E (Loose) · CAPEC Partial: CAPEC-24 · CWE Direct: CWE-636	"Could not scan" is a distinct outcome with its own policy, never silently collapsed into "clean". (1) Return a distinct UNSCANNED verdict for every limit (size, depth, time, decryption) and map it to hold or a visible flag by default. (2) Make the fail-open or fail-closed choice a per-tenant policy setting with its default set to fail closed, and log every fail-open event.
DP-10	Verdict Decay A verdict is computed once on content whose meaning can change later, such as remote URLs and remotely loaded content. STRIDE T (Loose) · CAPEC Partial: CAPEC-29 · CWE Partial: CWE-367, CWE-638	Content whose meaning depends on resources outside the message is judged at the moment of use, not only at delivery. (1) Evaluate rewritten URLs at click time against current intelligence, and block or warn when the destination has changed since delivery. (2) Set a verdict lifetime for remote-dependent content and re-scan delivered messages when the lifetime expires or new intelligence arrives.
DP-9	Unscanned Path A write path to the mailbox exists that does not traverse the controls: internal and cross-tenant mail, API or IMAP APPEND injection, calendar items, connectors, migration and import. STRIDE E (Loose) · CAPEC Partial: CAPEC-554, CAPEC-36 · CWE Direct: CWE-420, CWE-424	There is exactly one write path to the mailbox store, and every message takes it. (1) Route intra-tenant, cross-tenant, API-submitted and IMAP APPEND messages through the same scanning pipeline as internet mail. (2) Remove direct write access to the store from every service except the delivery agent, and enforce that with the store's own authorisation. (3) Test the single-path property continuously by injecting marked messages through every write interface (API, IMAP APPEND, calendar, import, migration) and asserting that each one appears in the scanner's log.
DP-8	Remediation Race Post-delivery retraction assumes the platform still controls every copy, but synced devices, forwards, rules and API consumers have already taken one. STRIDE I (Loose) · CAPEC None · CWE None	Remediation reaches every copy the platform created and reports the copies it could not reach. (1) Track each copy made by sync, forward, rule or API with the message identifier, so remediation can target each one. (2) Return a remediation report listing unreachable copies (offline devices, external forwards) so the tenant can act on them.

ID	THREAT	MITIGATION
DP-7	Tenant Confusion A shared hop attributes a message to a tenant from an attribute the sender controls, or applies one tenant's configuration, trusted status or allow list to another tenant's mail. STRIDE S, E (Clean) · CAPEC Partial: CAPEC-21 · CWE Direct: CWE-807, CWE-291, CWE-639	Tenant identity is resolved from a verified property, bound to the message at ingress, and every later decision is scoped by it. (1) Attribute a message to a tenant only from a verified property (a per-tenant client certificate for connectors, the verified recipient domain for inbound mail), never from the envelope sender or an IP address that a third party shares. (2) Store allow lists, connectors and trusted-sender rules keyed by tenant identifier, reject lookups that supply none, and never let attribution alone confer internal or trusted status. (3) Carry the tenant identifier in internal metadata outside the message, and have every service reject a message whose metadata is missing or whose tenant does not match the recipient domain. (4) Test tenancy with two tenants on the same shared IP range and the same sender domain, and assert that neither's configuration affects the other's mail.
DP-6	Induced Backpressure A sender drives load so that queues, deferrals or timeouts cause controls to be skipped or shortened. STRIDE D (Loose) · CAPEC Partial: CAPEC-125 · CWE Direct: CWE-636, CWE-770	Controls degrade to hold or defer under load, never to skip. (1) Reserve per-tenant queue and scanner capacity so one sender cannot consume what others need. (2) Defer with a 4xx response when scanner capacity is exhausted, rather than accepting and delivering unscanned.
DP-5	Loop and Amplification Forwarding, auto-replies and bounces between hops create loops or multiply mail. STRIDE D (Clean) · CAPEC Direct: CAPEC-490 · CWE Direct: CWE-406, CWE-799	Automatic mail is rate-limited and loop-detected on every path that can generate it. (1) Count the platform's own trace headers and refuse to forward or reply once a hop limit is reached. (2) Rate-limit auto-replies and automatic forwards per recipient and per trigger, and suppress them for mail that failed authentication.
DP-4	Verdict Inconsistency One message to several recipients is split, scanned or cached differently per recipient, and a cached verdict is reused where it does not apply. STRIDE T (Loose) · CAPEC Partial: CAPEC-141 · CWE Partial: CWE-1023, CWE-1250	One message produces one verdict per recipient policy, and cached verdicts are keyed on everything they depend on. (1) Key the verdict cache on the full content hash plus the sender identity, authentication result and tenant policy version. (2) Scan a split message once and attach the single verdict to every recipient copy, then apply per-recipient policy to that verdict. (3) Invalidate cached verdicts when the policy, the intelligence feed or the scanner version changes, not only when the content hash does.

ID	THREAT	MITIGATION
DP-3	Quarantine Release Abuse Quarantine, release and allow-list paths return a message to the mailbox without re-evaluating it. STRIDE E (Clean) · CAPEC Partial: CAPEC-62 · CWE Partial: CWE-424, CWE-841	A message leaving quarantine is re-evaluated with current intelligence, and release requires authenticated intent. (1) Re-scan on release and refuse to deliver if the current verdict is worse than at quarantine time. (2) Require an authenticated session for release, with single-use tokens for digest links and no release via GET.
DP-2	Pipeline Reconfiguration Whoever can change routing rules, connectors or transport rules can steer mail around the controls, and the change looks like ordinary administration. STRIDE T, E (Clean) · CAPEC Direct: CAPEC-176 · CWE Partial: CWE-1220, CWE-778	Changes to the path a message takes are privileged, approved and traceable to the message. (1) Require a second approver for any routing, connector or transport rule change that removes a control from the path. (2) Record the ordered list of controls each delivered message traversed, and alert when a message's path differs from the tenant's baseline.



Authentication protocols (AU)

SPF, DKIM, DMARC and ARC prove which domain handled a message, and the danger is that a pass is read as more than it means. These entries treat the protocols as trust signals that can be weaponised, in both the signing and the verifying role.

ID	THREAT	MITIGATION
AU·A	Pass as Endorsement The platform treats an authentication pass as a trust signal (filter bypass, reputation boost, a badge), though any attacker-owned domain can pass. STRIDE S (Loose) · CAPEC None · CWE Partial: CWE-654	An authentication pass asserts the sending domain and nothing else. (1) Feed authentication results only into DMARC disposition and domain reputation, never into filter bypass, score reduction or trust badges. (2) Evaluate domain reputation (age, history, similarity to known domains) as a separate input that an authentication pass cannot raise.
AU·K	Cross-Tenant Identity Shared sending infrastructure lets one tenant emit mail that authenticates as another tenant's domain. STRIDE S (Clean) · CAPEC Partial: CAPEC-151, CAPEC-195 · CWE Direct: CWE-283, CWE-291	Each tenant can authenticate only for domains it has proven it owns, and a shared upstream identifies its customers by something they cannot set. (1) Reject submission when the envelope sender or From domain is not in the tenant's verified domain list, and when accepting outbound mail from a shared upstream, identify the customer from a property that upstream stamps and the sender cannot forge (a tenant identifier header or a per-tenant certificate), never from the connecting IP. (2) Issue DKIM keys per tenant and per domain, and never sign a message with a key belonging to another tenant. (3) Audit outbound mail per tenant against that tenant's verified domains, and alert on any signed message whose domain the tenant does not own. (4) Give each tenant on a shared upstream its own inbound connector with its own certificate, so a tenant cannot present itself as another even to the upstream.
AU·Q	DKIM Replay A message the platform signed is re-sent to arbitrary recipients, because the signature binds neither recipient nor time. STRIDE S (Clean) · CAPEC Partial: CAPEC-60 · CWE Direct: CWE-294	A DKIM signature binds a message to its intended recipients and a time window. (1) Sign the To, Cc and Date headers, oversign them, and set a short expiry (x= tag) on every signature. (2) Limit the signing of mail from new, free or unverified accounts, and detect replay by rate-limiting identical signed messages per signature. (3) Monitor for the platform's own signatures appearing on mail that did not pass through its outbound path (a DKIM replay feed or recipient reports), and revoke the selector when replay is detected.

ID	THREAT	MITIGATION
AU-J	Partial Signature Coverage The signer leaves headers or body unsigned, or the verifier honours l= and tolerates duplicate headers, so content changes under a valid signature. ----- STRIDE S, T (Clean) · CAPEC Direct: CAPEC-477 · CWE Direct: CWE-349, CWE-347	A signature covers everything the recipient will see, and the verifier treats partial coverage as unsigned. (1) Sign and oversign From, To, Subject, Date, Reply-To, Content-Type and MIME-Version; do not use the l= tag when signing. (2) As a verifier, treat l= signatures and duplicated single-instance headers as a DKIM failure.
AU-10	Alignment Confusion The identifier that authentication verified is not the one the client displays: a second From header, a Sender or Resent-From standing in for a missing From, or a display name is shown while the evaluator checked something else. ----- STRIDE S (Clean) · CAPEC Partial: CAPEC-43, CAPEC-476 · CWE Direct: CWE-436, CWE-451	One identifier is authenticated, and the client displays only that identifier, parsed the same way. (1) Reject at SMTP time any message with no From header, more than one, or one that does not parse. (2) Share one address-parsing library between the DMARC evaluator and every client, tested against the same corpus of malformed headers, and never show Sender, Resent-From or a display name in place of the authenticated From.
AU-9	Identifier Handoff An authentication check silently substitutes one identifier for another: SPF verifies the HELO name because MAIL FROM is empty or does not resolve, and DMARC then aligns that pass against the MAIL FROM it never checked. ----- STRIDE S (Clean) · CAPEC Partial: CAPEC-475 · CWE Partial: CWE-1390	Every authentication result names the identifier it verified, and no result is applied to an identifier it did not check. (1) Record the checked identifier (HELO or MAIL FROM) in the SPF result, and have DMARC treat an SPF pass on HELO as no SPF result for MAIL FROM alignment. (2) Handle an empty or unresolvable MAIL FROM as a case of its own with an explicit policy rather than a silent substitution, and test the evaluator with messages engineered to make the preferred identifier fail.
AU-8	Laundered Trust Forwarders, mailing lists and ARC seals from untrustworthy intermediaries override an authentication failure. ----- STRIDE S (Clean) · CAPEC Partial: CAPEC-21 · CWE Direct: CWE-807	Only sealers the platform has deliberately trusted can override an authentication failure. (1) Maintain a short, reviewed list of trusted ARC sealers, and ignore ARC results from any sealer not on it. (2) Alert when a trusted sealer's override rate changes sharply, and have a procedure to remove a sealer within hours.

ID	THREAT	MITIGATION
AU-7	Weak or Shared Keys Signing keys are short, shared across tenants, never rotated, or their selectors are never retired. STRIDE S (Clean) · CAPEC Direct: CAPEC-485, CAPEC-474 · CWE Partial: CWE-326, CWE-324, CWE-653	Signing keys are strong, per tenant, rotated, and retired when their selectors are. (1) Generate 2048-bit RSA or Ed25519 keys per tenant and domain, and store them in an HSM or key management service. (2) Rotate keys on a fixed schedule with dual selectors, and remove the retired selector's DNS record after the rotation window. (3) Record every signing operation against the tenant and key that performed it, and alert on a key used for a domain it was not issued for. (4) Keep an inventory of published selectors per domain and remove any whose key is no longer in the key store.
AU-6	Error as Pass Temporary and permanent evaluation errors (lookup limits, timeouts, malformed records) are treated as neutral or pass, and a sender can induce them. STRIDE S (Loose) · CAPEC Partial: CAPEC-115 · CWE Direct: CWE-636	An authentication error has its own disposition, never silently mapped to pass or none. (1) Treat temperror as defer and permerror as fail for domains with a published policy. (2) Log the error class in Authentication-Results and expose it as a distinct input to downstream policy and scoring.
AU-5	Policy Override Local allow lists, exemptions or softened dispositions silently void the domain owner's published policy. STRIDE S, E (Loose) · CAPEC None · CWE Partial: CWE-183, CWE-696	The domain owner's published policy is overridden only by an explicit, scoped and visible exception. (1) Enforce DMARC reject and quarantine before allow lists are consulted, and make any exemption a per-sender, time-limited rule. (2) Report overridden dispositions to the domain owner in aggregate reports, and show the tenant admin a list of active overrides.
AU-4	Signing Oracle The platform signs content it did not originate, such as forwards, bounces, auto-replies and notifications carrying attacker-chosen content. STRIDE S (Clean) · CAPEC None · CWE Direct: CWE-441	The platform signs only content that originates from an authenticated sender it is authorised for. (1) Do not sign auto-forwards, bounces or notifications that carry third-party content with a tenant's domain; use a dedicated subdomain with its own policy instead. (2) Strip or quote attacker-controlled content in auto-replies and notifications to what is needed for the recipient to act. (3) Rate-limit automatic mail per account and per trigger, and refuse to sign automatic mail whose content exceeds a size or structure budget.

ID	THREAT	MITIGATION
AU-3	Signal Stripping Removing a signature or a record downgrades evaluation to a weaker path instead of raising suspicion. <hr/> STRIDE S, T (Clean) · CAPEC Partial: CAPEC-620 · CWE Partial: CWE-636, CWE-757	The absence of an expected signal is a failure, not a downgrade. (1) Record per sending domain whether it normally signs, and treat an unsigned message from a signing domain as a DKIM failure. (2) Require DKIM alignment, not SPF alone, for domains whose history shows consistent signing.
AU-2	Report Channel Abuse Aggregate and failure reports leak message data, go to unverified destinations, or are used for amplification. <hr/> STRIDE I, D (Clean) · CAPEC Partial: CAPEC-490 · CWE Partial: CWE-201, CWE-406	Reports go only to verified destinations, contain only what is needed, and are rate-limited. (1) Check the external destination verification record before sending any report to a different domain. (2) Redact message bodies from failure reports, and cap the number of reports sent per domain per hour.



Client protocols (CP)

Client access is where a mailbox is read, copied and reconfigured, so a weakness here exposes everything the rest of the platform protected. These entries cover IMAP, POP and SMTP submission, plus EWS, ActiveSync, JMAP and vendor APIs.

ID	THREAT	MITIGATION
CP·A	Legacy Authentication Protocol endpoints accept password-only authentication that bypasses MFA and access policy. STRIDE S, E (Clean) · CAPEC Partial: CAPEC-115, CAPEC-565 · CWE Direct: CWE-420, CWE-308	Every protocol endpoint enforces the same authentication and access policy as the web login. (1) Disable password-only and app-password authentication by default, and require OAuth or a device-bound credential on IMAP, POP and submission. (2) Evaluate conditional access (MFA, device, location) at the protocol gateway, not only at the web login. (3) Report per tenant which accounts still use legacy authentication and give the tenant a date-driven path to retire it, with telemetry on what would break. (4) Treat an authentication through a legacy protocol as a lower-assurance session with reduced rights (read-only, no rule changes, no export).
CP·K	Credential Exposure in Transit STARTTLS stripping, commands injected before the TLS upgrade, or cleartext fallback expose credentials. STRIDE I (Clean) · CAPEC Direct: CAPEC-620, CAPEC-157 · CWE Direct: CWE-319, CWE-523	Credentials are never accepted on a connection that is not already encrypted. (1) Offer implicit TLS ports only (993, 995, 465) and remove STARTTLS listeners for authentication. (2) If STARTTLS must be kept, discard any input buffered before the TLS handshake and reject AUTH before the upgrade.
CP·Q	Token and Session Persistence Tokens and sessions are over-scoped, unbound to a device, or survive a password reset. STRIDE S, E (Clean) · CAPEC Partial: CAPEC-60, CAPEC-593 · CWE Partial: CWE-613, CWE-1220	A credential change revokes every token and session, and tokens are bound to what they were issued to. (1) Revoke refresh tokens and active sessions on password reset, account disable and MFA change, propagating within minutes. (2) Bind tokens to the client (DPoP or mTLS) and scope them to the narrowest mail permission the client needs. (3) Expire sessions and tokens on an absolute lifetime as well as an idle one, and re-check account state (disabled, held, reset) on every token refresh.

ID	THREAT	MITIGATION
CP-J	Sync as Exfiltration Full mailbox replication by a new client is indistinguishable from normal use. <hr/> STRIDE I (Loose) · CAPEC None · CWE Partial: CWE-778	A new client's first full sync is visible and can be limited. (1) Notify the mailbox owner and tenant admin when a new client authenticates, and show its first-sync volume in the audit log. (2) Allow tenants to limit unmanaged clients to recent mail and to require approval for full-mailbox sync.
CP-10	Mailbox State Manipulation Rules, forwarding, delegation or appended messages are set through the protocol without any signal to the owner. <hr/> STRIDE T, R (Clean) · CAPEC Partial: CAPEC-176 · CWE Partial: CWE-223, CWE-1188	Any change to how a mailbox routes or shares mail is notified to its owner. (1) Send an out-of-band notification (push or SMS) when a rule, forward or delegate is created through any protocol. (2) Block external auto-forwarding rules by default and require admin approval per rule.
CP-9	Credentials and Caches at Rest Clients and intermediary services store credentials and mailbox copies outside the platform's control. <hr/> STRIDE I (Clean) · CAPEC Partial: CAPEC-37, CAPEC-204 · CWE Partial: CWE-522, CWE-524	The platform controls where its credentials and mail copies end up. (1) Issue short-lived tokens so no client holds a long-lived secret, and refuse third-party intermediaries that store user credentials. (2) Support remote wipe of client caches and enforce it through device-management APIs for managed clients.
CP-8	Autodiscovery Hijack Client configuration discovery sends credentials to an unintended or attacker-controlled host. <hr/> STRIDE S, I (Clean) · CAPEC Partial: CAPEC-154 · CWE Direct: CWE-923, CWE-941	A client sends credentials only to a host it has verified belongs to the mailbox provider. (1) Publish autodiscovery over HTTPS only, and have clients verify the certificate and domain match before sending any credential. (2) Fail closed: when the expected discovery host does not resolve, prompt the user rather than trying alternative hostnames.
CP-7	Authentication Oracle Differing responses or timing allow account enumeration and password spraying, with throttling inconsistent across protocols. <hr/> STRIDE I, S (Clean) · CAPEC Direct: CAPEC-575, CAPEC-565, CAPEC-49 · CWE Direct: CWE-204, CWE-208, CWE-307	Authentication responses and limits are uniform across users, errors and protocols. (1) Return an identical response and timing for unknown user, wrong password and locked account. (2) Share the throttling and lockout counters across IMAP, POP, submission, API and web login.

ID	THREAT	MITIGATION
CP-6	Third-Party Delegation App consent grants broad, durable mailbox access that the owner cannot easily see or revoke. <hr/> STRIDE E (Loose) · CAPEC Partial: CAPEC-122 · CWE Partial: CWE-1220	Third-party access is narrowly scoped, visible to the owner and revocable in one place. (1) Offer granular mail scopes (read recent, send only, folder-limited) and require admin consent for full-mailbox scopes. (2) Give users and admins a single page listing every app with mailbox access, with one-click revocation.
CP-5	Cross-Mailbox Access Shared folders, delegation or impersonation features allow access beyond the authenticated identity. <hr/> STRIDE E, I (Clean) · CAPEC Direct: CAPEC-1, CAPEC-180 · CWE Direct: CWE-863, CWE-639	Authorisation is checked on every object, on every request, against the authenticated identity. (1) Use per-mailbox, unguessable object identifiers and check ownership on every fetch, not only when listing. (2) Restrict impersonation rights to specific service accounts, log every impersonated request, and alert on impersonation of privileged users. (3) Test authorisation with an automated suite that requests every object type as a different user, a different tenant and a delegate, and fails the build on any success.
CP-4	Protocol Command Abuse Malformed or expensive commands (literals, searches, large fetches) cause injection or resource exhaustion on the server. <hr/> STRIDE T, D (Clean) · CAPEC Direct: CAPEC-183, CAPEC-130 · CWE Partial: CWE-770, CWE-943	Every command is bounded, isolated per user and never interpolated into a backend query. (1) Cap command length, literal size, search complexity and concurrent connections per session and per user. (2) Pass search terms as parameters to the index, never by string concatenation, and run searches with a per-tenant resource budget.
CP-3	Lockout as Denial of Service An attacker who knows a username can lock the account on demand by failing authentication deliberately, cutting the target off from mail at a moment of the attacker's choosing. <hr/> STRIDE D (Clean) · CAPEC Direct: CAPEC-2 · CWE Direct: CWE-645	Lockout protects the account without handing an attacker an off switch. (1) Lock out the source (address, device, session) rather than the account, and escalate to a risk-based challenge for the account itself. (2) Keep already-authenticated sessions alive through a lockout and give the mailbox owner a trusted recovery path that does not depend on the locked credential.
CP-2	Notification Leakage Push notifications and previews expose message content to third-party services and lock screens. <hr/> STRIDE I (Clean) · CAPEC None · CWE Direct: CWE-201, CWE-359	Notification payloads contain nothing the recipient would not want on a lock screen or a third-party server. (1) Send content-free push alerts and have the client fetch the preview over an authenticated channel. (2) Let tenants disable previews and sender names in notifications for sensitive mailboxes.



LAYER 04 OF 09 · THE EMAIL STACK

SMTP (SM)

PAR AVION
BY AIR MAIL

SMTP accepts whatever identity a peer asserts and secures each hop only if both ends insist. These entries cover the MTA-to-MTA conversation: identity, relay, transport security and parsing.

ID	THREAT	MITIGATION
SM·A	Unauthenticated Identity Assertion The server accepts any claimed envelope sender, header From and HELO identity. STRIDE S (Clean) · CAPEC Direct: CAPEC-194, CAPEC-151 · CWE Direct: CWE-346, CWE-807, CWE-350	Asserted identities are recorded but never acted on until something verifiable confirms them. (1) Base connector, routing and trust decisions on a verified property (authenticated session, client certificate, DKIM-aligned domain), never on HELO, PTR or envelope sender alone. (2) Treat a mismatch between HELO, PTR and connecting IP as a risk signal rather than an identity.
SM·K	Relay Abuse Open relays, permissive connectors or trusted-IP rules let others send through the platform. STRIDE S, E (Clean) · CAPEC Partial: CAPEC-212 · CWE Direct: CWE-441, CWE-291	Relay is granted to authenticated identities, never to network locations. (1) Require SMTP AUTH or a client certificate for any relay to a domain the platform does not host. (2) Review relay rules automatically and alert when a rule covers a shared cloud range or more than a small number of addresses.
SM·Q	TLS Downgrade STARTTLS is stripped or certificates go unvalidated, exposing mail in transit. STRIDE I, T (Clean) · CAPEC Direct: CAPEC-620, CAPEC-94, CAPEC-217 · CWE Direct: CWE-319, CWE-295, CWE-757	Transport security is enforced where the peer demands it and verified where the platform can. (1) Honour MTA-STS and DANE on outbound delivery, deferring rather than falling back to cleartext when the policy requires TLS. (2) Publish an MTA-STS policy in enforce mode and TLS-RPT for the platform's own domains. (3) Verify the peer's certificate chain and hostname for every outbound session, and report the result in TLS-RPT and in a per-domain delivery dashboard. (4) Require TLS 1.2 or later with a modern cipher list on both inbound and outbound, and record the negotiated version per session for audit.

ID	THREAT	MITIGATION
SM-J	SMTP Smuggling Two MTAs disagree on the end-of-data sequence, letting a sender inject a second message with a forged envelope. <hr/> STRIDE S, T (Clean) · CAPEC Partial: CAPEC-33 · CWE Direct: CWE-436, CWE-147	Both ends of every SMTP hop agree on where a message ends. (1) Accept only CRLF.CRLF as end of data, and reject or normalise bare CR and bare LF on input and output. (2) Test every MTA pair in the path against each other's handling of non-standard line endings and include the test in release checks. (3) Close the session, rather than accepting the data, when the end-of-data sequence is ambiguous, and log the peer for follow-up.
SM-10	Recipient Enumeration Recipient responses, their timing or later bounces reveal which addresses exist, so an attacker can harvest a tenant's directory. <hr/> STRIDE I (Clean) · CAPEC Direct: CAPEC-575 · CWE Direct: CWE-204, CWE-208	Invalid recipients are refused in session, uniformly, and probing is rate-limited. (1) Reject unknown recipients at RCPT TO with the same response and timing as valid-but-throttled ones. (2) Disable VRFY and EXPN and rate-limit RCPT failures per connecting IP and per sender.
SM-9	Command and Header Injection A metacharacter in an address, domain or field reaches a component that composes SMTP commands, message headers or the platform's own Authentication-Results, and is read as structure rather than data. <hr/> STRIDE T (Clean) · CAPEC Direct: CAPEC-134, CAPEC-41, CAPEC-183 · CWE Direct: CWE-93, CWE-116, CWE-77	No input can change the structure of a command, header or result the platform composes. (1) Reject CR, LF, parentheses, quotes and other delimiter characters in every address, domain, subject and custom header value at the boundary where it enters the platform. (2) Compose messages, commands and Authentication-Results with a library that encodes values as data, forbid string concatenation in code review and linting, and have the DMARC evaluator read results from a typed internal record rather than by re-parsing the header.
SM-8	Shared Reputation Poisoning One tenant's abuse burns the shared IP addresses and domains every tenant sends from. <hr/> STRIDE D (Loose) · CAPEC None · CWE Partial: CWE-653	Outbound reputation is segmented so one tenant's abuse cannot burn another's. (1) Start new and unverified tenants on a separate IP pool, and promote them to shared pools only after a clean sending history. (2) Detect abusive sending within minutes (bounce rate, complaint rate, volume spikes) and move the tenant to an isolated pool automatically.
SM-7	Submission Identity Mismatch An authenticated submitter can send with a From or envelope sender that is not theirs. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-195 · CWE Direct: CWE-862	A submitted identity is checked against what the authenticated user may use. (1) Verify that From and envelope sender match the authenticated user's own addresses or an explicitly granted send-as right. (2) Record send-as and send-on-behalf grants as auditable permissions and show them to the mailbox owner.

ID	THREAT	MITIGATION
SM-6	Resource Exhaustion Connection floods, slow senders, queue filling and mail bombing degrade or stop delivery. ----- STRIDE D (Clean) · CAPEC Direct: CAPEC-125, CAPEC-227, CAPEC-130 · CWE Direct: CWE-770	Resources are limited per peer, per sender and per tenant so that volume against one cannot stop delivery for all. (1) Set connection, rate and queue limits per connecting IP, per sender domain and per recipient, with separate tenant queue capacity. (2) Detect mail bombing by recipient-level volume anomalies and divert the excess to a holding queue rather than the inbox. (3) Keep a separate, protected ingress path for mail from known-good senders and for tenant-critical flows (authentication codes, alerts) so that a flood cannot delay them.
SM-5	Trace Forgery Received headers are forged or stripped while platform decisions or forensics rely on them. ----- STRIDE R, T (Clean) · CAPEC Partial: CAPEC-93, CAPEC-194 · CWE Direct: CWE-349, CWE-807	Only trace records the platform wrote are used for decisions, and the boundary is unambiguous. (1) Mark the platform's own Received headers with a verifiable token and ignore any trace header below the first one the platform wrote. (2) Keep the platform's routing and forensic records in its own logs, keyed to the message, not in the message.
SM-4	Extension Differential Hops handle extensions (pipelining, chunking, SMTPUTF8, 8BITMIME) inconsistently, creating exploitable disagreement. ----- STRIDE T (Loose) · CAPEC Partial: CAPEC-43 · CWE Direct: CWE-437, CWE-436	Every control handles every advertised extension, or the extension is not advertised. (1) Apply the same content hooks to BDAT (CHUNKING) as to DATA, and test each scanner against both paths. (2) Convert or reject messages that use an extension the next hop does not support rather than passing them through unchanged.
SM-3	Address Parsing Differential Quoted local parts, comments, aliases and rewriting make an address route differently from how it was validated. ----- STRIDE T, S (Clean) · CAPEC Partial: CAPEC-43 · CWE Direct: CWE-436, CWE-179	One parser validates, routes and displays addresses, and rewriting is re-checked. (1) Use a single address-parsing library across validation, routing and display, with a shared test corpus of quoted local parts, comments and non-ASCII addresses. (2) Re-apply recipient policy after alias expansion, sub-address stripping and rewriting, using the final mailbox identity. (3) Reject addresses that use syntax the platform has no business accepting (comments, quoted local parts with control characters, source routes) at the first hop.

ID	THREAT	MITIGATION
SM-2	<p>Backscatter Reflection</p> <p>A bounce or auto-reply for a message with a forged envelope sender goes to the victim named in it, so the platform delivers attacker content under its own good reputation.</p> <hr/> <p>STRIDE D, S (Clean) · CAPEC Partial: CAPEC-490 · CWE Direct: CWE-441</p>	<p>The platform never sends mail to an identity it has not verified, and bounces are mail.</p> <ol style="list-style-type: none"> (1) Reject in session so that no bounce is needed; where a later bounce is unavoidable, send it only when the envelope sender passed SPF or DKIM, and omit the original content. (2) Cap bounces and auto-replies per destination domain and suppress them entirely for mail that failed authentication.



MIME and S/MIME (MI)

Every component that handles a message should interpret it the same way, and most content attacks live where they do not. These entries cover how content is parsed, decoded, rendered, signed and encrypted.

ID	THREAT	MITIGATION
MI-A	Structure Differential Malformed boundaries or nesting make the scanner and the client see different body structures. STRIDE T (Loose) · CAPEC Partial: CAPEC-43 · CWE Direct: CWE-436, CWE-437	The structure the scanner inspects is the structure the client renders. (1) Parse once at ingress into a canonical MIME tree, reject messages that parse ambiguously, and deliver the canonical form. (2) Run differential tests between the scanner's parser and each supported client's parser on a corpus of malformed messages. (3) Deliver to the client a message the platform has re-serialised from its canonical tree, so the client never sees the bytes the scanner did not.
MI-K	Encoding Abuse Encoded-words, charset tricks and transfer-encoding quirks disguise content from inspection. STRIDE T (Clean) · CAPEC Direct: CAPEC-267, CAPEC-120, CAPEC-71, CAPEC-80 · CWE Direct: CWE-173, CWE-180	Content is decoded to a canonical form before inspection, in the same way the client decodes it. (1) Fully decode transfer encodings and encoded-words before every inspection, and treat undecodable content as unscanned. (2) Normalise charsets to UTF-8 and reject or flag nested, invalid or conflicting encodings. (3) Decode in a sandboxed worker with limits on size, depth and time, and treat hitting a limit as a verdict in its own right (see Nesting and Decompression Exhaustion).
MI-Q	Content-Type Confusion The declared type differs from the actual type, or a file is valid as several types at once. STRIDE T (Clean) · CAPEC Partial: CAPEC-209, CAPEC-636 · CWE Direct: CWE-430, CWE-646	A file's type is determined by its content, and all components agree on it. (1) Sniff the actual type of every attachment and scan by that type regardless of declaration or extension. (2) Block or rename attachments whose declared, extension and sniffed types disagree, and render previews only by sniffed type.

ID	THREAT	MITIGATION
MI-J	Active and Remote Content HTML and CSS track, exfiltrate or fetch content the platform never inspected. STRIDE I, E (Loose) · CAPEC None · CWE Partial: CWE-79, CWE-829	No content in a message can cause a fetch or execute code without the recipient's decision. (1) Sanitise HTML with an allow list that removes scripts, forms, external CSS and conditional comments. (2) Block remote content by default and, when loaded, fetch it through a proxy that re-scans it and strips tracking parameters. (3) Render HTML in the client inside an isolated frame with no script, no form submission and a content security policy that permits only proxied images.
MI-10	Signature Stripping and Wrapping A signature is removed, or made to appear to cover content it does not. STRIDE S, T (Clean) · CAPEC Direct: CAPEC-477 · CWE Direct: CWE-349, CWE-451	The interface shows exactly what a signature covers and nothing more. (1) Display a signature indicator per signed part, never for the whole message, and mark unsigned parts visibly. (2) Refuse to render signed and unsigned parts as one continuous body.
MI-9	Encryption as Blindfold and Oracle Encrypted content blinds the scanner, and malleable ciphertext leaks plaintext through the client. STRIDE I (Clean) · CAPEC Partial: CAPEC-463 · CWE Partial: CWE-353, CWE-636	Content the platform cannot inspect is handled by explicit policy, and clients reject malleable ciphertext. (1) Hold or flag encrypted mail the platform cannot decrypt, with the choice set per tenant and defaulting to a visible warning. (2) Require authenticated encryption, refuse to render modified ciphertext, and never load remote content from decrypted parts.
MI-8	Header Differential Duplicate, folded or malformed headers are read differently by different components. STRIDE T (Loose) · CAPEC Partial: CAPEC-43 · CWE Direct: CWE-436, CWE-235	Every component reads the same header occurrence, and ambiguity is rejected. (1) Reject at ingress any message with duplicate single-instance headers (From, Subject, Date, Message-ID). (2) Normalise header folding and whitespace once at ingress and pass the normalised message to every later component.
MI-7	Attachment Identity Deception Filename continuations, right-to-left overrides and double extensions misrepresent what an attachment is. STRIDE S (Clean) · CAPEC Direct: CAPEC-635, CAPEC-649 · CWE Direct: CWE-451, CWE-436	The attachment name a user sees is the name every component used, and it cannot misrepresent the type. (1) Strip or visibly render bidirectional control characters and zero-width characters in filenames. (2) Use one filename resolution across scanner and client when parameters disagree, and show the sniffed type next to the name.

ID	THREAT	MITIGATION
MI-6	Nesting and Decompression Exhaustion Archive bombs and deeply nested messages exhaust the parser or push it past its limits. <hr/> STRIDE D (Clean) · CAPEC Direct: CAPEC-197, CAPEC-230 · CWE Direct: CWE-409, CWE-674	Decompression and nesting limits are enforced while expanding, and reaching one is a verdict. (1) Enforce depth, ratio and total-size limits during expansion, aborting the moment a limit is hit. (2) Treat a hit limit as UNSCANNED (see Fail-Open Scanning) and expand archives in an isolated, time-bounded process.
MI-5	Embedded Format Blind Spots Attached messages, TNEF, calendar items, partial and external-body parts carry content the scanner does not unpack. <hr/> STRIDE T (Loose) · CAPEC Partial: CAPEC-636 · CWE Direct: CWE-437	Every container format the client opens is a format the scanner unpacks. (1) Maintain one list of container formats (message/rfc822, TNEF, calendar, archives) shared by the scanners and the client, and test coverage against it. (2) Refuse message/partial and message/external-body, and inspect calendar fields (location, description, URL) as body content.
MI-4	Display Divergence Text and HTML alternatives differ, or conditional styling changes what is shown in another client or after forwarding. <hr/> STRIDE S, T (Loose) · CAPEC Partial: CAPEC-148 · CWE Direct: CWE-437, CWE-451	Every alternative and every rendering variant is inspected. (1) Scan all MIME alternatives, not only the preferred one, and flag messages whose alternatives differ materially. (2) Strip CSS and markup that hides or reveals content conditionally (display:none, media queries, mso conditionals).
MI-3	Parser Memory Safety Complex untrusted formats are parsed in privileged processes such as scanners, converters and preview generators. <hr/> STRIDE E, T (Clean) · CAPEC Direct: CAPEC-100, CAPEC-28 · CWE Direct: CWE-653, CWE-250	Untrusted content is parsed in an isolated process with no access to anything else. (1) Run parsers, converters and preview generators in sandboxed, network-less workers with no credentials and no access to other messages. (2) Prefer memory-safe parser implementations and automate parser library updates with a short deployment deadline. (3) Apply resource limits (CPU, memory, time, file descriptors) per parse and treat a limit hit as a verdict, not as a crash to retry.

ID	THREAT	MITIGATION
MI-2	<p>Certificate and Key Handling</p> <p>Certificates are accepted with mismatched addresses or unchecked revocation, or private keys are escrowed where a compromise exposes all mail.</p> <p>STRIDE S, I (Clean) · CAPEC Direct: CAPEC-475, CAPEC-474 · CWE Partial: CWE-295, CWE-299, CWE-653</p>	<p>Certificates are validated against the sender shown, revocation is checked, and private keys are compartmentalised.</p> <ul style="list-style-type: none">(1) Match the certificate's email address to the displayed From, check revocation, and treat an unavailable revocation check as failure.(2) Hold private keys per tenant in an HSM or KMS with per-operation access control, never in a shared store beside the scanner.(3) Separate signature verification from decryption so that a verification failure is reported even when the message decrypts, and never show a verified mark for a message whose signature covers only part of it.



LAYER 06 OF 09 · THE EMAIL STACK

DNS layer (DN)

PAR AVION
BY AIR MAIL

DNS decides where mail goes and who may send it, so whoever controls or falsifies an answer controls the mail. These entries cover the records the platform publishes, hosts for tenants and resolves.

ID	THREAT	MITIGATION
DN-A	MX Redirection Cache poisoning, DNS account hijack or route hijack sends mail for a domain to an attacker. STRIDE S, T (Clean) · CAPEC Direct: CAPEC-142, CAPEC-585, CAPEC-598 · CWE None	The platform notices when mail for a domain stops arriving at it, and protects its own records. (1) Monitor inbound volume per hosted domain and alert on an unexpected drop or an MX that no longer points at the platform. (2) Protect the platform's registrar and DNS accounts with hardware MFA, change alerts and registry lock.
DN-K	Dangling Mail Records MX, delegated DKIM selectors or SPF includes point at deprovisioned resources someone else can claim. STRIDE S, E (Clean) · CAPEC None · CWE Partial: CWE-672	Deprovisioning removes or neutralises every record that pointed at the resource. (1) Generate per-tenant, unguessable hostnames and selectors so a departed tenant's records cannot be claimed by a new one. (2) Run a deprovisioning checklist that revokes keys, retires selectors and reserves the tenant's hostnames for a cooling-off period.
DN-Q	Unauthenticated Answers Without DNSSEC validation, every lookup the platform relies on (MX, SPF, DKIM, DMARC, MTA-STS, block lists) can be answered by whoever reaches the resolver first. STRIDE S, T (Clean) · CAPEC Direct: CAPEC-598, CAPEC-142 · CWE Direct: CWE-353, CWE-346	Lookups the platform relies on are authenticated, and validation failure is handled deliberately. (1) Use DNSSEC-validating resolvers and treat validation failure as a temporary error (defer), not as "no record". (2) Sign the platform's own mail zones so that recipients and senders can validate the records they look up.
DN-J	Transport Policy Downgrade MTA-STS policy or TLSA records are stripped, stale or taken over. STRIDE T, I (Clean) · CAPEC Partial: CAPEC-620 · CWE Partial: CWE-636	A transport policy that disappears or breaks raises suspicion rather than silently relaxing security. (1) Keep the MTA-STS policy host under the platform's own certificate automation with expiry alerts well in advance. (2) Cache sender-side policies and treat a previously seen policy that vanishes as a downgrade attempt to be deferred.

ID	THREAT	MITIGATION
DN-10	Domain Lifecycle Gap The platform keeps trusting, or holding mailboxes for, a tenant domain whose ownership has lapsed or changed. <hr/> STRIDE S (Loose) · CAPEC None · CWE Direct: CWE-283, CWE-672	Domain ownership is a continuing condition, re-verified over the life of the tenant. (1) Re-verify domain ownership on a schedule and on registrar change events, and suspend sending rights when verification fails. (2) Expire mailboxes, keys and sending rights for a domain whose ownership has lapsed, with a notified grace period. (3) Monitor registrar WHOIS and NS changes for every verified domain and treat a change of registrant or nameserver as a re-verification event. (4) Give the tenant admin a page listing every domain, its verification state and the date it was last proven.
DN-9	Weak Ownership Verification Tenant onboarding verifies a domain with a weak, replayable or never-rechecked proof. <hr/> STRIDE S (Clean) · CAPEC None · CWE Direct: CWE-283, CWE-340	Ownership proof is unique, single-use and specific to the claim being made. (1) Issue a random, single-use verification token per tenant per domain, and never derive it from the domain name. (2) Reject a claim to a domain or overlapping subdomain already verified by another tenant, and separate subdomain rights from parent rights. (3) Require the proof record to be present and correct at every re-verification, not only at onboarding, and remove the tenant's rights when the record disappears.
DN-8	Resolver Trust The platform's resolvers are poisonable, shared across tenants, or treat attacker-controlled answers as safe input. <hr/> STRIDE S, T (Clean) · CAPEC Direct: CAPEC-142 · CWE Partial: CWE-331, CWE-653	Resolvers are dedicated, validating and bound what they accept from the network. (1) Run dedicated, DNSSEC-validating resolvers on private addresses with source-port and transaction-ID randomisation. (2) Bound answer size, record count and TTL before passing any answer to an authentication or routing component. (3) Rate-limit queries per sending domain and per message so that one sender cannot use the resolver to amplify work against third parties (see Lookup Amplification). (4) Keep an independent second resolver path for critical lookups and compare answers when they disagree.
DN-7	Lookup Amplification Authentication checks trigger sender-directed DNS queries that exhaust the resolver or reflect onto a victim. <hr/> STRIDE D (Clean) · CAPEC Direct: CAPEC-490 · CWE Direct: CWE-405, CWE-406	Sender-controlled records cannot make the platform do unbounded work. (1) Enforce the SPF limit of ten DNS-querying mechanisms and void lookups, and treat exceeding it as permerror. (2) Cap total DNS queries per inbound message and per sender domain per minute, and cache negative results.

ID	THREAT	MITIGATION
DN-6	DNS Failure Semantics Lookup failures are treated as "no policy", and fallbacks such as implicit MX are followed unsafely. <hr/> STRIDE D, S (Loose) · CAPEC Partial: CAPEC-589 · CWE Direct: CWE-636, CWE-754	Each DNS failure mode has a defined, deliberate meaning. (1) Distinguish timeout, SERVFAIL and NXDOMAIN in every lookup, and map temporary failures to defer rather than "no policy". (2) Honour null MX and never fall back to an A or AAAA record for a domain that publishes one.
DN-5	Reputation Feed Dependency DNS-based blocklists are an integrity and availability dependency that can fail, lapse or be poisoned. <hr/> STRIDE D, T (Loose) · CAPEC Partial: CAPEC-589 · CWE Direct: CWE-654, CWE-1357	No single external feed can stop or open the mail flow on its own. (1) Require agreement between at least two reputation sources for a reject, and treat a list answering "listed" for a known-good test address as broken. (2) Monitor each list's responsiveness and domain registration, and fail to neutral when a list is unreachable.
DN-4	Cached Policy Poisoning A bad policy or record, once cached, outlives the attack that planted it. <hr/> STRIDE T (Clean) · CAPEC Direct: CAPEC-141 · CWE None	Cached policy cannot outlive the trust it was based on. (1) Cap the lifetime honoured for cached policies and records regardless of the published TTL. (2) Provide an operator control to flush cached entries for one domain, and alert on sudden changes to long-lived policies.
DN-3	Signing Failure Outage The platform's own signed zones or validating resolvers go dark: an expired signature, a failed key rollover or a validation bug makes every record the platform publishes or depends on unresolvable, and all mail stops. <hr/> STRIDE D (Loose) · CAPEC None · CWE None	The platform's own DNS cannot silently expire, and its failure is detected before the mail stops. (1) Automate key rollover and signature refresh, and monitor signature expiry and validation from an external validating resolver. (2) Rehearse rollover and recovery in a staging zone, and keep an emergency procedure to republish or unsign the zone.
DN-2	Internationalised Domain Confusion Punycode, homoglyph and malformed domains (NUL, invisible characters, a trailing period) are compared, resolved or displayed inconsistently across components. <hr/> STRIDE S (Clean) · CAPEC Direct: CAPEC-632, CAPEC-52 · CWE Direct: CWE-1289, CWE-1007, CWE-158	Domains are normalised to one canonical form before any component compares, resolves or displays them. (1) Normalise every domain to its A-label form at ingress, rejecting labels with control characters, NUL or invisible code points, and apply the same normalisation to allow lists, block lists, DNS lookups and authentication. (2) Flag mixed-script labels and labels confusable with a known contact's domain, and display them in a visibly distinct form.



Content scanners (CS)

A scanner is a probabilistic control that an attacker can study, evade and attack directly. These entries cover URL analysis, malware detection, sandboxes, machine learning (ML) and large language model (LLM) classifiers, and data loss prevention (DLP).

ID	THREAT	MITIGATION
CS-A	Analysis-Aware Content Content or a URL detects the scanner (IP range, user agent, sandbox artefacts, timing) and behaves benignly for it. STRIDE T (Loose) · CAPEC Partial: CAPEC-224 · CWE Partial: CWE-205	The scanner's view of content is indistinguishable from a user's. (1) Fetch URLs from residential-like, rotating egress with realistic browser fingerprints, and detonate samples in sandboxes that resemble real endpoints. (2) Treat "nothing happened" as inconclusive rather than clean, and combine it with destination reputation before deciding. (3) Rotate and measure the detonation environment's fingerprints against real user traffic, and rebuild it when attackers begin to distinguish it.
CS-K	Scanner Prompt Injection Message content is interpreted as instructions by an LLM-based classifier, summariser or assistant. STRIDE T, E (Loose) · CAPEC None · CWE Direct: CWE-1427	Message content is data to a model, never instructions, and no security decision depends on the model resisting it. (1) Pass message content to the classifier as a delimited, typed input with no tool access and a fixed output schema. (2) Back every model verdict with deterministic rules so that a manipulated model score cannot release a message on its own. (3) Audit the model's behaviour on a corpus of injection attempts as part of every model or prompt change, with a release gate on the detection rate. (4) Log model inputs and outputs for sampled traffic so that a manipulation campaign can be reconstructed afterwards.
CS-Q	Gated Content The payload sits behind a CAPTCHA, login, password or QR code that the scanner cannot pass. STRIDE T (Loose) · CAPEC None · CWE Partial: CWE-636	Content the scanner cannot reach gets its own verdict and gating counts against the message. (1) Return UNREACHABLE for gated content and apply a hold-or-flag policy to it rather than "clean". (2) Try passwords found in the message body or subject against protected archives, and score CAPTCHA and login gates as risk signals.

ID	THREAT	MITIGATION
CS-J	Reputation Laundering A URL routes through trusted domains, open redirects or the platform's own rewritten links, so only the first hop is judged. <hr/> STRIDE S (Loose) · CAPEC None · CWE Partial: CWE-601	A URL is judged by where it ends up, not where it starts. <ol style="list-style-type: none"> (1) Follow the complete redirect chain, including the platform's own rewrites, and judge the final destination. (2) Bind rewritten links to the recipient and message so a link cannot be lifted and reused elsewhere. (3) Re-evaluate the destination at the moment of click, and block or warn when it differs from what was judged at delivery (see Check Once, Use Later).
CS-10	Classifier Evasion Adversarial perturbation (padding, homoglyphs, text in images) moves content across an ML detector's decision boundary. <hr/> STRIDE T (Loose) · CAPEC None · CWE Direct: CWE-1039, CWE-654	No decision rests on a single statistical score. <ol style="list-style-type: none"> (1) Normalise input (strip hidden text, decode homoglyphs, OCR images) before classification. (2) Pair each ML classifier with a deterministic control (signature, policy, reputation) that can block regardless of score. (3) Watch the score distribution per tenant and per feature for shifts that indicate adversarial probing, and raise the threshold for sources that are probing. (4) Keep the model's features and thresholds out of anything the sender can observe (see Verdict Oracle).
CS-9	Classifier Poisoning Feedback loops such as user reports and quarantine releases let an attacker shape what the model learns. <hr/> STRIDE T (Clean) · CAPEC None · CWE None	Training signal is weighted by who provides it and watched for drift. <ol style="list-style-type: none"> (1) Weight feedback by account age, tenant reputation and corroboration, and exclude trial and new accounts from training. (2) Monitor label distributions per tenant and per source, and hold back model updates when a shift exceeds a threshold. (3) Review the training set for a sample of each update against ground truth, and keep a rollback to the last trusted model.
CS-8	Scanner as Attack Surface Parsing, detonating or fetching untrusted content leads to code execution, sandbox escape or server-side request forgery inside the platform. <hr/> STRIDE E (Clean) · CAPEC Direct: CAPEC-664, CAPEC-100, CAPEC-237 · CWE Partial: CWE-653, CWE-918	A compromised scanner can reach nothing but the sample in front of it. <ol style="list-style-type: none"> (1) Run detonation and URL fetching in ephemeral, network-isolated environments with no route to internal services and no credentials. (2) Destroy the environment after each sample and treat any outbound connection attempt as a finding. (3) Hold the scanner's own credentials (feed subscriptions, API keys) in a broker outside the detonation environment, so that a compromised sample cannot read them.

ID	THREAT	MITIGATION
CS-7	Scanner Side Effects Fetching URLs consumes one-time links, triggers actions on the recipient's behalf, or confirms the address to the sender. <hr/> STRIDE I (Loose) · CAPEC None · CWE Partial: CWE-441	The scanner observes without acting on the recipient's behalf. (1) Fetch with HEAD or a safe GET that follows no one-time or state-changing links, and skip links matching unsubscribe, confirm or approve patterns. (2) Fetch from egress that does not identify the product or tenant, and delay fetches randomly so timing does not confirm delivery.
CS-6	Verdict Oracle An attacker can test content against the scanner and iterate until it passes, or read its verdicts, scores and rule names in the headers delivered with the message. <hr/> STRIDE I (Clean) · CAPEC Partial: CAPEC-54 · CWE Direct: CWE-201, CWE-203	An attacker cannot learn what the scanner decided or why, whether by probing it or by reading what it wrote. (1) Strip verdict, score, rule-name and diagnostic headers before delivery and keep them in the platform's own logs, so they never travel with delivered, forwarded or replied mail. (2) Detect repeated near-identical submissions from one source, including trial and free-tier accounts, and degrade the signal they receive.
CS-5	Novelty Window Detection relies on known-bad indicators, so new domains and new payloads pass until the lists catch up. <hr/> STRIDE T (Loose) · CAPEC None · CWE Direct: CWE-184	What is new is treated as unknown, and unknown has a policy. (1) Apply extra scrutiny to domains registered within a configurable window and to never-seen file types or senders. (2) Re-judge delivered mail when intelligence arrives (see Remediation Race) so the novelty window closes retroactively.
CS-4	Modality Gap The payload is in a form the scanner does not analyse: image text, audio, QR codes, links inside documents. <hr/> STRIDE T (Loose) · CAPEC Partial: CAPEC-636 · CWE Direct: CWE-437	Every modality a user can act on is a modality the scanner inspects. (1) Extract and analyse links and text from images, QR codes, PDFs, documents and calendar items. (2) Add scanning coverage to the definition of done for every new client feature that displays content.
CS-3	Scanned Data Exposure Mail sent to third-party engines, cloud sandboxes or model APIs leaks, or cached verdicts and samples cross tenants. <hr/> STRIDE I (Clean) · CAPEC Partial: CAPEC-204 · CWE Direct: CWE-524, CWE-201	Content leaves the platform only under contract, and verdicts never cross tenants. (1) Restrict third-party engines to hash lookups by default and require tenant opt-in for sample submission, with retention terms in the contract. (2) Namespace verdict caches and samples per tenant so a cache hit reveals nothing about another tenant's mail.

ID	THREAT	MITIGATION
CS-2	<p>Exemption Abuse</p> <p>Allow lists, trusted-sender rules and skip conditions exempt content from scanning altogether.</p> <hr/> <p>STRIDE E (Clean) · CAPEC Partial: CAPEC-554 · CWE Direct: CWE-183, CWE-807</p>	<p>Exemptions are scoped, verified, time-limited and reviewed.</p> <ul style="list-style-type: none">(1) Bind exemptions to a verified property (DKIM-aligned domain, authenticated connector), never to a header or address the sender controls.(2) Expire exemptions by default and show tenant admins a periodic review of active exemptions.



The interface decides which facts about a message a person sees before they act on it. These entries cover what the client and the platform present, and the decisions the design leaves to the user.

ID	THREAT	MITIGATION
HF-A	Display Name Deception The interface shows the display name prominently and hides or truncates the address. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-148, CAPEC-98 · CWE Direct: CWE-451	The address is as visible as the name, in every view. (1) Show the full sender address next to the display name in message lists, readers and notifications without extra taps. (2) Mark first-time senders and display names that look like addresses or match a known contact's name. (3) Keep the display name and address visually distinct (type, weight) so that an address-like display name cannot masquerade as the address.
HF-K	Lookalike Rendering Homoglyph, internationalised and long-subdomain addresses are displayed without distinction from the genuine one. <hr/> STRIDE S (Clean) · CAPEC Direct: CAPEC-632, CAPEC-630 · CWE Direct: CWE-1007	Confusable domains are displayed so that they do not look like the genuine one. (1) Render punycode and mixed-script domains in a distinct visual form and emphasise the registrable domain. (2) Compare the sender domain to the user's contacts and the tenant's domains, and flag close matches. (3) Apply the same rendering in notifications, previews and the compose window, not only in the reader.
HF-Q	Thread Hijack An attacker's message is grouped into a trusted conversation and inherits its credibility. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-98 · CWE Partial: CWE-451, CWE-1023	A thread groups only messages that provably belong together. (1) Thread on Message-ID, In-Reply-To and References, never on subject alone. (2) Show a visible break and a warning when a new sender or domain joins an existing thread.
HF-J	Indicator Spoofing Banners, verified marks and "scanned" labels are imitated in the message body or suppressed by styling. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-222, CAPEC-173 · CWE Direct: CWE-451, CWE-1021	Security indicators live where message content cannot draw. (1) Render banners, verified marks and warnings in client chrome outside the message body area. (2) Sanitise message styling so it cannot overlay, hide or imitate chrome elements, and never insert indicators into the body.

ID	THREAT	MITIGATION
HF-10	Reply-Path Diversion Replies go to an address different from the visible sender, and the interface does not surface it. <hr/> STRIDE S, I (Clean) · CAPEC Partial: CAPEC-148 · CWE Direct: CWE-451	The user sees where a reply will go before sending it. (1) Show the Reply-To address in the compose view when it differs from From, with a warning if the domain differs. (2) Treat a cross-domain Reply-To as a risk signal in scoring and in the reader's sender display.
HF-9	Link Presentation Mismatch The displayed link differs from its target, or rewriting hides the real destination from the user. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-173, CAPEC-148 · CWE Direct: CWE-451	The user can see a link's true destination before following it. (1) Display the final destination domain on hover and long-press, including for rewritten links. (2) Flag link text that looks like a URL but points elsewhere.
HF-8	Warning Fatigue Warnings appear so often, or so indiscriminately, that users stop reading them. <hr/> STRIDE S (Loose) · CAPEC Partial: CAPEC-416 · CWE Partial: CWE-357	Warnings are specific, rare and measured. (1) Replace the generic external banner with targeted warnings that say what is unusual and what to do. (2) Measure click-through after each warning type and retire the ones that do not change behaviour.
HF-7	Trusted Internal Sender Mail from a compromised internal account carries no warning and receives more trust than external mail. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-163 · CWE Partial: CWE-424	Internal mail earns no trust it has not been checked for. (1) Apply the same content scanning to internal and intra-platform mail as to external mail. (2) Surface behavioural anomalies for internal senders (new device, unusual volume, first-time recipients) in the recipient's view.
HF-6	Platform Feature Mimicry Sharing invitations, calendar invites, quarantine digests and similar features deliver lures from genuine platform addresses. <hr/> STRIDE S (Clean) · CAPEC Partial: CAPEC-148 · CWE Partial: CWE-451, CWE-424	Platform notifications carry no user-chosen content that could be a lure. (1) Scan sharing invitations, calendar invites and digests like any other mail, including user-supplied fields. (2) Render user-supplied text in notifications visibly separated from the platform's own text.
HF-5	Auto-Added Content Invites, contacts and autocomplete entries are created from unsolicited mail without the user's action. <hr/> STRIDE T (Loose) · CAPEC None · CWE Partial: CWE-356	Nothing is added to the user's calendar, contacts or autocomplete without their action. (1) Hold calendar invites from unknown senders as pending rather than adding tentative events. (2) Populate autocomplete only from addresses the user has sent to, not from inbound mail.

ID	THREAT	MITIGATION
HF-4	Assistant-Mediated Deception AI summaries and suggested replies relay attacker content in the platform's own voice. <hr/> STRIDE S, T (Loose) · CAPEC None · CWE Partial: CWE-451, CWE-1427	An assistant presents message content as the message's claim, never as the platform's. (1) Attribute every summarised statement to the message and exclude links and instructions from summaries. (2) Isolate message content from the assistant's instructions (see Scanner Prompt Injection) and give the assistant no actions beyond summarising. (3) Show the user the exact passage the assistant drew on for each claim, so that hidden or off-screen text is exposed when it is summarised.
HF-3	Signal Loss in Compact Views Mobile and condensed views drop the indicators the desktop design relies on. <hr/> STRIDE S (Loose) · CAPEC None · CWE Direct: CWE-451	Every surface a user can act from shows the signals the decision needs. (1) Define a minimum indicator set (sender address, external marker, warning) required on every surface, including notifications and quick replies. (2) Disable actions such as quick reply from surfaces that cannot show the minimum set.
HF-2	Misdirected Send Autocomplete, reply-all and group expansion lead the user to send to unintended recipients. <hr/> STRIDE I (Loose) · CAPEC None · CWE Partial: CWE-356, CWE-451	The user sees who will receive a message before it leaves. (1) Warn on external, first-time and recently added recipients before sending. (2) Expand group recipients to a visible count and membership, and offer a short undo window after send.



Operations and storage (OP)

The operational plane holds more copies of every message than the mailbox store does, each under a weaker access model. These entries cover archive, backup, search and logs, support and export tooling, configuration, credentials and offboarding.

ID	THREAT	MITIGATION
OP-A	Support Access Platform staff can open, search or export any tenant's mailbox for troubleshooting, with no ticket, no tenant consent, no time limit and no record the tenant can see. STRIDE E, I (Clean) · CAPEC Partial: CAPEC-122 · CWE Partial: CWE-1220, CWE-778	Support access to tenant data is consented, scoped, time-limited and visible to the tenant. (1) Require a ticket and the tenant's approval (or a documented emergency path with after-the-fact notice) before a support engineer can open a mailbox, and expire the access automatically. (2) Log every support access to an append-only store outside the admin console, and show tenants an access report they can audit. (3) Give support tooling the minimum view needed (headers, routing, logs) and make reading message bodies a separate, rarer privilege.
OP-K	Bulk Export Compliance search, eDiscovery and mailbox export move whole mailboxes or tenants out of the platform in one action, under weaker controls than the mailbox itself. STRIDE I (Clean) · CAPEC Partial: CAPEC-122 · CWE Partial: CWE-424, CWE-799	Bulk export is a privileged, approved, rate-limited and visible operation. (1) Require a second approver or a step-up factor for any export of a whole mailbox or tenant, and notify the mailbox owner and tenant admin when it happens. (2) Deliver exports only to an authenticated, short-lived location, scanned and watermarked, and log who downloaded them. (3) Cap export volume per actor and per day, and alert on exports that do not match the actor's history.
OP-Q	Archive as Second Mailbox A journal or archive holds a copy of every message, indefinitely, under its own access model, outside remediation, retention and the mailbox's permissions. STRIDE I (Loose) · CAPEC Partial: CAPEC-150 · CWE Partial: CWE-424, CWE-1250	Every copy of a message is under the same access, remediation and retention model as the mailbox. (1) Enforce mailbox-level permissions on archive search, so that no one can read in the archive what they cannot read in the mailbox. (2) Make remediation, deletion and legal hold propagate to the archive in the same transaction, and reconcile the two stores on a schedule. (3) Put the archive on the platform's threat model and data-flow diagram as a store in its own right.

ID	THREAT	MITIGATION
OP-J	Backup Exposure Backups and snapshots hold mail, keys and credentials under a different key, a different access model and a different lifetime, and a restore reintroduces what remediation removed. <hr/> STRIDE I (Clean) · CAPEC Partial: CAPEC-150 · CWE Partial: CWE-530, CWE-1250	Backups are encrypted, restore is privileged, and a restore re-applies every control the live store enforces. (1) Encrypt backups with keys held outside the backup service, require two people to restore, and log every restore. (2) Run remediation, retention and legal hold against restored data before it becomes visible, and restore into a quarantined store by default. (3) Apply the live store's access model and lifetime to snapshots, and delete them on schedule.
OP-10	Unreviewed Configuration Change Platform-wide security configuration (policies, scanner thresholds, allow lists, connectors, TLS settings) is edited live, with no review, no diff and no record of the intended state. <hr/> STRIDE T, R (Clean) · CAPEC Direct: CAPEC-176 · CWE Partial: CWE-778	Security configuration is declared, reviewed, versioned and reconciled. (1) Keep the intended configuration as versioned code with a required reviewer, and apply it through a pipeline rather than by hand in a console. (2) Reconcile the live configuration against the declared state continuously and alert on drift, including changes made through break-glass paths. (3) Rehearse rollback of every security control's configuration and keep the last known-good state available.
OP-9	Connector Credentials Credentials for connectors, partner APIs, cloud storage and internal services sit in configuration, are shared across tenants or services, and are never rotated or scoped. <hr/> STRIDE S, E (Clean) · CAPEC Partial: CAPEC-555, CAPEC-560 · CWE Partial: CWE-260, CWE-522	Each credential is scoped to one purpose and one tenant, held in a secrets store, and rotated. (1) Store connector and partner credentials in a secrets manager with per-service access, never in configuration files or environment variables shared across services. (2) Issue one credential per tenant and per integration, scoped to the narrowest API permission, and rotate on a schedule and on staff departure. (3) Monitor the use of each credential and revoke on anomalous use.
OP-8	Retention and Deletion Gap Deletion, retention and legal hold are applied to the mailbox and not to its copies (cache, index, archive, backup, quarantine), so mail persists where it should not or vanishes where it must be kept. <hr/> STRIDE I, R (Loose) · CAPEC None · CWE Partial: CWE-1250, CWE-459	Deletion, retention and hold are enforced across every copy, and the platform can prove it. (1) Maintain an inventory of every store that holds message copies, and drive deletion, retention and hold from one service that reaches all of them. (2) Treat a copy that cannot be reached by hold or deletion as a defect, and reconcile stores against the inventory on a schedule. (3) Produce a deletion certificate per request that lists each store and the time the copy was removed.

ID	THREAT	MITIGATION
OP-7	Content in Logs Message content, addresses, subjects, URLs, tokens and headers end up in logs, traces, crash dumps, metrics labels and support tickets, often shipped to a third party. <hr/> STRIDE I (Clean) · CAPEC Partial: CAPEC-37 · CWE Direct: CWE-532, CWE-528	Logs carry identifiers, never content, and leave the platform only under contract. (1) Define an allow list of loggable fields (message ID, tenant, sizes, verdicts, timings) and strip or hash everything else at the logging library, not in each service. (2) Keep logs that must carry content (forensics) in a separate store with its own access control and retention, inside the platform. (3) Test with messages whose content is a canary string and alert when it appears in any log, trace or ticket.
OP-6	Search Index Leakage Search and indexing services hold message content with their own access model, so a query can return what the mailbox permissions would refuse, or another tenant's mail. <hr/> STRIDE I, E (Clean) · CAPEC Partial: CAPEC-1, CAPEC-180 · CWE Direct: CWE-1230	The index enforces the same tenancy and permissions as the mailbox store, at query time. (1) Partition the index per tenant with the tenant identity enforced in the index service from the authenticated session, not from a caller-supplied field. (2) Apply mailbox permissions at query time by joining against the authorisation source, rather than by rebuilding the index on a schedule. (3) Treat suggestions, autocomplete and result counts as content and subject them to the same checks.
OP-5	Audit Gap Security-relevant actions (quarantine release, rule and allow-list changes, support access, exports, key operations) are unlogged, logged mutably, or logged without the person who acted. <hr/> STRIDE R (Clean) · CAPEC Partial: CAPEC-268, CAPEC-571 · CWE Direct: CWE-778, CWE-223	Every security-relevant action is logged, immutably, and attributed to a person. (1) Enumerate security-relevant actions from the threat model and fail the release of any feature that performs one without logging it. (2) Write audit records to an append-only store that platform operators cannot alter, with retention set by policy. (3) Require individual authentication for privileged actions, so no audit record points at a shared role or a service account.
OP-4	Offboarding Residue When a tenant, user or integration leaves, its data, domains, keys, connectors, tokens and archive copies linger, and whoever acquires its name inherits them. <hr/> STRIDE E, S (Loose) · CAPEC None · CWE Partial: CWE-226, CWE-672, CWE-459	Offboarding is a defined procedure that removes or neutralises everything the departed party was given. (1) Keep an inventory of what each tenant, user and integration owns (data, domains, keys, connectors, tokens, grants) and drive offboarding from it, with a verifiable end state. (2) Hold departed tenants' domains and names in a cooling-off state that no new tenant can claim, and revoke every token, session and delegation at user departure. (3) Delete or quarantine residual data on a schedule and report what remains.

ID	THREAT	MITIGATION
OP-3	Alert Flood Monitoring raises one alert per event, so attacker-generated volume buries the alert that matters, and the on-call learns to ignore the channel. <hr/> STRIDE R, D (Loose) · CAPEC Partial: CAPEC-125 · CWE Partial: CWE-779	Alerts are rate-limited, grouped by cause, and the ones about people and privilege have their own channel. (1) Aggregate message-level alerts by campaign and source, and cap the rate at which any one cause can raise alerts. (2) Route alerts about privileged actions (support access, exports, configuration changes, key operations) to a separate, low-volume channel with a named owner. (3) Measure alert volume and response, and remove any alert that has not led to action in a defined period.
OP-2	Production Data Elsewhere Copies of production mail are used in staging, test, analytics and model training, under weaker credentials, broader access and no retention. <hr/> STRIDE I (Loose) · CAPEC None · CWE Partial: CWE-212	Real mail exists only in production, and anything derived from it is minimised and controlled. (1) Generate synthetic mail for staging and test, and forbid restores of production data into any other environment. (2) Where analytics or model training needs real content, minimise it at source, process it inside production's controls, and delete it on schedule. (3) Treat every non-production environment that holds tenant data as production for access control and monitoring.



THE WHOLE STACK · STRUCTURAL HAZARDS

Structural hazards (T)

PAR AVION
BY AIR MAIL

These eight hazards are properties of email itself, so no single component can fix them. Apply them to the whole design after the layers.

ID	THREAT	MITIGATION
T8	Envelope and Header Duality The identity used for routing and the identity shown to the user are independent, and every control must choose which one it checks. ----- STRIDE S (Loose) · CAPEC Partial: CAPEC-43 · CWE Direct: CWE-348	One sender identity is resolved at ingress, and it is the identity every control checks and every user sees. (1) Resolve a single canonical sender identity at the edge, reject messages where envelope and header identities are ambiguous, and carry the resolved identity in metadata. (2) Display only the resolved identity in clients, and make every control document which identity it evaluates.
T7	Hop-by-Hop Trust There is no end-to-end guarantee; each hop trusts the last, so the path is as strong as its weakest hop. ----- STRIDE S, T (Loose) · CAPEC Partial: CAPEC-21 · CWE Partial: CWE-807	The platform verifies for itself what it needs to trust, independent of what earlier hops claim. (1) Strip inbound trust assertions at every ingress and re-derive them from what the platform can verify. (2) Identify the hop whose compromise would be believed by all the others, and remove that single point of trust.
T6	Legitimate Mutation Forwarders, lists, gateways and the platform itself rewrite messages in transit for legitimate reasons, so no integrity control can tell an authorised change from an attack. ----- STRIDE T (Loose) · CAPEC None · CWE None	The platform verifies what arrives, not what was sent, and knows which of its own components change messages. (1) Inventory every component that rewrites messages and the authentication results each one breaks, and have each sign what it changed (ARC seal or DKIM) so the change is attributable. (2) Design integrity checks on what the platform itself observed at ingress rather than assuming the original sender's signature survives to the mailbox.
T5	Interpretation Differential Any two components reading the same bytes may disagree, and attacks live in the disagreement. ----- STRIDE T (Loose) · CAPEC Direct: CAPEC-43 · CWE Direct: CWE-436	A message is interpreted once, canonically, and ambiguity is rejected rather than guessed. (1) Canonicalise at ingress and pass the canonical form to every scanner and client. (2) Reject ambiguous input at the edge and maintain a differential test corpus across every parser in the path. (3) Treat parser disagreement as a release blocker: any message on which two components in the path differ is rejected until the parsers agree.

ID	THREAT	MITIGATION
T4	Authentication Is Not Trust The protocols prove which domain sent a message, never that the domain is benign. <hr/> STRIDE S (Loose) · CAPEC None · CWE Partial: CWE-654	Identity and trust are separate inputs, and an authentication pass never relaxes another control. (1) Keep authentication results out of scoring, bypass and badge decisions, using them only for DMARC disposition and domain-level reputation. (2) Make reputation and intent explicit controls with their own evidence, separate from authentication.
T3	Legacy Fail-Open Interoperability with every legacy sender means an absent security feature is treated as acceptable. <hr/> STRIDE I, T (Loose) · CAPEC Partial: CAPEC-620 · CWE Partial: CWE-757, CWE-636	Every opportunistic protection has a path and a date to become mandatory. (1) Publish and enforce policies (MTA-STS, DMARC reject, implicit TLS) for the platform's own domains and defaults. (2) Track each opportunistic protection with a tightening schedule, telemetry on what would break, and a per-tenant strict mode.
T2	Shared Infrastructure, Shared Fate Multi-tenant platforms pool identity, reputation and trust across customers who do not trust each other. <hr/> STRIDE E, I (Loose) · CAPEC Partial: CAPEC-124 · CWE Partial: CWE-653	The tenant boundary is enforced in the data layer and identity layer, not only in configuration. (1) Bind tenant identity at ingress and enforce it in every store, cache, queue and key store by construction. (2) Give each tenant its own keys, cache namespace, sending identity and verification tokens. (3) Test the boundary adversarially with a tenant that attempts to read, write, send as and configure another, and keep that test in the release pipeline. (4) Separate tenants' operational copies too (archive, index, backup, logs), not only their live mailboxes.
T1	Check Once, Use Later Store-and-forward separates the moment of inspection from the moment of use, and content or context can change in between. <hr/> STRIDE T (Loose) · CAPEC Direct: CAPEC-29 · CWE Partial: CWE-367	There is a control at the moment of use, not only at the moment of receipt. (1) Evaluate links at click, re-scan on release and re-judge delivered mail when intelligence changes. (2) Re-verify standing conditions (domain ownership, session validity, sender reputation) periodically and on change events. (3) Record for every decision the conditions it depended on, so that a change in any of them can trigger re-evaluation of the decisions that relied on it.

Sources

The issues behind these entries were already publicly disclosed in real systems; the contribution here is the translation into threats a designer can test against, and the collection. These are the original disclosures the post cites.

- Timo Longin, SEC Consult Vulnerability Lab, [SMTP Smuggling: Spoofing E-Mails Worldwide](#), 18 December 2023.
- Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky and Jörg Schwenk, [Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels](#), 27th USENIX Security Symposium, 2018.
- Jianjun Chen, Vern Paxson and Jian Jiang, [Composition Kills: A Case Study of Email Sender Authentication](#), 29th USENIX Security Symposium, 2020.
- Kaiwen Shen, Chuhan Wang, Minglei Guo, Xiaofeng Zheng, Chaoyi Lu, Baojun Liu, Yuxuan Zhao, Shuang Hao, Haixin Duan, Qingfeng Pan and Min Yang, [Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks](#), 30th USENIX Security Symposium, 2021.

© 2026 Jonathan Brett Crawley. CC BY-NC-ND 4.0, with additional permissions.

Licensed under Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0): you may share the whole taxonomy, unchanged and with credit, for non-commercial purposes. In addition, whether or not the use is commercial, you may use it to threat model systems, including for paying clients; use it internally and for training inside any organisation; and quote individual entries, with credit, in paid courses, reports and talks. Shipping it in a product, such as a tool's built-in library, a printed deck or a reprint for sale, needs written permission.

From The Unmodeled Attack Surface, ostering.com · Version 1.0, October 2026