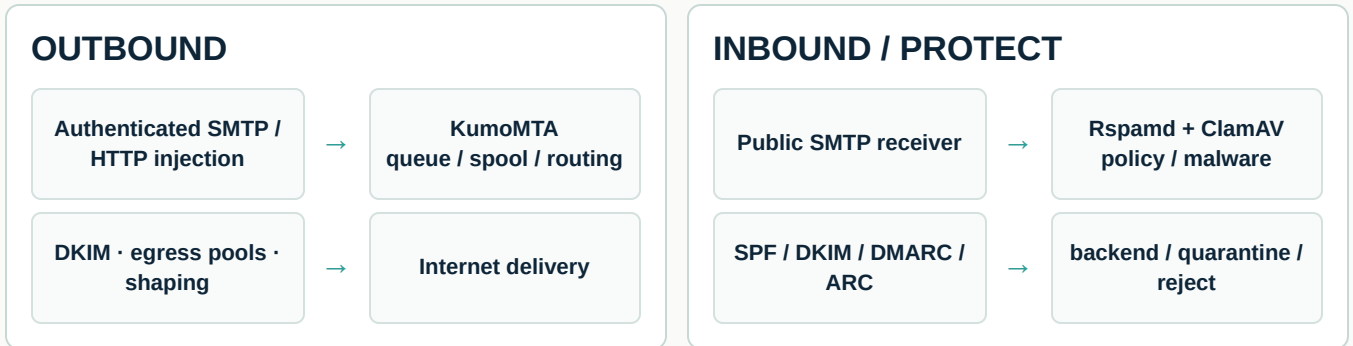
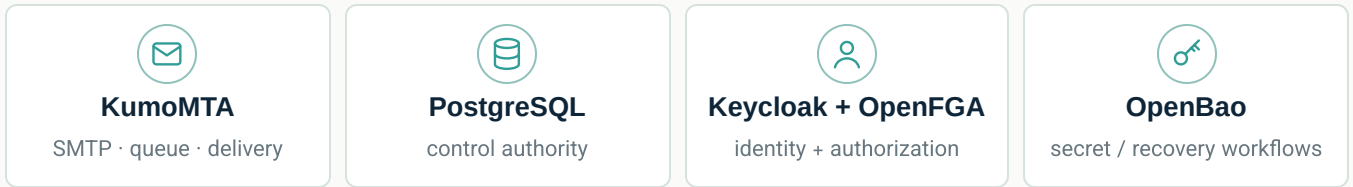


4SO Mail Gateway

Self-contained Mail Server & Gateway Platform

منصة Linux/VM-first للإرسال بكميات كبيرة، والاستقبال المحمي،
و Queue/Spool، و DKIM، و routing، والهوية، والعمليات المستدامة؛ مع فصل
واضح بين Mail Data Plane و Control Plane.



Mail Data Plane = Linux/VM workload

لا تعتمد KumoMTA و SMTP و queue/spool و sending IPs و DKIM hot path و HA على Kubernetes بوصفها runtime dependency.

Bounded Control Plane

تملك Keycloak و PostgreSQL و Rust Control API و OpenFGA و OpenBao مسارات identity و authorization و durable lifecycle.

Node-local spool

ال Spool محلي على Mail Node؛ ولا يُدعى وجود shared spool وهمي كجزء من معمارية المنتج.

PRODUCT BOUNDARY

أربع طبقات؛ دورة حياة واحدة للمنتج

لكلٍّ من SMTP runtime و inbound protection و control/identity و observability مالك واضح؛ ولا تحلّ UI أو MCP محل الجهات المرجعية الأساسية.

POLICY

Inbound Protection

Rspamd
mail security and policy processing



ClamAV
malware scanning



Authentication signals
SPF · DKIM · IPREV · DMARC · ARC



LINUX / VM

Mail Data Plane

KumoMTA
submission · public SMTP · delivery · queue/spool



HAProxy
stable internal transport / selected HA endpoints



Unbound + Valkey
resolver path + shared runtime authority where required



EVIDENCE

Observability & Operations

Prometheus
metrics and runtime evidence



Grafana
operational visibility



Product workflows
mail · queue · TLS · routing · deliverability state



AUTHORITY

Control & Identity

Rust Control API + PostgreSQL
durable product authority



Keycloak + OpenFGA
identity + product authorization



OpenBao
secret material / recovery workflows



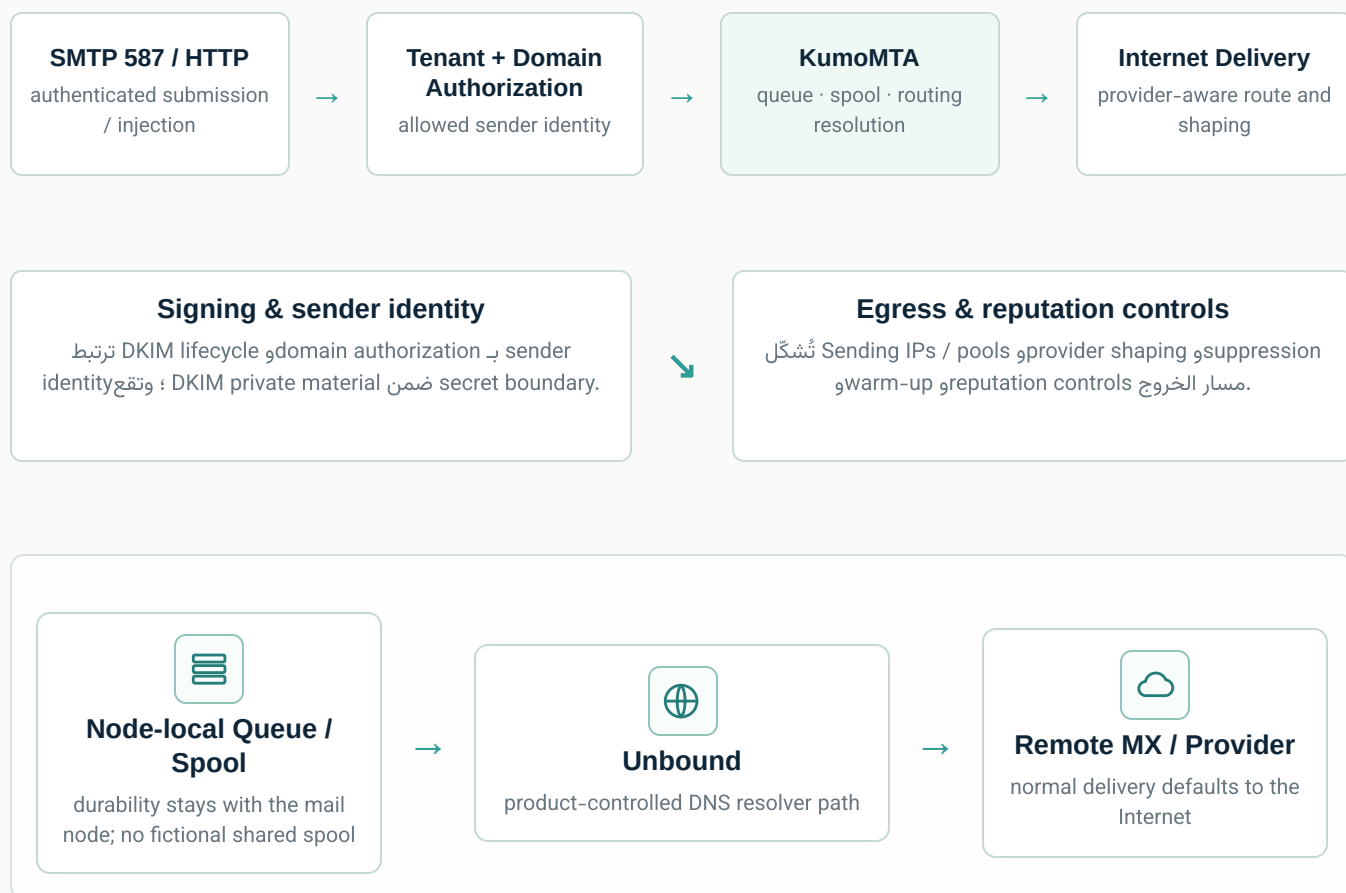
مبدأ الملكية: تحتفظ PostgreSQL بمرجعية Control Plane؛ وتملك KumoMTA ال mail hot path وال node-local queue/spool.



OUTBOUND PATH

من الإرسال إلى التسليم عبر الإنترنت

يتمركز Outbound path على KumoMTA؛ إذ تُطبَّق domain authorization و DKIM و egress pool و shaping قبل delivery، بينما يبقى الـ spool على Mail Node نفسها.



Stable transport ≠ shared spool

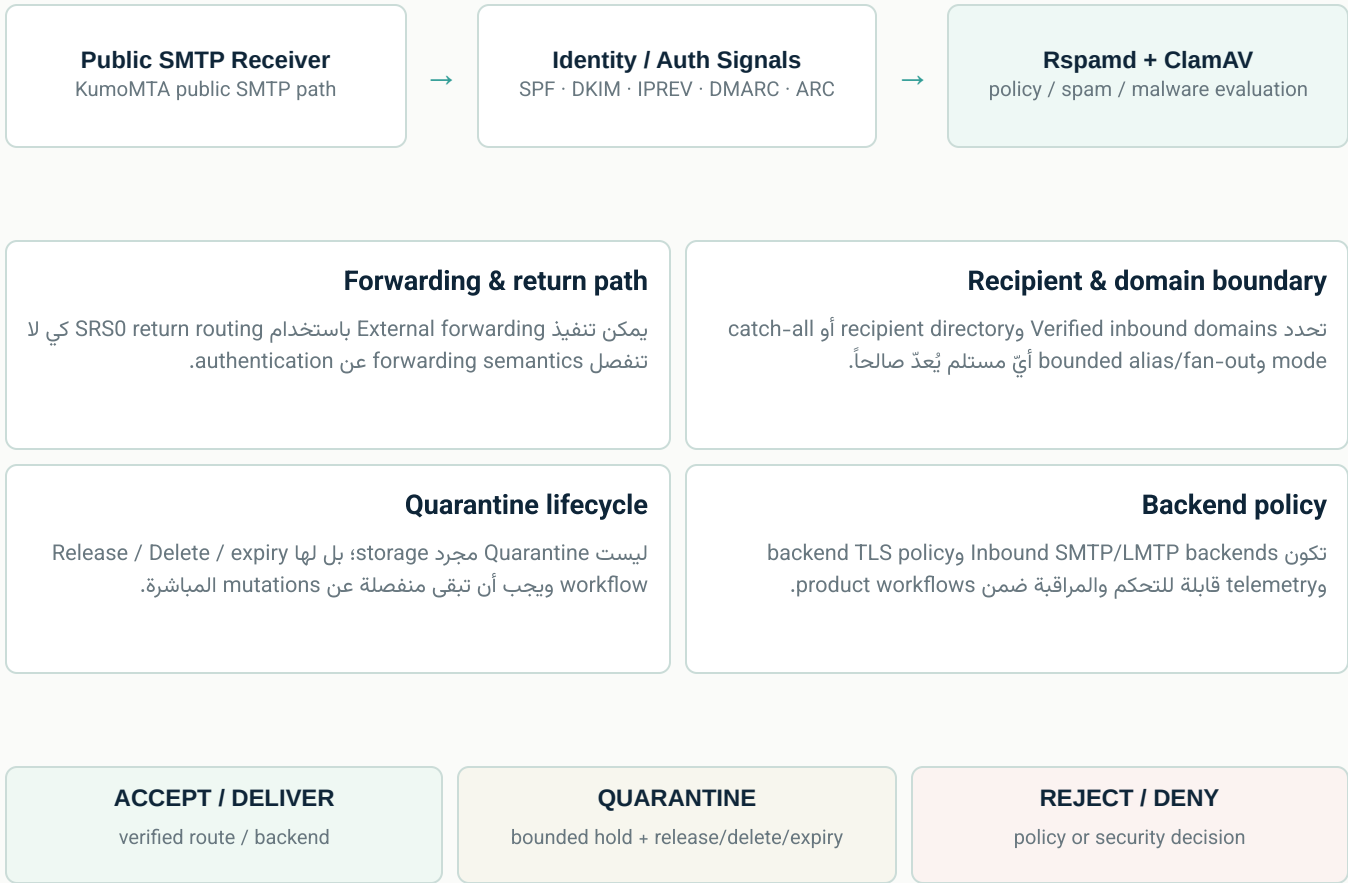
نُستخدم HAProxy لـ selected stable transport / HA endpoints، لكن الـ spool يبقى node-local ولا يُفترض أنه storage fabric مشترك.



INBOUND PROTECTION

الاستقبال والسياسة والبرمجيات الخبيثة وقرار التسليم

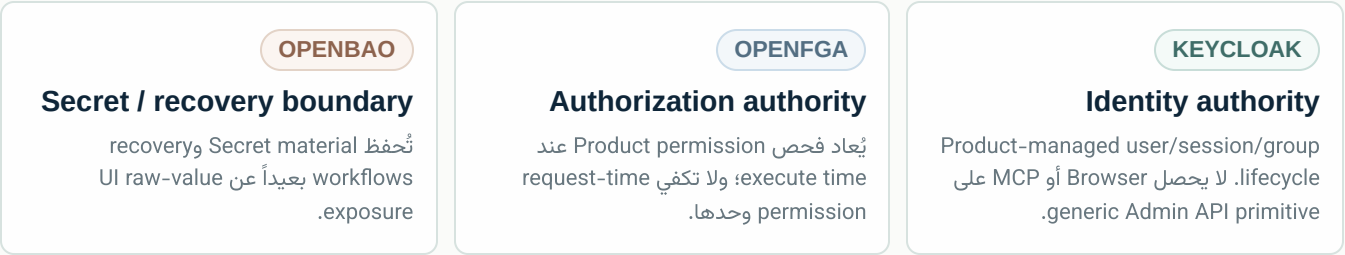
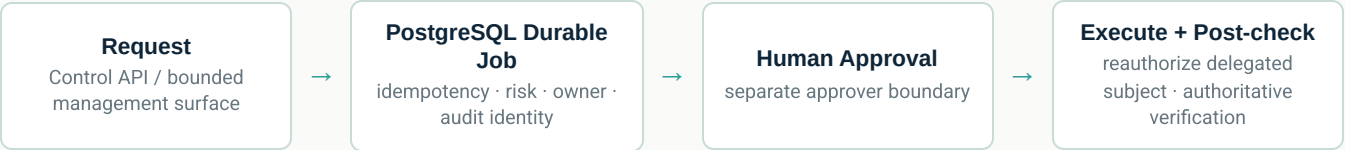
إلى جانب SMTP reception، يُبقي Inbound path كلاً من backend و anti-malware و anti-spam و authentication signals و quarantine lifecycle و policy ضمن مسار واحد قابل للمراقبة.



HIGH-RISK IAM

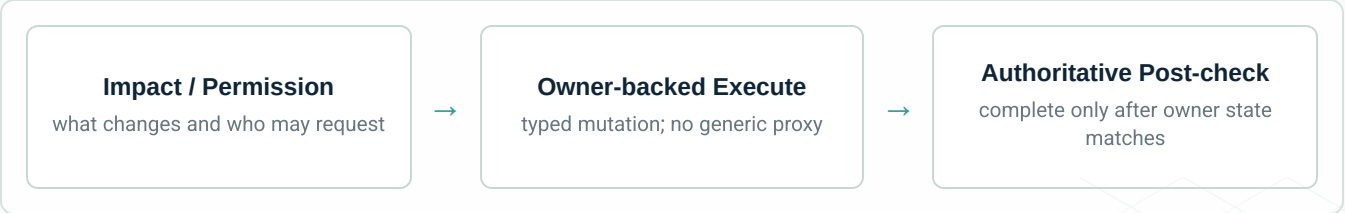
لا اختصار لأي تغيير حساس خارج سلسلة الموافقة

ترتبط Identity و access mutations الحساسة بـ durable
PostgreSQL job وموافقة بشرية مستقلة و reauthorization عند التنفيذ و authoritative post-check.



لا تملك MCP صلاحية self-approval

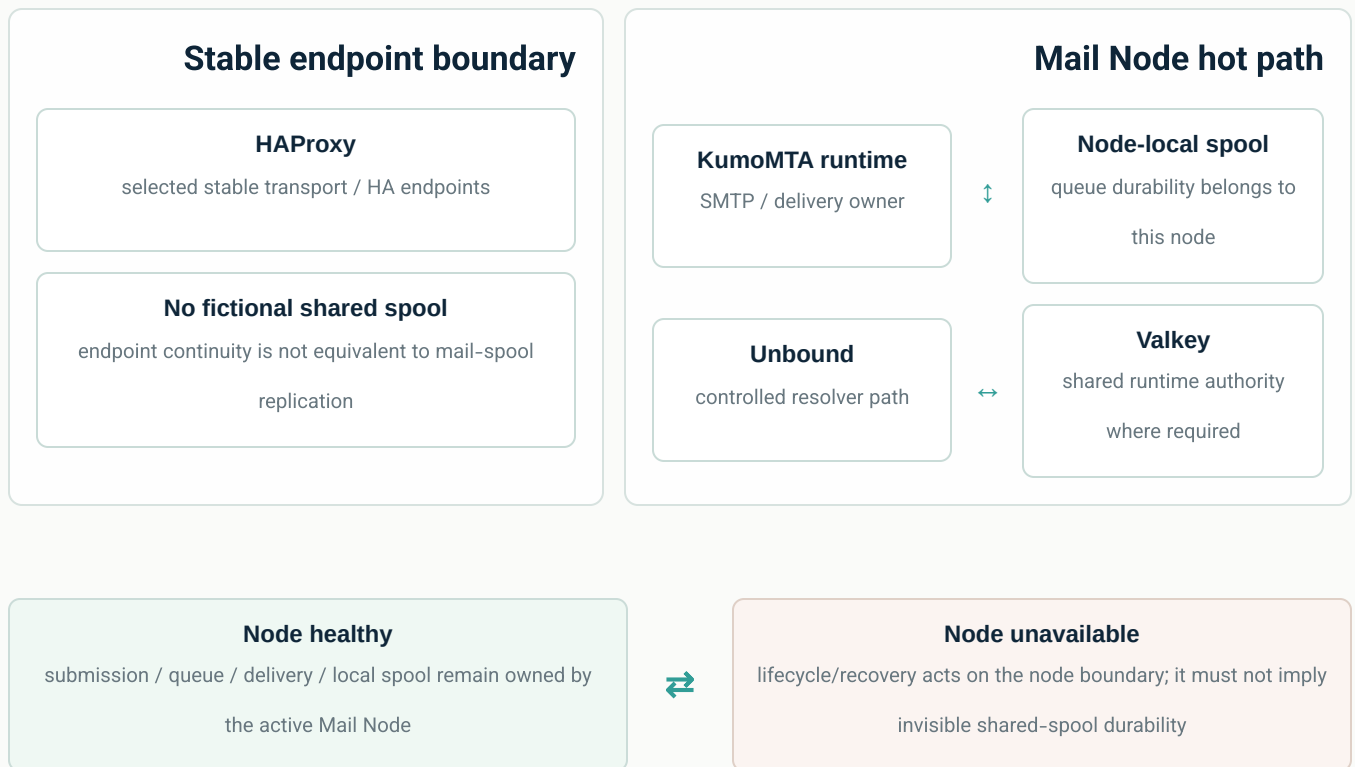
يمكن لـ MCP تنفيذ bounded request أو read ضمن صلاحيته الخاصة، لكن لا يوجد generic approve/execute IAM mutation bypass.



QUEUE, SPOOL & FAILURE BOUNDARY

ال Spool محلي؛ ويجب أن تحافظ الاستمرارية على هذا الحد

لا يمكن إخفاء Mail Node failure بافتراض وجود shared storage. تُبقي المعمارية product-owned ال spool بنمط node-local وتفصل HA endpoint عن data durability.



Kubernetes is not Mail Data Plane runtime authority

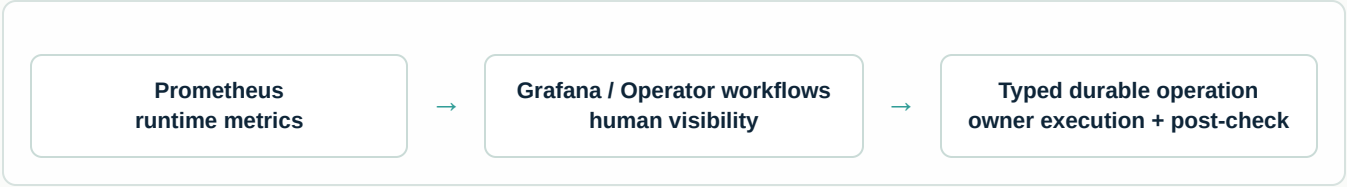
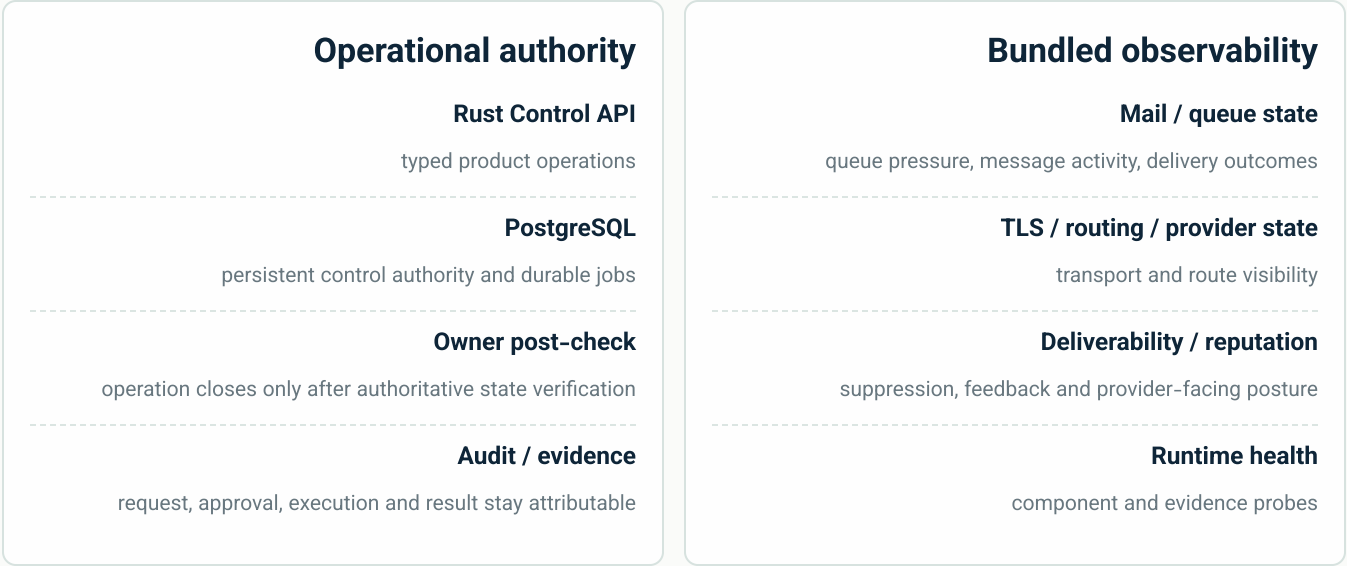
قد تُستخدم Kubernetes في أجزاء أخرى من delivery infrastructure، لكن sending IP / spool / SMTP / KumomTA. HA و DKIM hot path تبقى Linux/VM-first.



OBSERVABILITY & CONTROL LOOP

يجب أن تتحول حالة Mail إلى عمليات قابلة للتنفيذ

توفر Prometheus وGrafana الـ visibility؛ بينما تُغلق owner APIs وdurable operations دورة mutation وrecovery. ولا تحلّ Monitoring authority محل runtime authority.



ACTION & OPERATIONS CATALOG

دورة حياة Mail من مسار الرسالة إلى مسار الهوية

Receiver / Protect

IN

public SMTP verified domains SPF/DKIM/DMARC
Rspamd ClamAV backend TLS quarantine

ترتبط Policy و malware decisions بـ recipient/backend/quarantine workflow

Sender / Outbound

OUT

SMTP submission HTTP injection domain auth
DKIM egress pools routing shaping
suppression

تبقى KumoMTA مالكة مسار queue/spool و Internet delivery

Runtime & Operations

OPS

queue/history Unbound Valkey HAProxy
Prometheus Grafana recovery

لكلّ من Visibility و durable operation و runtime owner حدّ (boundary) مستقل.

Identity & Sensitive Mutations

IAM

Keycloak OpenFGA OpenBao durable job
human approval reauthorize post-check

لا يُعرّف أي generic self-approve / execute bypass لـ management agent

المعمارية في جملة واحدة

4SO Mail Gateway هي Mail Data Plane مستقلة على Linux/VM و Control Plane خاصة بالمنتج لـ lifecycle و identity و authorization و recovery؛ وليست wrapper لـ Kubernetes-native mail runtime و hosting panel

Rspamd + ClamAV inbound protection 02

KumoMTA owns SMTP + queue/spool 01

PostgreSQL durable control authority 04

Unbound + Valkey runtime services 03

Prometheus + Grafana observability 06

Keycloak + OpenFGA + OpenBao 05

Own the mail path. Bound every sensitive mutation. Observe the runtime without confusing visibility with authority.

تترابط Outbound و Inbound و Identity و Operations ضمن واحد self-contained product boundary