Technical Overview & Security Posture

PRATA is a single-tenant, on-premises marketing platform. This document specifies the deployment model, operating environment, network architecture, access control, privilege separation, data custody, and maintenance posture for technical assessment.

Tenancy	Inbound ports	Data residency	Transport	Operator privilege
Single	**0**	**On-premises**	**TLS e2e**	**App only**

1. Deployment model

PRATA runs on dedicated hardware located at the client's place of business, on the client's own network. There is no multi-tenant cloud component, no shared database, and no pooled compute. Each installation is a discrete single-tenant system serving one business.

The client owns the hardware outright. The platform is licensed for perpetual use on that hardware. There is no activation server and no entitlement check that can revoke operation. A lapsed licence changes what the installation receives, never whether it runs.

PARAMETER	SPECIFICATION
Tenancy model	Single-tenant. One installation serves one business. No data, compute, or credential store is shared between installations.
Hosting	On-premises, client-owned hardware, client-controlled network.
Licensing	Initial term paid in advance covering the first twelve months. Renewal thereafter is $1 per year and carries platform upgrades, integration maintenance, and third-party API revisions.
Lapsed licence	The installation continues to operate at the last version the client paid through, debranded, in perpetuity. Available once the initial twelve-month term is complete.
Vendor dependency	None for operation. The platform does not contact TanFlag for authorization and continues to function without vendor availability.
Cloud components	None for application logic or data storage. A managed edge network provides encrypted transport and authentication only; it does not store business data.

2. Operating environment

LAYER	SPECIFICATION
Processor architecture	ARM64 / aarch64. Quad-core 64-bit Arm Cortex-A76 @ 2.4 GHz (Broadcom BCM2712). Cryptography extensions present.
Memory	8 GB LPDDR4X, 32-bit interface, ~17 GB/s bandwidth.
Operating system	Debian-based Linux, 64-bit, headless. No desktop environment installed.
Storage	512 GB NVMe SSD over PCIe 2.0. Selected over removable flash for write endurance under sustained database load.
Service isolation	All application services run in discrete containers under a supervised container runtime. Services do not share a filesystem namespace.
Restart policy	All services carry automatic restart policies and recover unattended following power loss, reboot, or host restart.
Data layer	PostgreSQL, local to the appliance, not exposed beyond the container network.

LAYER	SPECIFICATION
Time	Hardware real-time clock with battery retention, synchronized via NTP. Required for scheduled operations and log integrity.
Administration	Command line over SSH. No graphical administration console is exposed to any network.
Peripherals	None. The appliance runs headless with no monitor, keyboard, or input device attached in production.

3. Network architecture

Remote access is provided by an outbound-only encrypted tunnel from the appliance to a global edge network. The appliance initiates and maintains the connection; the edge does not initiate connections to the appliance. No inbound ports are opened, no port forwarding is configured, and no public IP address is required.

PROPERTY	SPECIFICATION
Attack surface	The appliance presents no listening service to the public internet. It cannot be discovered by external IP or port scanning.
Transport	Four concurrent connections to geographically distributed edge nodes. Primary transport QUIC over UDP 7844; automatic fallback to HTTP/2 over TCP 7844.
Encryption in transit	TLS between appliance and edge. TLS between edge and end user. Certificates issued and renewed at the edge; no certificate material is managed on client equipment.
NAT traversal	Functions behind CGNAT and on networks where inbound port forwarding is unavailable or administratively prohibited.
Client-side infrastructure	No reverse proxy, dynamic DNS, VPN concentrator, or certificate automation is deployed on client equipment.
Local addressing	Static DHCP reservation bound to the appliance MAC address, so network identity persists across router restart and lease expiry.
Failure mode	If the tunnel cannot establish, the platform becomes unreachable remotely. Local processing, scheduled workflows, and data retention continue unaffected.

Required egress

DESTINATION	PORT	PROTO	PURPOSE
Edge tunnel endpoints	7844	UDP	Primary transport (QUIC)
Edge tunnel endpoints	7844	TCP	Fallback transport (HTTP/2)
Connected platform APIs	443	TCP	HTTPS to configured service providers; optional edge features
DNS resolvers	53	UDP/TCP	Name resolution
NTP	123	UDP	Time synchronization

Firewall configuration

A firewall blocking all ingress and permitting only the egress specified above is a complete configuration for this deployment. Where a firewall enforces SNI or requires IP-based rather than hostname-based rules, TanFlag supplies current edge destination ranges on request; these are published by the edge provider and subject to change. TLS interception on the management tunnel prevents the connection from establishing and requires an exemption.

4. Access control and identity

Access is gated at the network edge, upstream of client hardware. Unauthenticated requests are not forwarded to the appliance.

PARAMETER	SPECIFICATION
Enforcement point	Network edge, upstream of the appliance. Authentication is evaluated before the request is forwarded.
Policy scope	Per named individual. Access is granted to specific identities, not to a shared credential or a network range.
Application layer	The application enforces its own session, role, and permission model behind the edge policy. Two independent layers must be satisfied.
Provisioning	Adding, removing, or restricting a user is a policy change effective immediately. It does not require a change on the appliance or a service restart.
Revocation	Immediate at the edge. A revoked identity cannot reach the appliance regardless of any application-layer session state.
Public paths	Automation callback endpoints required for third-party integrations are explicitly enumerated and scoped. All other paths require authentication.

5. Privilege separation and the operator boundary

Staff who use PRATA have access to the application interface only. They do not have, and cannot obtain, access to the host operating system, the database, the automation and integration layer, or any stored credential, API key, OAuth token, or platform secret.

CONTROL	IMPLEMENTATION
Credential storage	All connected-account credentials are held in an encrypted credential store within the automation layer, which is not reachable from the application interface.
Separate authentication	The automation and data-administration surfaces sit behind independent edge authentication restricted to TanFlag identities.
Operator visibility	The operator sees interfaces and results. The operator cannot view, export, or extract the secrets that authorize those results.
Persistence	The boundary is permanent. It is not a setup-phase restriction that relaxes after handover.
Host access	No client identity holds shell, container, or database access to the appliance at any point in the lifecycle.

5.1 Boundary outcomes

SCENARIO	OUTCOME
Employee departure	No platform credentials are held by staff and none can be exported on departure.
Account compromise	Exposure is limited to the application surface. The credential store, database, and host are unaffected.
Misconfiguration	The automation layer is unreachable from any client identity and cannot be altered client-side.
Credential disclosure	Staff hold no connected-account credentials and cannot disclose them.

6. Data custody

PARAMETER	SPECIFICATION
Storage location	All business data resides in the local PostgreSQL instance on the client-owned appliance, on client premises.
Scope of data	Customer records, review history, message content, campaign data, scheduling data, and analytics.
Egress of business data	Occurs only when a client-configured workflow deliberately transmits it to a client-connected service. Publishing a post transmits that post to the platform it publishes on.
Vendor-side storage	None. TanFlag operates no central store of client business data and holds no replica.
Telemetry	None. No usage reporting, no analytics beacon, no diagnostic upload.
Data monetization	None. Business data is not aggregated, resold, licensed, or used for model training.
Authorization dependency	None. The platform does not contact TanFlag for permission to operate and does not degrade if it cannot reach TanFlag.
Portability	Data resides in a standard relational database on hardware the client owns and remains readable with standard tooling.

7. Maintenance and support model

PRATA is a closed appliance. Client staff and client IT do not administer the platform, apply updates, or modify configuration. TanFlag performs all maintenance, patching, and updates remotely. Restricting write access to a single maintainer keeps configuration consistent across the installed base and makes fault diagnosis deterministic.

AREA	MODEL
Administrative access	TanFlag retains persistent administrative access to the appliance for the life of the support relationship. This is what makes remote patching, configuration change, and fault resolution possible without a site visit. Access is over the outbound management tunnel only and is restricted to TanFlag identities at the network edge.
Patching	Performed by TanFlag remotely over the management tunnel.
Configuration changes	Performed by TanFlag. Client-initiated changes are made by request, not by client access.
Client obligations	Supply power. Supply network. Do not unplug or relocate. Notify TanFlag in advance of network or ISP changes.
Client IT burden	None. Client IT is not required to support, monitor, patch, or troubleshoot the platform.
Fault handling	Reported to TanFlag directly. Local remediation is neither expected nor supported.

7.1 Licence lapse

Renewal is $1 per year from year two forward and carries platform upgrades, integration maintenance, and third-party API revisions. Non-renewal after the initial twelve-month term has the following effects.

ON LAPSE	OUTCOME
Operation	Continues. The installation runs at the last version the client paid through, in perpetuity. Version entitlement is cumulative: a client who renews through v2 and then lapses retains v2, not v1.
Branding	Removed. The installation is no longer represented as PRATA. Clients are free to white-label the system for their own use after the initial term.
Updates	None. No feature releases, no integration maintenance, and no third-party API revisions are applied to a lapsed installation.

ON LAPSE	OUTCOME
Edge protection	Retained. Transport encryption and edge authentication continue on the provider's free tier for as long as that tier exists.
Modification rights	Not granted at any tier. The platform is not opened for client-side editing, whether licensed or lapsed.

Vendor continuity

The platform runs on client-owned hardware and does not require TanFlag's continued existence to operate. In the event TanFlag ceased operations, existing installations would continue running as configured; the exposure is loss of future support and updates. Because connected third-party platforms revise their APIs on independent schedules, an unmaintained installation degrades progressively as those interfaces change rather than failing at a single point.

8. Physical and power resilience

Hardware-level failure modes and their mitigations.

FAILURE MODE	MITIGATION
Unclean shutdown	The appliance and the site network equipment are both carried by an uninterruptible power supply (425VA / 255W), sized well above the connected load. Brief interruptions do not drop the system mid-write, and remote access survives the outage because the router remains powered.
Storage endurance	The platform runs from solid-state NVMe rather than removable flash media. Removable flash under continuous database write load is a known and predictable failure mode; NVMe is not subject to it on this duty cycle.
Thermal	Aluminum-alloy enclosure with heatsink and active cooling, specified to prevent thermal throttling under sustained continuous load.
Power quality	Line-interactive UPS with surge suppression between mains and appliance.
Network identity	Static DHCP reservation, so the appliance address persists across router restart and lease expiry.
Unattended recovery	All services carry automatic restart policies. The system returns to full operation without intervention after power restoration.

9. Security posture summary

CONTROL	IMPLEMENTATION
Inbound network exposure	None. Zero open ports, no port forwarding, no public IP, no DMZ placement.
External discoverability	None. Not resolvable by external IP or port scanning.
Transport encryption	TLS end to end. Certificates issued and renewed at edge; none managed on client equipment.
Authentication	Enforced at network edge before reaching client hardware, plus independent application-layer session and role enforcement.
Identity scope	Per named individual. Immediate revocation at the edge.
Credential storage	Encrypted, isolated from the user-facing application, behind separate authentication.
Operator privilege	Application interface only. No host, container, database, or secret access.
Data residency	Client premises, single-tenant, no replication, no vendor-side copy.
Telemetry and monetization	None.
Administrative access	TanFlag only, persistent for the life of the support relationship, over the outbound management tunnel. Single maintainer across the lifecycle.
Vendor dependency for operation	None. Operates without contact with TanFlag. A lapsed licence freezes the version; it does not disable the system.
Physical resilience	UPS-backed appliance and network equipment; NVMe storage; active cooling; unattended restart.

10. Component disclosure

TanFlag does not publish the specific component inventory of the platform. The architecture, security model, network requirements, egress specification, privilege model, and data-handling practices are documented in full in this document, and TanFlag will answer specific questions about any of them under a mutual non-disclosure agreement.

Requests for component-level detail should be directed to TanFlag with the reviewing organisation and scope of assessment identified.

Technical questions regarding this document: TanFlag: (443) 991-8984