Sentra

UNIFIED EDGE SECURITY PLATFORM

TECHNICAL DATASHEET · FINANCIAL INSTITUTIONS EDITION

Unified security, traffic and observability across the application and DNS layers

DNS Firewall · Web Application Firewall (WAF) · Multi-layer DDoS defense · Load balancing · TLS/PKI management · SIEM-ready observability — from a single control plane, deployable on-prem or air-gapped.

Document type	Technical Datasheet (v1.0)	Classification	Confidential / Commercial
Audience	Security & Infrastructure Architecture	Industry	Banking & Finance
Scope	Architecture · Capabilities · Compliance · PoC	Date	[To be filled]

Prepared by: **[Company Name]** · Contact: [full name] · [email] · [phone]

01 — EXECUTIVE SUMMARY

Why Sentra?

Sentra is a **unified edge security platform** built to protect the internet-facing applications of financial institutions end to end — internet banking, mobile API gateways, corporate portals and payment endpoints. It consolidates the WAF, DDoS, load balancer, DNS and logging/analytics products that are usually procured separately into a single control plane, reducing operational complexity, vendor count and mean time to respond (MTTR).

6-in-1	L3–L7	On-Prem	100%
WAF · DDoS · LB · DNS · TLS · Analytics	Network-to-application coverage	Air-gapped & data sovereignty	Tenant isolation

HIGHLIGHTS FOR FINANCIAL INSTITUTIONS

- **Data sovereignty:** The entire stack runs inside the institution; log and traffic data never leaves the premises.
- **Fail-closed defaults:** Geo/IP allow-lists *deny* on ambiguity — a strict security posture by design.
- **Immutable audit trail:** Every configuration change is recorded and reversible (undo).
- **Controlled release:** Changes are staged first, then promoted to production via an approved *Deploy*.
- **SIEM integration:** Centralized log forwarding via rsyslog/syslog plus ELK-based forensic analysis.

CORE PROBLEMS SOLVED

- Application-layer defense against OWASP Top 10 and automated bot/vulnerability scanning traffic.
- Service continuity under volumetric and application-layer DDoS attacks.
- Centralized enforcement of geographic and IP-based access policies.
- Single-pane certificate lifecycle and TLS hardening management.
- Real-time visibility into security events and incident response.

> This document describes technical capabilities only. Exact performance figures and capacity plans are measured during a **Proof of Concept (PoC)** run against the institution's real traffic profile (see §11).

02 — SOLUTION ARCHITECTURE

Control plane + intelligent data plane

Sentra operates in two tiers: a central **control plane** where configuration is managed, and distributed **edge (node) servers** that handle visitor traffic. Administrators make all changes in the panel/API; changes are applied to the fleet only via **Deploy**, over the DataPlane API and SPOE synchronization.

2.1 Request Lifecycle

Client → TLS termination (HAProxy) → L3/L4 rate & connection limits (stick-tables) → **ac-agent (SPOE)**: geo/IP decision + per-pool DDoS → **WAF (ModSecurity/OWASP CRS)**: inspection, learn/block → Load balancing + health checks → **Origin server**. In parallel: access & WAF events → rsyslog → Logstash → Elasticsearch.

2.2 Component Inventory

COMPONENT	TIER	RESPONSIBILITY	TECHNOLOGY
sentradns-admin	Control	Management panel, REST API, multi-tenant orchestration, deploy pipeline, audit trail	Go 1.25 · PostgreSQL
lb	Data (edge)	Load balancing, TLS termination, health checks, stick-table DDoS	HAProxy 3.3 · DataPlane API v3
waf	Data (edge)	Application-layer inspection, learn/block, data-leakage protection	libmodsecurity 3.0.x · OWASP CRS
ac-agent	Data (edge)	Real-time geo/IP decisions, per-pool DDoS, GeoIP resolution	Go · HAProxy SPOE
sentra-agent	Data (edge)	Node operations/diagnostics API, service management, bootstrap	Go · HTTP
sentradns-dns	Data (edge)	Authoritative DNS + DNS firewall, external secondary	Go · NSD/BIND · TSIG
Analytics (ELK)	Control	Log ingestion, search, real-time insight dashboards	Elasticsearch · Logstash · Metricbeat
AI Assistant	Control	Operations assistant, approval-gated action proposals	Multi-provider LLM (OpenAI-compatible)
Penetra optional	Federated	AI-assisted penetration testing, CVE verification	Federation API · RoE guard

2.3 High-Availability (HA) Topology

DATA PLANE

- Horizontally scalable multi-node edge fleet; each node serves traffic independently.
- Active per-origin health checks; unhealthy origins are removed automatically.
- Failover/backup origins and maintenance mode enable zero-downtime servicing.
- A node failure reroutes traffic to remaining nodes (via upstream LB/anycast).

CONTROL PLANE

- A control-plane outage does *not* affect traffic: edge nodes keep serving with their current configuration.
- State durability through PostgreSQL backup/replication.
- The deploy pipeline reports partial success; *force deploy* realigns on drift.
- Configuration is centrally sourced; a rebuilt node restores automatically via bootstrap.

03 — APPLICATION-LAYER SECURITY (WAF)

ModSecurity + OWASP Core Rule Set

The Sentra WAF engine is built on the industry-standard **libmodsecurity** and the **OWASP Core Rule Set (CRS)**. Each pool (application) can have an independent profile, sensitivity (paranoia) level and mode assignment.

3.1 OWASP Top 10 Coverage Matrix

OWASP TOP 10 (2021)	SENTRA CONTROL	STATUS
A01 Broken Access Control	Geo/IP access policies, IP allow-only, rate limiting, path-based rule sets	✓
A02 Cryptographic Failures	TLS 1.2/1.3 enforcement, HSTS, weak-cipher blocking, Full-Strict origin validation	✓
A03 Injection (SQLi/Cmd)	CRS SQLi/RCE/LFI/RFI rule groups, paranoia 1–4	✓
A04 Insecure Design	Behavioral baseline via Learn mode, gradual hardening	✓
A05 Security Misconfiguration	Central policy, chain/expiry auditing, secure defaults	✓
A06 Vulnerable Components	Penetra CVE verification (optional), signature/scan detection	✓
A07 Authentication Failures	Auth-bypass detection (CRS), rate limiting, IP reputation	✓
A08 Data Integrity Failures	Protocol/method enforcement, deserialization rules	✓
A09 Logging & Monitoring	Full event logging, ELK analytics, SIEM forwarding, audit trail	✓
A10 SSRF	Protocol/scheme restrictions, egress/request-pattern rules	✓

OPERATING MODES

- **Learn (Observe):** Rules are evaluated and violations logged, but *traffic is not blocked* — to safely calibrate false positives on a live application.
- **Block (Enforce):** Violations are blocked immediately.
- Logs clearly distinguish **LEARN** vs **BLK**, eliminating migration risk.

TUNING & FALSE-POSITIVE MANAGEMENT

- Paranoia 1–4: balance protection strictness against sensitivity.
- Request & Response protections: SQLi, XSS, RCE, scanner, data leakage (SQL/PHP/IIS error leakage, webshell).
- Built-in **CMS exclusions** (WordPress/Drupal, etc.) for rapid rollout.
- From the Logs screen, *one-click* rule disable (per-host/global) and IP block/whitelist.

Health-check endpoints can be exempted from WAF inspection; static-file bypass avoids unnecessary inspection and latency.

04 — DDOS DEFENSE & ACCESS CONTROL

Multi-layer rate limiting and geo/IP policies

4.1 Layered Defense

LAYER	MECHANISM	EXAMPLE CONTROL
L3 / L4	HAProxy stick-tables	Per-source-IP request/connection rate; silent reject (TCP RST) on threshold — before the WAF
Connection	Connection cap	Per-pool concurrent-connection ceiling (level presets: 8000/4000/2000/1000)
L7 (application)	ac-agent SPOE + WAF	Per-pool protection level, challenge, request-rate/anomaly
Policy	Geo / IP rules	Country and IP/CIDR allow/deny, block or log

PROTECTION LEVELS

- **Off · Low · Medium · High · Under Attack** — per pool.
- **Inherit:** A pool inherits the organization default; when the org profile changes, all inheritors update on the next deploy.
- Actions: **block · challenge · log**; challenge TTL configurable (5 min–24 h).

GEOGRAPHIC & IP ACCESS

- **Geo:** whitelist ("only these countries") or blacklist ("all except these"), by ISO codes.
- **IP:** allow-only (only permitted IPs) or blacklist; global or per-pool scope.
- GeoIP-based resolution; the decision point is in SPOE, at microsecond scale.

Fail-closed design (a critical advantage for finance): Geo/IP whitelist modes *deny* access when a match is ambiguous or geo data is missing. This technically guarantees a "deny on doubt" principle — but before enabling, at least one allow rule and (for geo) a loaded GeoIP database must be present. Sentra makes this secure posture the default.

05 — TLS/PKI, LOAD BALANCING & DNS

Traffic management and encryption

TLS / PKI MANAGEMENT

- Central certificate store: **PEM** and **PFX/PKCS12** upload.
- **ACME-native** automatic certificates (HAProxy 3.3 crt_store) — Let's Encrypt compatible renewal.
- Encryption modes: **Off · Flexible · Full · Full (Strict)** (origin certificate validation).
- Minimum TLS version (1.0–1.3), **HSTS**, **HTTP/2**, **0-RTT**.
- Certificate chain auditing (missing intermediate / expiry / untrusted root) and Origin CA generation.
- Wildcard and SAN certificates automatically cover matching hostnames.

LOAD BALANCING

- Algorithms: **Round Robin · Least Connection · Source IP · URI · URL Param**.
- Active health checks: interval, fall/rise thresholds, custom path/code/method.
- Weighted origin distribution, failover/backup, maintenance mode.
- Source-IP session persistence support.
- **Quick Pool:** auto-discovery of origin/port/TLS from a hostname.

5.1 DNS Security

AUTHORITATIVE DNS

- Full record management: A, AAAA, CNAME, MX, TXT, NS, SRV, CAA.
- Zone import: **BIND · Cloudflare · JSON**; export and versioned deploy.
- External **secondary** (NSD/BIND) support; per-zone **TSIG**-keyed zone transfer and notify.

DNS FIREWALL (ENDPOINT)

- Category-based domain filtering (malware, phishing, etc.).
- Reusable **profiles**, safe search, custom allow/block lists.
- Client/CIDR-based profile assignment, automatic device enrollment via token.

06 — OBSERVABILITY & FORENSICS

Real-time visibility, SIEM integration and audit trail

ANALYTICS (ELK-BASED)

- **WAF Security:** total events, unique attacker IPs/countries, attack-origin map, top attack types and triggered rules.
- **Load Balancer:** request/error rate, latency p50/p95/p99, top URLs, countries, termination states.
- **System Performance:** response time, request rate, connection and network metrics via Metricbeat.
- Time range (1h/24h/7d) and per-pool filtering.

SIEM & LOG FORWARDING

- Forwarding to a central log node via **rsyslog/syslog** (Logstash input).
- Structured WAF/access events — forwardable to enterprise SIEM (Splunk/QRadar, etc.) over syslog.
- Log detail includes full event JSON, match and tags; *one-click* response actions.
- Search over Elasticsearch (Lucene query language) with retention policy.

6.1 Immutable Audit Trail

Every configuration change — made in the panel, via API, or through the AI assistant — is recorded with its source (ai/ui/api), status, summary, rationale and timestamp. Eligible operations are **reversible (undo)**. This provides full traceability for financial audit and post-incident review.

Who · **When** · **Which source** (UI/API/AI) · **What changed** (target + field diff) · **Rationale** · **Status** (applied/undone) — all queryable.

07 — MULTI-TENANCY & AUTHORIZATION

Isolation, roles and governance

Sentra is **multi-tenant** by design. Each organization is fully isolated with its own set of domains, pools, certificates, users and policies. Different business units within a holding/subsidiary structure can be managed as separate organizations; a superadmin layer provides fleet-wide visibility.

7.1 Role-Based Access Control (RBAC)

ROLE	VIEW	BASIC OPS	PROFILE/CLIENT/TOKEN	FULL MGMT + DEPLOY	USER MGMT
Viewer	✓	—	—	—	—
User	✓	✓	—	—	—
Manager	✓	✓	✓	—	—
Admin	✓	✓	✓	✓	✓

A separate platform-wide **superadmin** tier provides organization creation, fleet visibility and centralized domain management.

7.2 Change Governance

STAGED

Changes are prepared first and never applied to production automatically. "N pending changes" indicator.

DEPLOY

Approved release; typed (LB/WAF/Security). Partial-success reporting and *force deploy*.

AUDIT + UNDO

Every operation is recorded and reversible; orphan cleanup (CLI) guards against drift.

08 — AI OPERATIONS & PENETRA

Human-approved automation and offensive security

AI OPERATIONS ASSISTANT

- Multi-provider LLM (OpenAI-compatible API: Groq/Ollama/Cerebras/DeepSeek — *self-hostable on-prem*).
- **Human-in-the-loop:** The assistant never applies a write operation automatically; it presents risk level and rationale via an *Action Card*, and the operator **approves**.
- Every AI-originated operation enters the audit trail and is reversible.
- Org-scoped tool registry — tenant boundaries are enforced at the LLM layer too.

PENETRA — CTEM & PENTEST PLATFORM

SEPARATE PRODUCT

- Three analysis tiers: **passive** (DNS/TLS/headers/CT-log discovery — always safe) → **mining** (behavioural baseline from WAF and access logs) → **active** (SQLi/XSS/SSRF/LFI, Nuclei, port scan, directory fuzzing).
- **RoE (Rules of Engagement) guard:** Active scanning runs only when a written engagement scope is defined; otherwise it is rejected. Full audit trail.
- **Log-driven policy mining:** learns each URL's method/parameter schema from Sentra's edge logs and proposes WAF policy — data external-only scanners cannot see.
- Integrated into Sentra via federation; findings stay in the institution's database. Also runs standalone (without Sentra).

> The AI layer is optional and can run on a **self-hosted LLM**, so privacy-sensitive institutions can use it without sending any data to an external service.

09 — DEPLOYMENT, INTEGRATION & SCALING

Deployment models and system requirements

ON-PREM

Entire stack inside the institution. Data sovereignty, internal-network visibility. Distributed as Debian packages (.deb).

AIR-GAPPED / BYOL

No-internet environments. Offline **Ed25519**-signed license + entitlement engine. AWS Marketplace BYOL AMI.

SAAS / MANAGED

Cloud control plane + managed edge. Fast to deploy (ideal for evaluation/PoC).

9.1 Integration Points

INTEGRATION	METHOD	STATUS
REST API	Full management API; automation/IaC and CI/CD integration	**Available**
SIEM / Logging	rsyslog/syslog forwarding + ELK; routing to external SIEM	**Available**
API authentication	Email/password session + organization API key	**Available**
ACME / PKI	Let's Encrypt-compatible automatic certificates; enterprise CA upload	**Available**
SSO (SAML/OIDC)	Single sign-on with enterprise identity provider	**Roadmap**
MFA / 2FA	Multi-factor authentication	**Roadmap**

9.2 Network & Port Matrix (summary)

DIRECTION	PORT/PROTOCOL	PURPOSE
External → Edge	443/TCP (HTTPS), 80/TCP (redirect)	Visitor traffic
External → DNS	53/UDP,TCP	Authoritative DNS / DNS firewall
Control → Edge	DataPlane API (mgmt), SPOE sync	Configuration distribution
Edge → Log	syslog (rsyslog)	Central log forwarding
Admin → Control	Panel/HTTPS + REST API	Management access

The exact port plan and segmentation (DMZ/internal) are finalized during the PoC per the institution's architecture.

9.3 Sizing

The data plane is **HAProxy**-based, proven in the industry for high concurrency and low latency. Per-node capacity depends on the traffic profile (RPS, concurrent connections, TLS handshake rate, WAF paranoia level) and hardware. The exact capacity and node-count plan is determined by **measuring during the PoC** against the institution's real load profile.

10 — COMPLIANCE & REGULATION

Technical controls that support regulatory compliance

Sentra **supports** the technical controls required by the frameworks below. (Certification is achieved through the institution's process, policy and audit as a whole — the mapping below shows the technical capabilities the platform provides.)

FRAMEWORK	RELEVANT REQUIREMENT	TECHNICAL CONTROL PROVIDED BY SENTRA
PCI-DSS	Req. 1/6.4.2 (WAF), 4 (TLS), 10 (logging & monitoring)	OWASP WAF, TLS 1.2/1.3 enforcement, full audit trail + SIEM forwarding
BRSA / BDDK (IT Regulation)	Penetration testing, access control, logging, data residency	Penetra pentest, RBAC, logging/monitoring, **on-prem data sovereignty**
KVKK (TR Data Protection)	Personal-data security, access limitation, audit logging	Tenant isolation, geo/IP access, audit trail, data kept on premises
ISO/IEC 27001	A.8/A.12/A.13 access, operations, communications security	RBAC, change governance, network security controls, monitoring
GDPR	Integrity & confidentiality, data minimization	Encryption, access control, data localization via self-hosted AI

DATA SOVEREIGNTY

- In on-prem/air-gapped deployment, traffic and log data **never leave the institution**.
- The AI layer can run on a self-hosted LLM without sending data to any external service.

ACCOUNTABILITY

- Immutable audit trail + undo provides a full "who, what, when" record.
- Controlled deploy enforces change governance and an approval chain.

> The compliance mapping is informational and should be evaluated together with the institution's existing policy and audit processes.

11 — POC METHODOLOGY & ROADMAP

Proof of Concept process

A Sentra PoC is run in a controlled environment against the institution's real (or representative) traffic profile. A typical PoC completes in 1–2 weeks, with technical success criteria agreed in writing up front.

PHASE	CONTENT	OUTPUT
1. Preparation	Scope, target applications, success criteria, RoE; network/port plan	PoC plan
2. Installation	On-prem admin + 1+ edge node; DNS/pool/origin definition	Running environment
3. Security	WAF learn→block calibration, DDoS/geo/IP policies, TLS	Hardened profile
4. Observability	ELK dashboards, SIEM forwarding, audit-trail verification	Visibility
5. Validation	Controlled attack scenarios, Penetra (optional), load testing	Evidence report
6. Evaluation	Success-criteria comparison, sizing, production plan	Findings & proposal

11.1 Roadmap (Transparency)

NEAR TERM

- Planned SSO (SAML/OIDC) for enterprise identity integration.
- Planned MFA / 2FA for administrator authentication.

CURRENT MATURITY

- Production WAF, DDoS, LB, DNS, TLS, analytics, RBAC, audit trail, SIEM forwarding.
- Production On-prem/air-gapped deployment, BYOL licensing.

Next Step

To plan a PoC tailored to your institution and arrange a technical deep-dive session, please get in touch.

[Company Name] · [full name] · [email] · [phone] · [web]