SALUS

SECURITY & DEPLOYMENT DATASHEET

Security, *inside your perimeter*

Review how Salus handles data, keys, access and operational evidence in your environment. Core protection runs locally; the deployment defines identity integration, retention and optional capabilities. Twenty-five named controls give your security team a clear basis for review.

DETECT, REPLACE, SEND, RESTORE, RECORD

Local
processing and state in your environment

CPU
core text detection; GPU additions on request

Your keys
customer-controlled mappings and review data

25
named controls with delivery scope

02 Deployment and data custody
03 Control catalogue
04 Security review

PUBLISHED BY
SALUS

OCTOBER 2026
26 OCTOBER 2026

Designed for your environment

Salus runs inside your perimeter. Your platform controls storage, keys, access and the chosen AI route. Sensitive values are replaced before protected content continues to the model. **The same controls apply to every Salus surface**: Engine, Desktop, Salus Chat, the gateway relay and the meeting note-taker all run on the one Engine in your environment.

INSIDE YOUR ENVIRONMENT	AT THE BOUNDARY	SELECTED AI PROVIDER
Original content and state	**Protected content**	**Works over tokens**
Salus, policy, token mappings, keys and review records.	Category-typed tokens preserve distinct references. Source images stay inside.	Authorised restoration happens on the return path, inside your environment.

The AI provider and your infrastructure remain under your organisation's contracts and controls.

Deployment and operating scope

AREA	WHAT THE DEPLOYMENT PROVIDES
Surfaces `Core / delivered`	Salus Engine (API) and Salus Desktop are core. Salus Chat, the protected gateway relay and the meeting note-taker are delivered per deployment on the same Engine, inside the same perimeter and under the same controls, keys and review records.
Runtime `Core / workload-sized`	Private Helm deployment for Kubernetes and OpenShift, with non-root containers and mirrored registries. Text detection runs on CPU. Optional OCR and Semantic Layer processing use GPU acceleration.
State and key custody `Core`	Token mappings, configuration and review records use your PostgreSQL; coordination and rate limits use your Redis. Keys remain yours. No document, key or product telemetry is sent to a Salus-hosted service.
Calling systems `Core`	Organisation-scoped API keys, route permissions, distributed rate and concurrency limits. Restoration is a separate authorised operation inside the workflow.
Identity and administration `Configured`	Console access, languages, directory integration through Active Directory, LDAP or single sign-on, and group-to-role mappings are configured for the deployment. Administration, review and restoration permissions can be separated.
Security and review data `Core / configured storage`	Security events carry stable codes without sensitive values. Review storage is configured to encrypt values with your key and retain them for the agreed period. Recording to PostgreSQL is best-effort, with loss alerts.
Release and monitoring `Core / configured / delivered`	Pinned models and rules, a release manifest with image and model hashes, and CycloneDX SBOM. Signing is configured to your release process. OpenMetrics is core; dashboards and alerts are delivered in your monitoring platform.

> **Token lifecycle.** The same value keeps its token while its Context is retained. Mappings are retained per Context and can be deleted per Context. Review-record retention and token-mapping deletion are defined separately in the deployment.

Your platform owns

Network access, ingress TLS, certificates, database operations, backups, provider credentials and the authorised destinations for restored values.

Agree before activation

Workloads, file types, languages, identity roles, retention, failure handling and capacity. OCR and semantic policies are available on request and validated for the workload.

25 controls, with delivery scope

Use the control codes in architecture reviews, pilot acceptance and procurement. Confirm the applicable scope for your environment and selected workflow.

Core
Included in the relevant Salus deployment.

Configured
Set up for your environment during rollout.

Delivered
Built or extended for the agreed engagement.

CODE	CONTROL	SCOPE
A / DETECTION		
SC-01	Sensitive-value detection with validated rules and specialised models.	Core
SC-02	Identifier checksums where defined; labels and context otherwise.	Core
SC-03	Supported telecom identifiers, including IMSI, ICCID, IMEI and MSISDN.	Core
SC-04	Contextual verification of supported candidate types.	Core
SC-05	Organisation-specific identifier formats for the agreed workflow.	Delivered
SC-06	Local file protection; source images are never forwarded.	Core
B / PROTECTION AND RESTORATION		
SC-07	Opaque, category-typed tokens scoped to a retained Context.	Core
SC-08	Optional format-preserving encryption with customer-held keys.	Configured
SC-09	Authorised restoration inside the perimeter and relevant Context.	Core
SC-10	Stop the workflow when required protection cannot complete.	Core
SC-11	Gateway protection and restoration, including supported text streaming.	Configured
SC-12	Managed Desktop workflows, with review for supported file paths.	Configured
C / ORGANISATION, IDENTITY AND OPERATIONS		
SC-13	Organisation-scoped API keys, route permissions and isolation.	Core
SC-14	Distributed rate and concurrency limits through shared Redis.	Core
SC-15	Administration console and API-key lifecycle management.	Core
SC-16	Review of recorded runs; no silent retraining from traffic or feedback.	Core
D / EVIDENCE AND AUDIT		
SC-17	ECS security events with stable codes and no sensitive values.	Core
SC-18	PostgreSQL review records, best-effort recording and loss alerts.	Core
SC-19	Service metrics through OpenMetrics.	Core
SC-20	Restore events: key identity, organisation, request and time.	Core
SC-21	Finding detail: class, confidence, detector, verifier result and replacement.	Core
E / DEPLOYMENT AND SUPPLY CHAIN		
SC-22	Private Helm deployment, non-root containers and mirrored registries.	Core
SC-23	Release manifest, model and image hashes, and CycloneDX SBOM.	Core
SC-24	No Salus-side document, key or product-telemetry copy.	Core
SC-25	CPU text detection under pinned model and rule versions.	Core

Optional and deployment-specific scope. OCR and semantic policies are available on request and use GPU acceleration. Directory integration, policy, retention and signing are configured. Dashboards, alerts and additional identifier formats are delivered for the engagement.

Framework mappings to OWASP Top 10 for LLMs, NIST AI RMF and ISO 27001 Annex A support the review. Mapping is not certification. Use the deployment scope and acceptance evidence to determine which requirements are met in your environment.

Review one complete data flow with your security team. Agree the boundaries, permissions and evidence before moving the workflow into production.

NEXT STEP

Scope your security review

Bring your architecture, identity requirements and retention policy. Together, define the deployment scope and the checks your pilot must pass.

DETECT → REPLACE → SEND → RESTORE → RECORD

SALUS

salusapp.ai

Read alongside the Salus Technical Overview, Benchmark Report, Use Case Guide and Whitepaper.
This datasheet describes control and deployment scope. Benchmark measurements and illustrative workflows are published separately.

Salus is a product of Paramosoft Yazılım Hizmetleri Limited Şirketi.
Address: İzzet Paşa Mahallesi, Yeni Yol Caddesi No: 3, Nurol Tower, Floor 34, Office 3409, Şişli, İstanbul.

© 2026 Paramosoft Yazılım Hizmetleri Limited Şirketi. Salus Security & Deployment Datasheet, October 2026. Capabilities are core, configured per deployment or delivered per deployment. Customer acceptance is measured on the agreed deployment. Tokens constitute reversible pseudonymisation, not anonymisation.

SALUS