Deltawall

SOLUTION BRIEF

Deltawall solution brief

EU-sovereign AI-usage control: capabilities, architecture, console, specifications, use cases and honest limits.

September 2026 · Deltawall B.V. · deltawall.ai

EU-sovereign AI-usage control

Deltawall stops sensitive data from leaking into AI tools, produces a tamper-evident audit record for the DPO and the auditor, and gives the CISO a posture dashboard. It is proxy-free by design: inspection and enforcement happen in the browser, at the moment of interaction, and raw content never leaves the device.

Core product capabilities

1. **On-device detection.** Prompts and files are classified in the browser before they are sent. Raw content never leaves the endpoint.
2. **Real-time, last-mile control.** Allow, Log, Warn, Redact and Block, applied at the input box at submit. A Warn can require a written business justification before the user proceeds.
3. **File-upload inspection.** The file picker, drag-and-drop and paste all pass through one on-device scan: PDF, DOCX, XLSX, PPTX, CSV, TXT, MD and JSON.
4. **Tamper-evident evidence log.** Hash chain, Merkle sealing and Ed25519 signatures, with a standalone offline verifier and exportable evidence packs.
5. **Privacy by design.** The backend stores data-class labels and salted hashes only. Subjects are pseudonymised. GDPR erasure works by salt deletion.
6. **No individual scoring.** Dashboards aggregate to department level only. Built to be works-council safe.
7. **Zero interception.** No TLS interception, no root certificate, no kernel driver and no per-app hooking. User mode and the browser sandbox only.
8. **Developer and API governance.** An opt-in, OpenAI-compatible gateway applies the same policy and payload redaction to apps, scripts and agents.

Architecture

COMPONENT	ROLE
Browser extension	Chrome, Edge and Firefox (Manifest V3). Sensor and enforcer: detects, evaluates policy, then redacts or blocks in the page.
Detection engine	Two layers: checksum, format and context validators for exact data classes, and an on-device ONNX model for names, addresses, health data and organisation-confidential text. The checksum layer always wins.
Policy engine	A rule language, evaluator and simulator, with four ready-made EU compliance templates.
Evidence log	Hash-chained, Merkle-sealed, Ed25519-signed records of every decision.
Management console	Multi-tenant web console with role-based access, backed by PostgreSQL, hosted in the EU region you choose.
AI gateway (opt-in)	OpenAI-compatible endpoint for developers and apps: per-key policy, payload redaction and a provider allow-list.
MDM policy bundles	Desktop AI apps are governed with exported blocklists for your MDM, not by interception.

A standalone **evidence verifier** checks an exported evidence pack without any access to Deltawall, and a **model training pipeline** benchmarks the on-device model with a precision gate on checksum classes in continuous integration.

The console

One web console for the CISO, the DPO and the auditor. It shows data-class labels and salted hashes, never content.

- **Posture overview:** AI-usage risk across the organisation, by department.
- **Activity:** events by data class, destination and department.
- **Telemetry:** a searchable log explorer with live tail, facets and a volume chart.
- **Policies:** rule builder, templates, simulator and version history.
- **Employees and rollout:** directory coverage and extension pairing.
- **Evidence:** browse the chain, run Verify chain in one click, export JSON, CSV or PDF.
- **Compliance:** template status, retention and minimisation, the DPIA template and the works-council pack.
- **Admin and privacy:** members and roles, works-council mode and four-eyes unmasking.

Technical specifications

AREA	SPECIFICATION
Browsers	Chrome, Edge, Firefox
AI sites covered	ChatGPT, Claude, Gemini, Microsoft Copilot, Perplexity, DeepSeek
Financial data	IBAN, payment card, Dutch VAT (BTW), KvK number
National identifiers	BSN, German Steuer-ID, German Steuernummer, EU national ID, BIG number
Personal data	Email, phone, IP address, date of birth, Dutch postcode
Secrets	API key, generic secret, private key, JWT, AWS key, GCP key
Model classes (Chrome, Edge)	Person name, postal address, health data, organisation-confidential
Other	Source code, uninspectable content
File types	PDF, DOCX, XLSX, PPTX, CSV, TXT, MD, JSON
Policy actions	Allow, Log, Warn, Redact, Block
Policy templates	GDPR baseline, Financial (DORA-aligned), Government (strict EU residency), Education
Channels	Browser, Gateway, Desktop (MDM policy only)
Gateway providers	Mistral (EU), Azure OpenAI EU (EU), OpenAI, Anthropic, DeepSeek
Roles	Owner, Admin, Security engineer, Analyst, Auditor, DPO
Desktop apps (MDM)	ChatGPT Desktop, Claude Desktop, DeepSeek Desktop, Microsoft Copilot
MDM outputs	AppLocker policy, DNS blocklist, Jamf profile
Evidence export	JSON pack, CSV, PDF
Supply chain	CycloneDX SBOM, dependency audit gate, container image scanning, CRA incident workflow

Roadmap, not offered today: single sign-on through OIDC (Microsoft Entra ID, Google Workspace, Okta, Keycloak) is built and will be offered after early access; SAML needs an external SAML-to-OIDC bridge. Shadow-AI discovery has an ingest API but needs a DNS or metadata feed before it can report.

Use cases

1. **AI data leakage prevention.** IBANs are masked in the input box before send. Secrets are blocked at submit, with the reason shown to the user.
2. **AI access control.** Block non-EU or unsanctioned AI providers, with rules per department and per destination.
3. **Safe file uploads to AI.** Documents are scanned on the device and sensitive files are stopped before upload. Scanned PDFs are flagged as cannot-inspect.
4. **Developer and API governance.** The gateway redacts or blocks payloads and enforces EU-resident providers for apps and scripts.
5. **Audit and regulator evidence.** Export a signed evidence pack that anyone can verify independently, offline.
6. **Works-council-safe monitoring.** No individual tracking. Identity is unmasked only with four-eyes approval, where the approver must differ from the requester.

Key benefits

- **Content stays on the device.** The extension's options page lists every payload that left the browser: labels, hashes and metadata.
- **Evidence you can prove.** The audit record is tamper-evident and can be verified without trusting Deltawall.
- **EU-sovereign.** Hosted in your EU region, with an EU-first provider allow-list and a ready rule to block non-EU AI.
- **Zero infrastructure change.** No proxy, no certificates and no network rerouting.
- **Small risk surface.** User mode and the browser sandbox only. No kernel components anywhere in the product.
- **Supply-chain hygiene.** An SBOM for every artifact, an audit gate, image scanning and a Cyber Resilience Act reporting workflow.

Honest limits

- No OCR. Scanned PDFs are flagged as uninspectable, not read.
- Redact works on the browser and gateway channels. On the desktop channel a Redact rule returns an error and never silently downgrades.
- Redact applies to typed prompts, and the user presses send again after masking. A file that needs redaction is stopped, not rewritten.
- The on-device model runs in Chrome and Edge. Firefox uses the deterministic layer.
- The upload guard and the model fail open on error or timeout, so a broken scanner cannot break the AI site.

- Browser coverage is bounded to the AI sites listed in this brief.

Control AI usage without intercepting anyone's traffic. Book a 30-minute demo at deltawall.ai/demo, or request early access at deltawall.ai/early-access.

Deltawall B.V. · info@deltawall.ai · deltawall.ai