EXECUTIVE SUMMARY

CID222 is a multi-platform API Gateway-based AI security solution that protects enterprises from data leakage, compliance violations, and emerging AI threats. Deployed transparently across your AI infrastructure with sub-150ms latency, CID222 provides comprehensive protection for OpenAI, Claude, Azure OpenAI, Gemini, and custom LLM implementations.

THE CHALLANGE

- 89% of organizations use AI without adequate data protection
- 73% of employees use unauthorized AI tools, exposing sensitive data
- Organizations have 0% visibility into AI model interactions and data flows
- Average GDPR fine for data leakage: $4.4M
- Shadow AI spreading across organizations—unapproved, unmonitored, and unstoppable

CORE FEATURES

INPUT & OUTPUT FILTERING

Bidirectional protection with NER and regex-based detection of PII/PHI/financial data. Real-time masking on inputs and intelligent output sanitization prevents data leakage, hallucinations, and sensitive information exposure. Supports 40+ pattern rules with >90% accuracy.

POLICY ENGINE

Dynamic policy-as-code system using Policy Agent. Define, version, and enforce custom privacy rules with JSON templates. Real-time policy violation alerts and audit trails.

OCR & DOCUMENT PROCESSING

Extract and mask sensitive data from images, PDFs, and scanned documents. Comprehensive text recognition with automated PII/PHI redaction across multiple file formats.

AUDIT & OBSERVABILITY

Complete audit trails with Elastic/MongoDb logging, Prometheus metrics, and SIEM integration. Track every request, masking event, and policy decision with <150ms latency.

DEPLOYMENT OPTIONS

CLOUD & HYBRID

Fully managed SaaS with automatic updates and 99.9% uptime SLA. Hybrid deployment combining cloud scalability with on-premises control for sensitive data processing.

ON-PREMISES

Deploy on Docker, Kubernetes, or bare metal within your infrastructure. Air-gapped deployments available. Complete data sovereignty and zero cloud dependencies.

TECHNICAL SPECIFICATIONS

SPECIFICATION	DETAILS
API Gateway Latency	<150ms
Detection Accuracy	>90%
Pattern Rules	50+ built-in, custom rules
Uptime SLA	99,9% (Cloud)
Supported LLMs	OpenAI, Claude, Azure, Gemini, Custom
	LLMs

COMPLIANCE & CERTIFICATIONS

- GDPR - General Data Protection Regulation
- EU AI Act - Fully compliant and audit-ready
- ISO 27001 - Information Security Management
- ISO 42001 - AI Management System Standard
- SOC 2 Type II - Security & Confidentiality
- HIPAA - Healthcare data protection
- KVKK - Turkish Personal Data Protection Law

TARGET INDUSTRIES

- Financial Services - AI for customer service, fraud detection, risk assessment
- Healthcare & Life Sciences
- HIPAA-compliant AI diagnostics and patient care
- Insurance - Claims processing and customer interactions
- Retail & E-Commerce- Customer service and personalization engines
- Government & Public Sector - Compliance-critical AI applications
- Manufacturing & Enterprise - Data sovereignty and IP protection

COMING SOON

- SIEM Integration - Unified threat intelligence platform
- XDR Capabilities - Extended detection and response
- MCP Support - Model Context Protocol security
- Conversation Hardening - Advanced agent security

CID222

Security Begins Where AI Thinks