PRODUCT FACT SHEET

Cyprawall

AI Firewall & AI-Usage Governance Platform

Vendor: Baseel

PRODUCT OVERVIEW

Cyprawall is an AI firewall and AI-usage governance platform built for organizations that need visibility and control over how employees interact with generative AI tools. As AI adoption inside companies increasingly happens outside IT's knowledge ("shadow AI"), Cyprawall sits between users and public AI services to discover what's being used, inspect what's being sent, stop sensitive data from leaving the organization, and keep a defensible audit record of everything that happened. It is positioned as an enterprise security control — rolled out and managed by a security team, not a self-serve productivity tool.

TARGET CUSTOMERS

- Mid-to-large enterprises with a dedicated IT/security or GRC function
- Regulated industries (finance, legal, healthcare, government) where data leakage via AI tools is a compliance risk
- Security and compliance teams responsible for AI governance, data loss prevention, and SIEM-based monitoring
- Organizations with a distributed workforce using a mix of managed and unmanaged devices (desktop, mobile, browser)

CORE CAPABILITIES

01 Shadow AI discovery

Identifies unsanctioned AI tool usage by reading OAuth grants across Google Workspace, Microsoft Entra ID, Slack, GitHub, and GitLab, surfacing tools IT didn't approve or know about.

02 Real-time traffic interception

Inspects traffic to major AI services (ChatGPT, Gemini, Claude) as it happens, and blocks or redacts PII, credentials/secrets, and proprietary source code before a prompt ever leaves the organization's network.

03 Flexible deployment architecture

Three ways to enforce policy depending on the environment:

- **Network gateway** (TLS-inspecting proxy) for network-level enforcement
- **Desktop agent** (Windows, macOS) and Android agent for device-level enforcement

contactus@baseel.com · +44 20 4540 0111

- **Browser extension** for lightweight, browser-level enforcement

04 **AI tool risk scoring**
Evaluates and scores AI tools in use by risk level, helping security teams prioritize which tools need review, restriction, or removal.

05 **Tamper-evident audit logging**
Maintains a hash-chained audit log of AI usage and policy actions, exportable to the customer's SIEM for compliance and incident investigation.

06 **Guided AI tool decommissioning**
Generates off-boarding checklists to help teams systematically retire or restrict risky/unsanctioned AI tools.

USE CASES

- **Shadow AI visibility:** Give security teams a single view of every AI tool employees are actually using, not just the ones IT approved.
- **Data loss prevention for AI:** Stop PII, trade secrets, source code, and other sensitive data from being pasted into public AI chat tools.
- **Compliance & audit readiness:** Produce a tamper-evident, exportable record of AI usage activity to satisfy internal audit, regulatory, or incident-response requirements.
- **Risk-based AI governance:** Score and triage AI tools by risk so security teams can decide what to allow, restrict, or block.
- **Controlled AI tool retirement:** Decommission risky or redundant AI tools with a structured, repeatable checklist rather than ad hoc blocking.

DEPLOYMENT

- **Model:** Software / SaaS — multi-tenant cloud control plane
- **Enforcement components:** network gateway (proxy), desktop agent (Windows/macOS), Android agent, browser extension — deployed in combination based on the customer's environment
- **Alternative deployment:** self-hosted / on-premises installation available for customers that cannot use a multi-tenant cloud control plane
- **Integration:** audit log export to customer SIEM

COMPANY INFO & CONTACT

- **Vendor:** Baseel
- **Official website:** http://uat-ai-firewall.cypra.ai/
- **Address:** 167-169 Great Portland Street, London, W1W 5PF
- **Phone:** +44 20 4540 0111
- **Email:** contactus@baseel.com