

AI Firewall

See the AI your people already use — and control what it can touch.

Generative AI has become the fastest-growing shadow IT in the enterprise. AI Firewall discovers the AI tools your people use — sanctioned or not — scores their risk, and controls what they can do. Built on the Browse layer, so you can embrace AI without the blind spot.

WHY AI FIREWALL

Let your people use AI. **Just not blindly.**

Staff are already pasting documents, code and customer data into AI tools — mostly on personal accounts, mostly invisible to IT. AI Firewall gives you the visibility and control to say yes to AI safely.



SHADOW AI Discover

- Surface the generative-AI tools in use across your organisation — sanctioned or not — from a catalogue of recognised AI applications.
- Distinguish the tools you've approved from the ones your people found for themselves.



RISK-SCORED Assess

- Every AI app, and the actions within it, carries a risk score — drawn from a catalog of 2,000+ cloud apps and 8,000+ rated actions.
- See which tools touch your data, and how risky each interaction really is.



ACTION-LEVEL Control

- Allow, block or track by action — stop uploads and shares of sensitive data to AI tools while letting people use the ones you trust.
- Enable AI safely, instead of blanket-blocking it and pushing people to personal accounts.

Built on the Browse layer — [Web Security](#) and [Cloud Application Security](#) — delivered through a single CloudUSS interface.

THE BLIND SPOT

Generative AI is the new shadow IT.

AI tools are the fastest new way for confidential data to leave your organisation – and most of it happens where traditional controls can't see. Analysts warn that a large share of AI-related data loss now stems from staff using generative AI outside IT's line of sight. AI Firewall closes that gap without standing in your people's way.

IP & source code

Customer & patient data

Personal accounts

Unsanctioned tools

Regulated data

No audit trail

CAPABILITY

See it. Control it. **Enable it.**

Three moves at the web and cloud edge, built on the CASB and Web Security you already know.



See every AI tool

- ✓ Discover the generative-AI apps your people use, sanctioned or not
- ✓ Distinguish corporate from personal-account access to AI services
- ✓ Classify tools as approved or unapproved, per user and group



Control the data

- ✓ Allow, block or track uploads, shares and downloads to AI tools by action
- ✓ Check file type by MIME inspection to limit what can be uploaded to an AI service
- ✓ Inline agent and gateway see browser-based AI use that API-only tools miss



Enable safe use

- ✓ Permit the AI tools you trust while restricting the risky ones
- ✓ Give people a sanctioned path so they don't route around you
- ✓ Report on who used which AI tool, when, and what they did

2,000+

cloud apps discovered

8,000+

actions risk-rated

Inline

coverage of browser AI usage

1 click

to enable for Web Security customers

Discovered, scored, controlled.

[illegible]

The screenshot displays the Cisco ISE GUI for configuring a Cisco Sanitized App. The interface is organized into several panels:

- Active:** Shows the app name "Cisco Sanitized App" and a description: "This rule allows the Cisco Sanitized App." Below this is a "Description" field.
- Selected Conditions:** Lists conditions such as "On host with Sanitized App" and "Sanitize Generate Action".
- Selected Monitors:** Lists monitors like "Sanitize Generate Action".
- Selected Actions:** Lists actions including "Log level", "Template", and "Sanitized App". The "Sanitized App" action is highlighted, showing its configuration.

The "Sanitized App" action configuration includes a "Sanitized App" dropdown menu and a "Sanitized App" text input field.

What you get.

Permit the AI tools you trust while restricting risky ones, and report on who used which tool, when, and what they did.

DEPLOYMENT

Inline where it matters, across desktop and mobile.

Agent	Windows and MacOS agents enforce policy at the endpoint, inline and proxy-less – seeing browser-based AI usage that API-only tools cannot.
Gateway	TrustLayer Gateway installs on a lightweight VM or physical server in under 30 minutes to extend policy across your own network.
Mobile Gateway	Extends protection to managed iOS and Android devices when AI apps are accessed via the browser (native mobile apps are not supported).
Instant enablement	Cloud application control can be enabled instantly for existing Web Security customers, with no additional hardware, software or configuration changes.

MANAGEMENT & REPORTING

Central control.

Policy Engine	Sophisticated policy engine including AzureAD attributes, IP, MAC address, device type, custom tags and differential actions, combined with AND/OR logic.
File Controls	MIME-type checking inspects the kind of file being uploaded and can block it before it reaches an AI tool. Full data loss prevention (DLP) is on the roadmap.
Web Portal	Fully integrated with TrustLayer's other modules, the CloudUSS dashboard offers a single pane of glass for management and reporting.
Reporting & Audit	Query logs by user, device, cloud app, action, risk level and outcome, for visibility and compliance. Log streaming to SIEM available.

PART OF THE TRUSTLAYER PLATFORM

AI Firewall is part of the Browse layer, built on Web Security and CASB. Eight solutions, four layers, one platform.



Browse

Web

CASB



Posture

CSPM

SSPM



Mail

Email

Archiving



Users

SAT

MFA