AI USAGE & AGENT SECURITY

AI Guard

AI adoption.
With boundaries you define.

Evaluate AI use, prompts and managed agent actions within a defined visibility and policy scope in the ScoutByt ecosystem.

AT A GLANCE

01 Browser & prompt controls

02 Model traffic policies

03 Managed agent boundaries

04 Audit & security events

AI Guard represents the evaluation scope of the AI security approach presented as ScoutByt AI Security. Available controls depend on the supported surface, configured policy and validated deployment scope.

CAPABILITIES & WORKFLOW

Evaluate AI controls within clear boundaries.

01 ## Understand AI use

Within a validated evaluation, Browser Guard and Application Discovery can support visibility into AI use across supported environments.

02 ## Set data and prompt boundaries

Within supported traffic paths, Prompt Guard and AI Gateway can apply configured controls to prompts and model traffic.

03 ## Define agent access

Within a defined evaluation, Agent Guard and MCP & Tool Control can assess managed sessions, resource access and tool actions.

04 ## Review the decisions

Where enabled in the evaluated scope, Policy Center and Audit & Security Events can bring policy decisions and security context into review.

AI usage surfaces

Context & policy

Scoped controls

Audit & review

USE CASES & DEPLOYMENT

Validate the environment before enforcement.

Enterprise AI adoption	Assess browser-based AI use and define appropriate data boundaries.
Developer workflows	Evaluate model traffic and tool calls within supported developer environments.
Managed agent sessions	Define resource-access and action boundaries for a controlled evaluation.

Integration areas: Supported browsers · Model gateways · Developer environments · MCP & managed tools

The supported environment and control matrix are agreed during technical discovery. Naming an integration category does not imply every provider or version is supported.

info@softbytlabs.com