

PRODUCT OVERVIEW

Before the threat becomes visible.

Govern AI with confidence.

ScoutByt AI Security Product Overview

An enterprise security platform designed to bring browser use, developer tools, model traffic, and AI agents under a common visibility and policy-driven governance approach.

AI VISIBILITY

PROMPT & DATA PROTECTION

AGENT & TOOL CONTROL

A SOFTBYT LABS PRODUCT FAMILY • PUBLIC OVERVIEW



PRODUCT OVERVIEW

Why now?

Enterprise AI adoption is expanding quickly, while risk is no longer confined to a single application.



Shadow AI

Unapproved tools can create visibility, accountability, and governance gaps.



Data leakage

Prompts, files, and copy-paste flows may unintentionally expose sensitive information.



Excessive agent authority

An AI agent does not automatically need every resource its user can access.



Fragmented control

Browsers, desktop apps, developer tools, and model traffic are different security surfaces.

Core approach

Do not simply ban AI. Make it visible, bounded, and policy-driven.

PRODUCT OVERVIEW

Layered protection in one platform

ScoutByt does not force one control method onto every surface; it uses the security points supported by each surface.

**Browser Guard**

Evaluate prompts, files, and data movement across supported browser surfaces.

**Prompt Guard**

Inspect sensitive content before provider delivery on supported flows.

**AI Gateway**

Route supported model traffic through central security and data policy.

**Agent Guard**

Govern supported AI agents with controlled sessions and resource boundaries.

**MCP & Tool Control**

Keep approved tools and integrations within policy.

**Application Discovery / Policy Center**

Gain visibility first, then apply central policies in controlled stages.

Identity + Policy + Resource + Network + Audit

The platform treats user authorization and AI-agent authorization as separate security decisions.

PRODUCT OVERVIEW

Business value and rollout

A staged, measurable adoption model designed to preserve business continuity.

1

Discover

Make AI surfaces and risky behavior visible.

2

Define policy

Set rules by data, user, device, and use case.

3

Pilot

Validate impact with selected users and applications.

4

Apply in stages

Increase enforcement only across proven surfaces.

Risk visibility

Assess shadow AI and fragmented usage through a common view.

Data protection

Reduce the risk of sensitive content leaving through model traffic.

Separate AI authority

Distinguish user access from agent access.

On-prem priority

Align with central management and data-sovereignty needs.

Lower operational impact

Progress in stages while assessing workflow impact.

Vendor-neutral model

Create common governance without depending on one AI provider.

Contact Softbyt Labs for a technical assessment and pilot plan.