Velatir

HUMANS-IN-THE-LOOP

The visibility gap organisations have with AI

Most organisations can't say how AI is being used inside them. The tools arrived quickly and spread through everyday work. What is missing is visibility. Which tools are in use, who relies on them, and where data actually goes.

Velatir

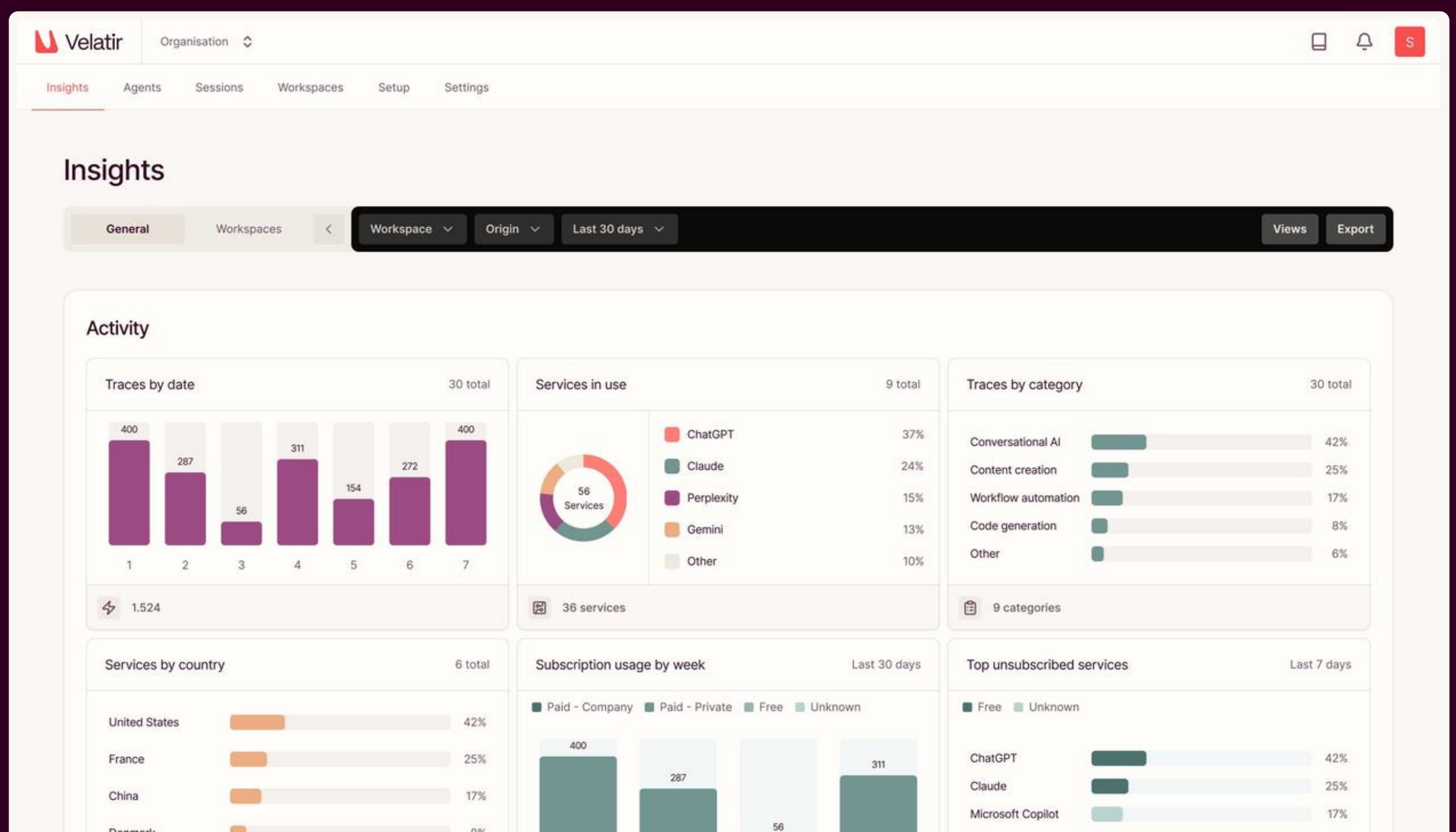
THE MOMENT WE ARE IN

Most companies are not failing at AI. They are failing at controlling it.

AI is being adopted faster than most organisations were designed to absorb. New tools arrive before the last ones are understood. Velatir gives you a way to see what is in use and decide how it should be handled. People stay accountable for those decisions. The work keeps them informed.

WHAT WE CAN SEE

AI adoption is often invisible



Velatir

THE VISION

Every organisation needs a way to coordinate how AI is used. Velatir is that layer.

AI is already distributed across teams, tools, and individuals. Most organisations didn't plan it that way. It happened gradually, and now they're managing the consequences.

A year ago, most organisations were running one or two approved tools. ChatGPT here, Copilot there. Today those same organisations are running dozens, often without realising it. Every team has found their own shortcuts, and the list keeps growing. Keeping up with what's in use has become harder than getting people to use AI in the first place.

Without clear governance, the result is predictable. Overlapping tools, inconsistent outputs, no clear ownership. Complexity compounds quietly until it starts costing you.

The organisations that get the most from AI will be the ones who know what they have, who is responsible for it, and how it connects.

Velatir

THE PROBLEM

AI tools are already in use across your organisation. Most of them have never been reviewed, approved, or tracked.

Visibility

You don't have a full picture of which tools your teams are using, how they're being used, or what data is moving through them.

Exposure

Employees are sharing data with AI tools the organisation has never reviewed. It is happening today, across every team, without any record.

Friction

Without a clear picture of AI usage, leadership cannot make confident decisions about where to invest or expand. Uncertainty slows progress.

Velatir

THE PRODUCT & WHY US

The infrastructure layer every AI-enabled organisation will need.

Velatir sits across every AI tool your organisation uses. Not inside one service, but across all of them. That gives you consistent visibility, control, and accountability regardless of what your teams are using.

01 Full visibility

AI activity across 4,200+ tools is logged and surfaced in one place. You can see which tools are in use, by which teams, what data is moving through them, and how your organisation compares to industry peers.

02 Agentic supervision

Velatir enforces your policies across every AI service. Unapproved services can be blocked. Sensitive inputs are intercepted before they leave your organisation. Over time, the platform learns your organisational boundaries and applies them consistently.

03 EU-ready by default

Velatir is built for the European regulatory environment. GDPR, the EU AI Act, and emerging obligations are reflected in how the platform works. Your organisation stays audit-ready without additional effort.

Velatir

AI GOVERNANCE PLATFORM

Visibility and guidance for every AI interaction

Velatir deploys specialised agents where your team uses AI. They provide real-time guidance, protect sensitive information, and give your organisation clear visibility into how AI is used across workspaces.

How it works

1 Deploy agents

Assign agents to workspaces. Each one brings domain expertise in areas like data protection or brand compliance.

2 Guide interactions

Agents work alongside employees in real time. When a critical action needs a human decision, it escalates to Slack or Teams.

3 Gain visibility

Every interaction generates insight. See which AI tools are used, identify patterns, and spot areas that need attention.

Instant visibility

From the moment agents are active, your organisation sees how AI is used. No configuration required.

- Which AI tools and services are in use
- Usage patterns and trends across workspaces
- Areas that may need closer attention
- Audit-ready records of every interaction

Real-time guidance

Agents work where employees interact with AI. They provide guidance and protect sensitive information in real time.

- Protect sensitive data and credentials in context
- Guide brand, compliance, and operational standards
- Escalate critical decisions to the right people
- Agents improve as humans resolve escalations

Specialised agents

Gatekeeper

Access Control

Data Protection

Sensitive Data

Brand Guardian — Coming soon

Content Standards

Each agent brings domain expertise into AI interactions. Gatekeeper controls access to AI services. Data Protection detects sensitive information before it leaves the organisation. Brand Guardian reviews AI-generated content against your standards. Optional skills extend each agent with additional intelligence, such as compliance mapping or brand perception monitoring.

Deployment

Browser extension

Agents operate directly inside AI tools. Immediate guidance with no changes to existing workflows.

System integration

Deeper integration for organisations that need governance across internal tools and AI workflows.

MCP

Expand agent capabilities across external tools and systems at the infrastructure level.

Velatir

SECURITY & PRIVACY

Data Security & Privacy Overview

EU Sovereign

AI governance built on EU infrastructure, with full data sovereignty and privacy-preserving architecture.

Infrastructure

EU-only hosting
All data processed and stored within the EU. No data leaves EU jurisdiction.

Encryption everywhere
TLS/HTTPS enforced in transit. All stored data encrypted at rest.

Workspace isolation
Strict multi-tenancy. Cross-tenant access is architecturally impossible.

Fail-open design
If Velatir is unreachable, employee workflow is never blocked.

Certifications & Audits

ISO 27001 Certified

CIS Controls v8.1
Self-certification in progress.

SOC 2
Aligned with SOC 2 control framework.

Penetration testing
Independently tested and audited.

Data Handling

Three storage levels
Organizations choose full trace, summarized, or no data stored

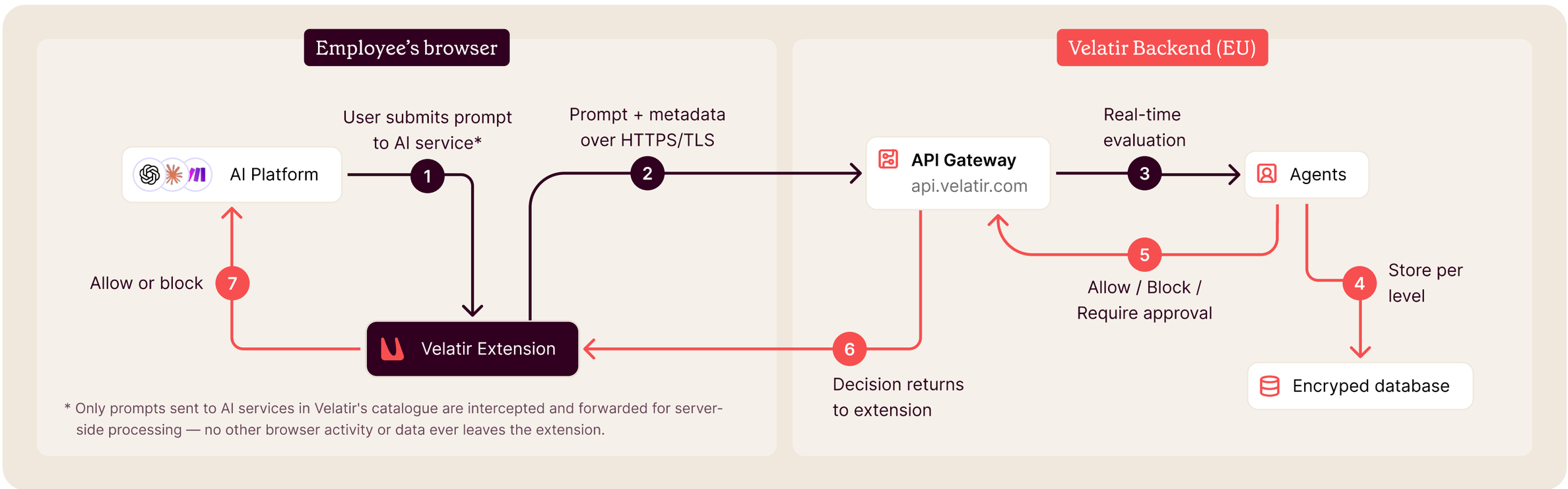
Privacy-preserving
Data sent only to your configured Velatir endpoint

API key security
Keys SHA-256 hashed before storage. Never stored in plaintext.

Monitoring
Continuous vulnerability management, change and configuration controls.

How data flows

From prompt to decision. Every step encrypted, every action governed by your policies.



Three levels of data storage

Your organization controls exactly how much data Velatir retains. Configured at the organization level.

Full Trace Data

Prompt content
Stored (encrypted at rest)

What's recorded
Full input, output, service, model, timestamps, session

Use case
Complete audit trail and compliance reporting

1

Summarized Trace Data

Prompt content
Processed in-flight only, never persisted

What's recorded
Summary and assessment only

Use case
Policy enforcement and usage analytics

2

No Data Stored

Prompt content
Never sent to backend

What's recorded
Service name, direction, timestamp only

Use case
Governance without data rentetion

3

Velatir never collects

Any of the following, from any service

- Browser history, cookies, or credentials
- Data from non-AI websites
- Personal files or downloads
- Any data outside AI platform interactions

Velatir

AI GOVERNANCE PLATFORM

Operational compliance for AI

Velatir gives your organisation the operational foundation to meet EU requirements on AI, data protection, and security. Instead of treating compliance as a separate project, it becomes part of how your team already uses AI.

How it works

1 Map what's in use

Velatir identifies which AI tools and services are active across your organisation.

2 Apply controls

Agents apply data protection, access control, and content standards in AI interactions.

3 Document continuously

Every interaction is logged. An audit trail builds automatically.

What Velatir provides

Four operational capabilities. Each one supports obligations across multiple EU regulations.

Inventory and Visibility

AI Act · GDPR · NIS2

A live overview of which AI tools and services are in use, who uses them, and how. The foundation for risk assessment, processing records, and supply chain oversight.

Data Protection

GDPR · NIS2

Detection of sensitive and personal data before it reaches external AI services. Reduces the risk of accidental transfers and supports lawful data processing.

Access Control

AI Act · NIS2

Gatekeeper agents manage which AI services are available and to whom. Organisational policies are applied at the point of use.

Continuous Documentation

AI Act · GDPR · NIS2

Every AI interaction is recorded. Audit-ready records that support transparency obligations, processing documentation, and incident response.

How this maps to regulations

AI Act

Obligations vary by risk level. For deployers of high-risk AI, requirements include transparency, human oversight, and risk management.

- Inventory and classification support based on use case and risk level
- Human escalation when an interaction requires judgment
- Interaction records for transparency and audit obligations

GDPR

Using AI with personal data creates data protection obligations. Velatir helps meet them in practice.

- Detection of sensitive and personal data before it leaves the organisation
- Visibility into which AI services process what types of data
- Records that support processing documentation under Article 30
- Controls that reduce the risk of unauthorised data transfers

NIS2

Organisations in scope must manage cybersecurity risk across their network and information systems, including third-party AI services.

- Oversight of third-party AI services used by employees
- Access control policies applied through Gatekeeper agents (Art. 21(2)(i))
- Interaction records that support incident detection and response
- Visibility that contributes to supply chain risk management

Deployment

Browser extension

Active inside AI tools from day one. No changes to existing workflows.

System integration

Connects governance to internal tools and AI workflows.

MCP

Extends agent capabilities across tools and systems at infrastructure level.

Velatir

THE TEAM



Michael Blicher Sørensen

CEO

Michael on LinkedIn



Elias Sørensen

CTO

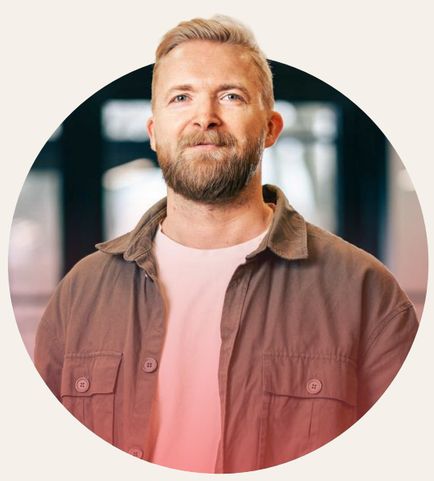
Elias on LinkedIn



Christian Møller

COO

Christian on LinkedIn



Andreas Paulli

CPO

Andreas on LinkedIn

