Datasheet

Veraify AI Security

Veraify gives security teams complete visibility and control over AI usage on every endpoint — discovering every AI tool in use, enforcing policy in real time, and protecting sensitive data before it leaves the device.

AI Usage Visibility

Real-time inventory of every AI app, model, platform and user prompt — sanctioned or not.

AI Audit Logs

Full detailed audit logs for AI usage activity, including user prompts and sensitive data submission to AI tools.

AI Governance

Easy, simple-click based sensitive data protection and prompt injection protection policy enforcement.

Introduction

As enterprises adopt AI in their organizations to improve their productivity, processes and business advantage, IT and Infosec teams require observability, auditing and governance control on AI transformation. Enterprises can't be expected to deploy complex and manual distributed components to gain visibility and control on AI due to limited budgets, time and expertise on the evolving AI technology. The AI Security solution must be simple to deploy, easy to manage and have full control on all modes of AI usage.

Deploys in under a day

> Veraify Promise → Lightweight agent for macOS and Windows. No network changes, no proxy, no user friction.

Customer Use Cases

Enterprises have immediate requirements for the following AI use cases.

Veraify AI Security

1) AI Observability / Shadow AI

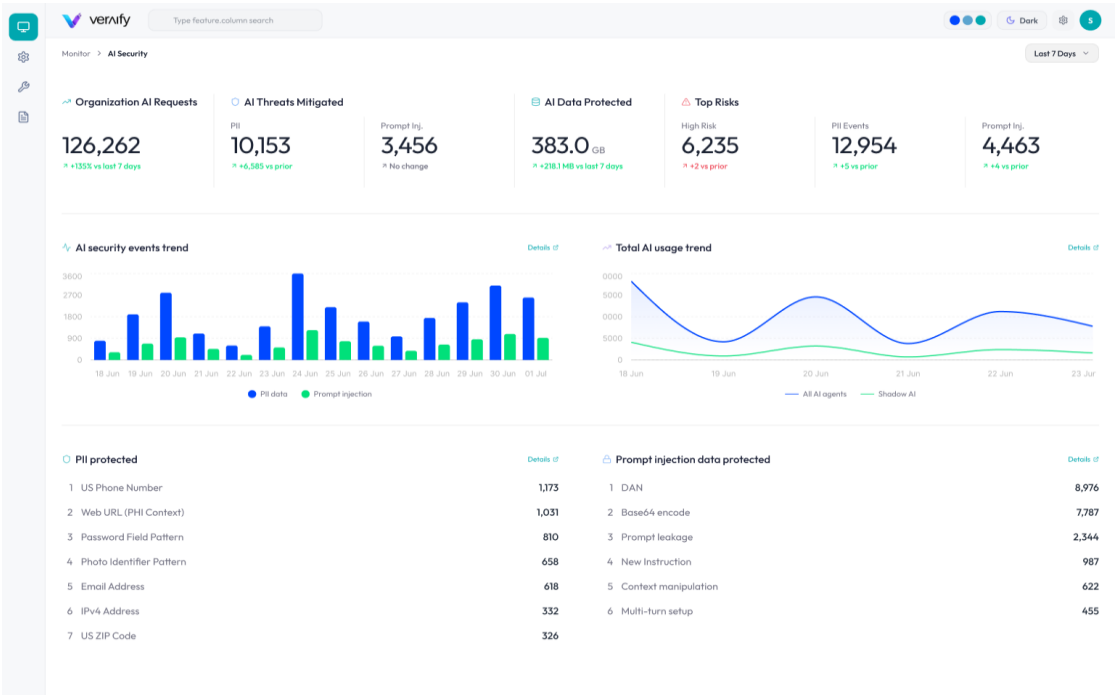
Enterprises need visibility and insights into the AI usage in their organization. Employees, contractors and 3rd party users leverage AI tools for all types of business functions but, Shadow AI poses biggest risk for enterprise. IT and Security teams need to gain insight into the AI usage to mitigate the AI risks.

2) AI Audit Logging

Every enterprise must comply with regulatory compliance requirements. It is critical to have evidence for AI compliance – proof for having visibility and control over AI usage – so that enterprise can be confident that AI risks are mitigated and their customers are well protected. Detailed AI audit logs are required to be submitted as evidence for regulatory compliance.

3) AI Governance

Observability and Insights will lead to controls for the AI usage that is compliant with the enterprise policies. Ability to define control policies in easy and simple steps, minimal ongoing maintenance to cover all forms for AI tools and new AI products will be become critical. AI security is not a one-time define-and-forget configuration; hence ease and simplicity of AI governance is important.



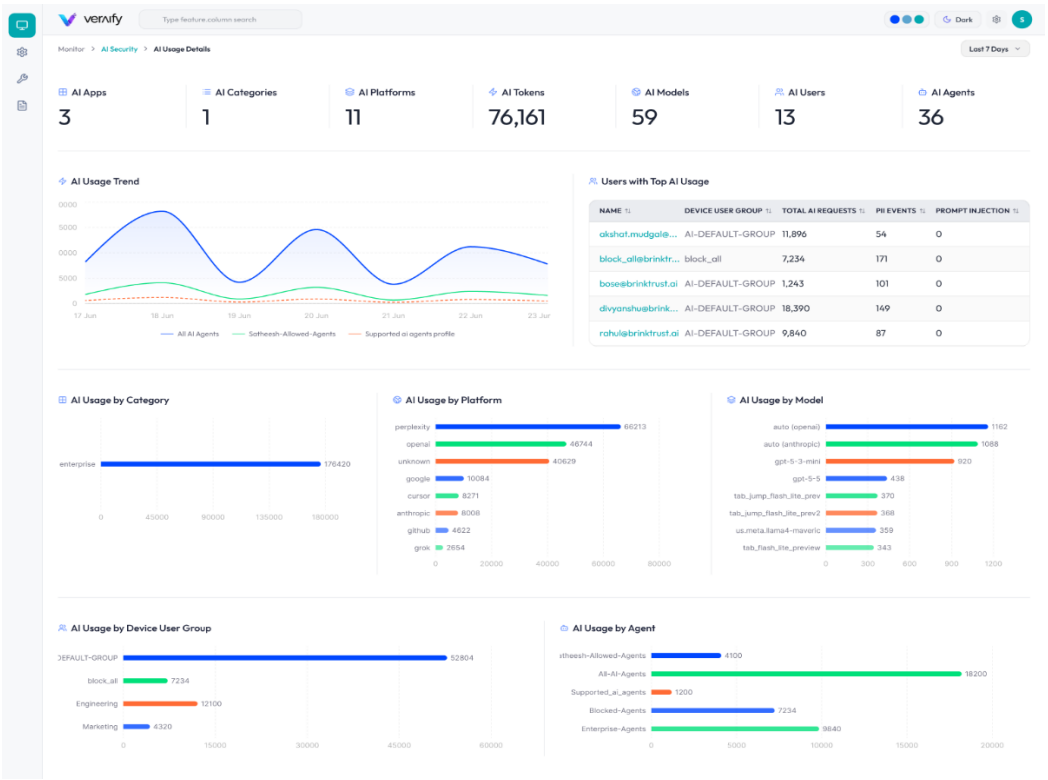
Veraify AI Security

Veraify Capabilities

Veraify, powered by Cloudbrink, is an innovative AI-native platform that caters to the enterprise AI Security needs using the following capabilities.

Capability	Description
Pre-defined AI Tools catalogue	Veraify provides built-in pre-defined catalogue of all AI tools, eliminating the need for IT/Security teams to write complex URL & DLP policies, for which AI Security and Audit policies can be applied
Pre-defined PII catalogue and Prompt Injection attack definitions	Veraify provides built-in pre-defined catalogue of most commonly leaked sensitive data definitions and corresponding actions to be applied, eliminates the need for IT/Security teams to built custom policies
AI Tools support	Unlike browser-based or cloud proxy based approach, Veraify enforces AI policies at the source of AI traffic which is the endpoint. Hence, AI tools consumed in any form – Web, native app, API, CLI/IDE, etc. – are supported by Veraify AI Security
Shadow AI detection	Veraify is capable of dynamically learning all the AI tools and services that users are accessing, without any need for IT/Security teams to write detection policies
Detailed Audit Logging	Veraify provides detailed audit logs for all AI usage activity, including the context sensitive information such as timestamp, user prompt, user role, AI model and tool used, etc.
Log Granularity	Veraify supports controls for log granularity, including full logs, metadata logs, sensitive data hashing logs, or no-logs options
AI Firewalling	Veraify supports both approaches of allowing all AI tools with selective block/redact or blocking all AI tools with selective allow and masking of sensitive data
Role-based AI Security	Veraify supports ability to define AI security policies based on user identity and role
Centralized AI Insights	Veraify provides enterprise-level, role-level and individual user level drill-down of AI usage. This is immensely helpful for IT/Security teams to triage and track any incidents.
Risk Vectors	Veraify provides insights into the top risk sources or vectors to help IT/Security teams to focus on most critical aspects without spending too much time on searching for risk origins

High-performance AI and SASE	Veraify, powered by Cloudbrink, leverages the high-performance globally distributed Edge overlay network infrastructure to deliver high-performance AI tool access along with the SASE functionality
Unified Agent for AI, ZTNA, SWG and QOE	Veraify agent is a unified agent that can be extended to support SASE, SWG and Quality of Experience capabilities



Try Veraify in Minutes

Enterprises looking for effective and easy-to-use AI Security solutions can start their journey with a free subscription of Veraify. Enterprises will quickly gain deep visibility and insights into the AI usage by their users in matter of minutes. Delivered as a software-only solution with no requirements of network or app or AI tool changes, Veraify enables enterprises to adopt AI safely and effectively.

Request a demo

Start a free AI audit → veraify.com/demo