Kaspersky AI Protect

kaspersky bring on the future

Kaspersky AI Protect is the best-in-class solution for detection of AI-borne as well as traditional threats that can be integrated with almost any application.

Kaspersky AI Protect (KAIP) provides comprehensive protection for web portals and applications, proxy servers, network attached storage and mail gateways. It is easy to manage and deploy through HTTP and ICAP as a standalone service, scalable cluster, or Docker container.

Kaspersky AI Protect has new features enabling it to check LLM files and AI agents for malicious functionality

Key Functionality

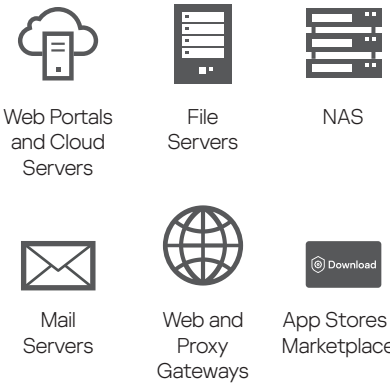
Kaspersky AI Protect can work in Linux environments in one of two modes:

- **REST-like service** that receives HTTP requests from client apps, scans objects passed in these requests, and sends back HTTP responses with scan results.
- **ICAP server** that scans HTTP traffic that passes through a proxy server / NAS / Web Application Firewall / NGFW / any other solutions communicating through ICAP protocol. This integration model also allows scanning the URLs requested by users; web pages with malicious, phishing or adware content are then filtered out.

Kaspersky AI Protect is also available as a Linux Docker container (in HTTP & ICAP mode). It can be deployed as an individual container, to Docker Swarm, to Kubernetes, to AWS EKS, and any similar cloud environments.

Kaspersky AI Protect includes a web-based graphical user interface that allows you to easily configure the product behavior, review its service events, and scan results.

Integration Scenarios



How AI Can Threaten Business Today

LLM Vulnerabilities

- Large Language Model (LLM) files with formats such as .pth, .pt, .pkl, .kers, and .ckpt might contain malicious code
- Execution of malicious functionality of an infected LLM can lead to private data leaks, including passwords and bank card numbers

Rogue AI Agents and Skills

- Malware is often disguised as AI agents
- Over 92,000 malicious attacks disguised as AI services have been detected in H1 2026 by Kaspersky
- Starting from February 2026, OpenClaw Skills activity on the system is scanned by Kaspersky Scan Engine 2.2. Currently, over twenty thousand incidents of malicious OpenClaw skill activity are detected each month.

Security Features for AI Models and AI Agents in Kaspersky AI Protect

LLM Model File Deep Scanning

- Scans model files such as .pth, .pt, .pkl, .kers, and .ckpt to detect malicious code and backdoor injections.

AI Agent Security Detection

- Provides cross-platform malicious detection capabilities for agent skills.
- Detects malicious plugins, preventing devices from being controlled or added to botnets, helping avoid API key leakage, credential theft, sensitive data exfiltration, and malicious command execution risks.

Comprehensive Malware Protection

- Heuristic detection + machine learning, linked to cloud-based threat intelligence for millisecond-level response.
- Deep unpacking, multi-layer packer detection, and intelligent cleanup/remediation.
- Precise filtering of phishing sites and malicious URLs.

Core Advantages

- Cluster-mode horizontal scaling, enabling stress-free scanning of massive files.
- HTTP REST-like / ICAP dual protocols, seamless integration with existing systems.
- Offline updates suitable for physically isolated and weak-network environments.
- Supports security scanning of LLM and Skills files.

Technology Alliances

Kaspersky technologies are offered for integration into third party hardware and software security products and services. All solutions are backed by professional technology partnership support.

Learn more at www.kaspersky.com/oem

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com