SOVEREIGN CYBERSECURITY
made in EUROPE

IKARUS HarfangLab

European Endpoint Security Platform

HarfangLab Guard feat. IKARUS: EDR & EPP & optional ASM in a single agent

TLP:CLEAR

Security Value Drivers

- One of the most performant EDR agents on the market
- 100 % Cyber Technology “Made in Europe”
- EU cloud, on-premises, or air-gapped deployment
- Real-time detection, hunting & response
- Full transparency with open detection rules

HarfangLab Guard feat. **IKARUS** is a comprehensive European endpoint security platform that combines **Endpoint Protection (EPP)**, **Endpoint Detection & Response (EDR)** and optional **Attack Surface Management (ASM)** in a single agent.
Developed and operated in Europe, the solution meets the requirements from mid-sized organizations to large enterprises, government organizations and critical infrastructure operators for effectiveness, transparency and data sovereignty.
Organizations always retain full control over all data collected by HarfangLab Guard feat. IKARUS. An open rule set in standardized formats such as YARA and Sigma enables white-box transparency: security teams can trace and understand alerts and, if needed, adapt the rules accordingly.

EDR: More context, faster response

EDR (Endpoint Detection & Response) makes security-relevant activities on endpoints visible, detects anomalies and attack patterns, and enables rapid response — from investigation to remote incident response. This allows security teams to prioritize incidents, investigate efficiently, and remediate targeted threats.
Combined with the integrated IKARUS Malware Scan Engine, HarfangLab Guard feat. IKARUS reliably blocks malware before execution, reducing the workload on systems and analysts. The platform detects even targeted attacks, correlates anomalies into actionable alerts, and provides full traceability through a white-box approach.

Independetly validated

- » MITRE ATT&CK evaluations 2023 & 2024
- » ANSSI CSPN-certified & ANSSI-qualified
- » BSI-certified (BSI-DSZ-BSZ-0021-2025)

IKARUS Security GmbH | Erdberger Lände 40-48 | Stiege A, Top 6.1 | 1030 Vienna | Austria | Tel: +43 1 589 95-0 | office@ikarus.at | IKARUSsecurity.com
Reg. No. 64708i | Jurisdiction Vienna | VAT ID: ATU15191405 | Erste Bank Österreich | IBAN: AT14 2011 1821 2208 2100 | BIC: GIBAATWWXXX

IKARUS

Three modules in a single lightweight agent

Endpoint Protection (EPP) – powered by IKARUS Malware Scan Engine

Multi-layered malware detection reliably blocks malicious code before execution.

- Real-time malware detection and blocking
- Protection even in offline or air-gapped environments
- Cross-platform malware detection
- Reduced workload for analysts and systems

Endpoint Detection & Response (EDR) – HarfangLab technology

EDR correlates endpoint signals into attack chains and enables fast understanding of real-world attacks – supporting rapid analysis and response.

- Real-time endpoint telemetry (processes, network, events)
- Anomaly detection & attack-chain correlation
- Threat hunting & remote incident response
- Forensic timelines for root-cause analysis
- Threat intelligence enrichment (IOCs, context)
- Agent self-protection against deactivation/tampering

Attack Surface Management (ASM) – optional add-on

ASM provides continuous visibility into real-world attack surfaces supporting pro-active remediation and prioritization.

- CVE and exposure visibility per endpoint
- Detection of shadow IT and unmanaged assets
- Risk prioritization based on context and exploitability
- Agent-based, no additional network scanning required

Typical Use Cases

» Enterprise endpoint protection & response
» SOC-driven threat hunting & incident response
» Regulated, on-prem & air-gapped deployment
» Exposure visibility with optional ASM

IKARUS Security GmbH | Erdberger Lände 40-48 | Stiege A, Top 6.1 | 1030 Vienna | Austria | Tel: +43 1 589 95-0 | office@ikarus.at | IKARUSsecurity.com
Reg. No. 64708i | Jurisdiction Vienna | VAT ID: ATU15191405 | Erste Bank Österreich | IBAN: AT14 2011 1821 2208 2100 | BIC: GIBAATWWXXX

Architecture

HarfangLab Guard feat. IKARUS combines the prevention and isolation of identified threats with in-depth analysis and response capabilities.

The lightweight **agent** continuously scans clients and servers for malware and anomalies. It contains the complete threat detection logic, ensuring local protection remains active even when connectivity is interrupted. In parallel, it collects endpoint telemetry in real time and transfers it transparently to the management console.

Flexible deployment models – consistent feature set

- EU cloud hosting in Austrian and German data centers
- On-premises deployment in your own infrastructure
- Air-gapped / offline-capable for isolated systems
- MDR option via managed service partners

The optional **ASM module** uses the same agent data to make exposures and CVEs visible – without additional infrastructure. The scope of collected data can be defined individually and is always fully transparent.

The **IKARUS Malware Scan Engine** enhances the Endpoint Detection & Response system with high-performance malware prevention: threats are detected immediately – regardless of the platform they were written for – and blocked before execution. This reduces the workload on the EDR system and security analysts and eliminates the need for an additional antivirus client.

Through the **management console**, security teams configure policies, investigate incidents, and initiate remote response actions. Real-time alerts can be handled across affected endpoints simultaneously or responses can be automated. Graphical process and event views support forensics and root-cause analysis.

Lightweight, efficient, and scalable

For high performance and stability, the EDR agent is developed in Rust. Combined with the IKARUS Malware Scan Engine, which is designed for speed and reliability, HarfangLab Guard feat. IKARUS delivers an exceptionally efficient and scalable system. The capacity of an instance or database can be increased without service interruption.
Agent installation does not require a reboot, allowing administrators to expand and adapt the environment easily.

Integration into existing SOC workflows

- Connectors for SIEM / SOAR / NDR / Threat Intelligence as well as file analysis environments
- API-enabled / API-ready (automatable and extensible for custom use cases)

IKARUS Security GmbH | Erdberger Lände 40-48 | Stiege A, Top 6.1 | 1030 Vienna | Austria | Tel: +43 1 589 95-0 | office@ikarus.at | IKARUSsecurity.com
Reg. No. 64708i | Jurisdiction Vienna | VAT ID: ATU15191405 | Erste Bank Österreich | IBAN: AT14 2011 1821 2208 2100 | BIC: GIBAATWWXXX

Key features

Detection & Prevention

Multi-layered malware detection reliably blocks malicious code before execution.

- **Detect and block threats – even offline:** The IKARUS Malware Scan Engine combined with IOC/anomaly detection brings strong prevention together with EDR context. Detection logic in the agent ensures protection even when connectivity is interrupted. An open rule set makes alerts traceable.
- **Self-protection and tamper resistance:** Protection against uninstallation, deactivation and manipulation; bypass attempts are detected and reported. Console–agent communication is encrypted and certificate-based.
- **Attack Surface Management (ASM) – optional:** Visibility into exposures and vulnerabilities per endpoint, including unmanaged assets and prioritization based on context/exploitability. Uses agent telemetry – no additional network scans required.

Investigation, Threat Hunting & Incident Response

- **Investigate and remediate incidents:** Qualify alerts, trace attack paths and perform threat hunting. Isolate endpoints, download files, stop processes/tasks/services and remediate affected systems.
- **Visual incident analysis (timelines):** Timelines with processes, network connections, event logs and alerts; investigation and remediation actions can be initiated directly from the view.
- **Telemetry for real-time investigations:** Live or event-driven (e.g., on alerts) to support investigations and IOC research. Scope and granularity are policy-controlled.

Operations, Integrations & Control

- **Granular security management:** Whitelist/exception management reduces false positives; dashboards, reports and preconfigured views for alerts, telemetry, analysis and threat hunting.
- **Threat intelligence integration:** Integration of YARA/SIGMA rules and IOCs; feeds via upload/API, connectors (e.g., MISP) or SOAR/playbooks.
- **SIEM/SOAR & interoperability:** Integration into existing SOC workflows via connectors and interfaces; telemetry can be used for custom analytics and use cases.

Supported platforms

» Windows » Linux » macOS

IKARUS Security GmbH | Erdberger Lände 40-48 | Stiege A, Top 6.1 | 1030 Vienna | Austria | Tel: +43 1 589 95-0 | office@ikarus.at | IKARUSsecurity.com
Reg. No. 64708i | Jurisdiction Vienna | VAT ID: ATU15191405 | Erste Bank Österreich | IBAN: AT14 2011 1821 2208 2100 | BIC: GIBAATWWXXX

Contact & further information:

IKARUS Security GmbH
Phone: +43 1 58995-500
Email: sales@ikarus.at

About IKARUS

IKARUS Security is an independent European cybersecurity company with proprietary malware detection technology and threat intelligence, IT and OT security solutions, and cybersecurity services. Since 1986, IKARUS has protected enterprises, public authorities and critical infrastructure with technology-driven solutions and operational expertise.

About HarfangLab

HarfangLab is a French cybersecurity company specializing in powerful Endpoint and Detection technologies. HarfangLab was the first EDR to be certified by ANSSI, and today boasts a large number of customers, including administrations, companies and international organizations operating in highly sensitive sectors. solutions are characterized by their openness and seamless integration with other security components, their transparency through the accessibility of the processed data and their strategic autonomy through the choice of hosting - cloud or own infrastructure.