IKARUS

HarfangLab



HarfangLab Guard feat. IKARUS

Endpoint Protection, Detection and Response system developed and operated in Europe

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 of mid-sized to large enterprises, government organizations and critical infrastructure operators for effectiveness, transparency and data sovereignty.

Supported platforms

- ✓ Windows
- ✓ Linux
- ✓ macOS

Unique transparency, security 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.

Independently validated

- ✓ **MITRE ATT&CK** Evaluations 2023 & 2024
- ✓ **ANSSI** CSPN-certified & ANSSI-qualified
- ✓ **BSI**-certified (BSI-DSZ-BSZ-0021-2025)

© IKARUS Security GmbH. All rights reserved. TLP:GREEN

Prevention, Response and Attack Surface Management

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 before damage occurs
- ✓ 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 and helps reduce risk before vulnerabilities are exploited – without additional infrastructure or network scans.

- ✓ 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

© IKARUS Security GmbH. All rights reserved. TLP:GREEN

Architecture

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

The **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. It also collects and transfers telemetry data to the management console in real time. The optional ASM module uses the same telemetry to make exposures and CVEs visible – without additional infrastructure. The scope of collected data can be defined individually and is always fully transparent.

Flexible deployment models – consistent feature set

- ✓ **EU cloud hosting** in data centers in Austria/Europe
- ✓ **On-premises deployment** in your own infrastructure
- ✓ **Air-gapped / offline-capable** for isolated systems
- ✓ **MDR option** via managed service partners

The **IKARUS Malware Scan Engine** enhances the Endpoint Detection & Response system with the strengths of a high-performance antivirus layer: malware is detected immediately—regardless of the platform it was written for – and blocked before execution. This reduces the workload on the EDR system and security analysts, making an additional antivirus client unnecessary.

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

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)

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.

© IKARUS Security GmbH. All rights reserved. TLP:GREEN

Key features

Detection & Prevention

- ✓ **Detect and block known and unknown threats:** 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.

© IKARUS Security GmbH. All rights reserved. TLP:GREEN

Request personal consultation, a live-demo, or a PoV:

IKARUS Security GmbH

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

About IKARUS

IKARUS Security has been developing and operating leading cyber security solutions since 1986. The company‘s own developments focus on the renowned IKARUS Malware Scan Engine, efficient cloud solutions and the protection of critical infrastructures. Together with selected technology partners, IKARUS offers additional security services for companies of all sizes and industries as well as for critical infrastructures. These range from the modular IKARUS Threat Intelligence Platform with local and international CTI, through Incident Response Services and dvanced Threat Protection, to the integration of innovative OT security sensors.

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 characterised 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.

© IKARUS Security GmbH. All rights reserved. TLP:GREEN