IKARUS security software

HarfangLab


**HarfangLab Guard feat. IKARUS**

# Endpoint Protection, Detection and Response-System made in Europe

The increasing complexity of modern attacks is pushing the limits of pure antivirus software. EDR capabilities extend protection by placing the often subtly interlocking steps of an attack chain in a temporal and contextual context. This enables targeted threats to be identified and blocked more quickly.

While antivirus software can detect and block malicious code in milliseconds, endpoint detection and response (EDR) systems aim to visualise endpoint activity and report possible signs of an attack. They collect telemetry data from clients and servers, identify anomalies and uncover patterns or correlations in processes that may indicate security breaches. At the same time, they provide security analysts with tools to directly access devices and systems, analyse processes and defend against attacks.

## European EDR & EPP solution for critical infrastructure, government and enterprise

- ✓ **Defence** against new and known threats
- ✓ Comprehensive **visibility** via end devices (incl. app inventory)
- ✓ Automated **real-time responses** to security incidents

HarfangLab Guard feat. IKARUS is a comprehensive EDR and EPP-System, developed by cybersecurity companies HarfangLab from France and IKARUS Security Software from Austria. By combining their best technologies, the companies are creating a strong European system that can compete with the features and detection capabilities of the international market leaders, while preserving European cyber sovereignty.

HarfangLab Guard feat. IKARUS It even identifies targeted attacks, alerts on anomalies, detects attack patterns and blocks malware in real time. Your IT team can focus on the security incidents that really matter - and respond immediately from the management console.

## Unrivalled transparency, security and data sovereignty

**DEPLOYMENT**

- ✓ **Cloud hosting** in the data centre in Austria/Europe
- ✓ **On-premises deployment** with full features and performance
- ✓ **MDR option** (Managed Detection & Response) via IKARUS partner

HarfangLab Guard feat. IKARUS is developed and hosted 100% in Europe. The focus of data processing is on the needs of European organisations and critical infrastructures.

At all times, organisations retain full control over all the data that is collected by HarfangLab Guard feat. IKARUS. Another unique feature is the open view of EDR rules and regulations, allowing security analysts to not only see alarms, but to track and understand them.

## EPP and EDR in one central interface

HarfangLab Guard feat. IKARUS consists of an agent that is installed on clients or servers, a central management console and the integrated IKARUS Malware Scan Engine. Thus, the solution combines in-depth analysis and response options with powerful malware detection and the ability to block and isolate detected threats.

» The **agent** scans your clients and servers for malware and anomalies. It contains all the threat detection logic so that local protection is maintained even if the connection is lost. The agent also collects real-time telemetry and sends it to the management console. The amount of data collected can be customised and viewed at any time.

» The **IKARUS Malware Scan Engine** extends the Endpoint Detection and Response features with the benefits of a powerful antivirus solution: Malware is instantly detected and blocked before execution, regardless of the platform it is written for. This preserves and focuses the resources of the EDR system and security analysts. There is no need for a separate antivirus client.

» The **management console** allows security teams to customise security settings, investigate incidents and respond immediately. Real-time alerts can be processed simultaneously across all affected endpoints or responses can be automated. The graphical representation of events and processes makes it easier to reconstruct and analyse security incidents.

The EDR agents were developed in the RUST programming language to optimise performance and stability. Combined with the IKARUS Malware Scan Engine, designed for speed and reliability, HarfangLab Guard feat. IKARUS is an extraordinarily efficient, scalable system.

The capacity of an instance or database can be easily increased without service interruption. Agent installation does not require a reboot, allowing administrators to easily expand and adapt the network.

## Main features

- ✓ **Detect and block known and unknown threats:** Through the integration of the IKARUS Malware Scan Engine and the detection of IOCs and anomalies, HarfangLab Guard feat. IKARUS offers comprehensive endpoint protection, that combines the benefits of a strong antivirus solution with endpoint and detection features. With all detection logic on the endpoint agent, your devices and servers are protected even when disconnected. The open ruleset allows IT security analysts to understand what events triggered an alert.
- ✓ **Investigate and remediate security incidents:** Security teams are given all the tools and information they need to qualify and track alerts and launch threat hunting campaigns to stop targeted attacks in their tracks. Endpoints can be quarantined individually or collectively, files downloaded, processes, scheduled tasks or services stopped based on specific criteria, and files or the registry cleaned of infections. A threat is displayed with its criticality, the number of security events per agent and a view of the MITRE ATT&CK matrix.
- ✓ **Comprehensive telemetry data of the end devices:** Telemetry data can be transmitted continuously (‚live') or based on alerts to enable real-time investigation and search for indicators. The amount of telemetry transmitted can also be customised and granularly set via policies.
- ✓ **Graphical view of security events or processes:** For each security incident, a timeline is created that lists all relevant telemetry data and, for endpoints, all processes started, network connections, event logs and alerts, so that analysis can begin immediately. The full context of the incident or individual process steps can be viewed. Actions for investigation or remediation can be accessed directly from the graph.
- ✓ **Customised security management:** A detailed whitelist management system allows you to define exceptions to detection rules or heuristics based on specific criteria, reducing false positives. Dashboards that generate specific reports based on security events, binary or driver metadata, investigation results, telemetry data or agent event logs can also be used to customise views in the management portal. Pre-configured dashboards are available for alerts, all telemetry, analysis and threat hunting.
- ✓ **Threat Intelligence integration:** HarfangLab Guard feat. IKARUS uses signature-based malware detection, YARA and SIGMA rules, driver IOCs, artificial intelligence and behaviour-based detection. Additional threat intelligence feeds can be integrated through uploads (manually or via API), rule creation, via the MISP connector or via playbooks via SOARs. The IKARUS TIP has a dedicated interface for quick and easy integration.

## ADDITIONAL CUSTOMER BENEFITS

- ✓ **Open ruleset** so that alarms can not only be seen, but also understood
- ✓ Tool for **threat hunting** and in-depth analysis
- ✓ Integration with **SIEM/SOAR** and Threat Intelligence
- ✓ **On-Premises deployment** with full functionality and performance
- ✓ **Efficient, fast** and compatible with Windows, Linux, and MacOS
- ✓ Personal **German-speaking and local support** from IKARUS and Managed Service Partners

## Information and professional advice:

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

## Independent tests by MITRE ATT&CK Evaluations

The MITRE ATT&CK Evaluations test the effectiveness of various solutions using realistic attack scenarios. They confirm HarfangLab's strong performance both in detecting individual attack steps and in protecting by blocking the threats.

MITRE ATT&CK Evaluations Enterprise 2024
MIRTE ATT&CK Evaluations Enterprise 2023 - Turla

## About IKARUS

IKARUS Security Software 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.

we provide security

www.IKARUSsecurity.com

**IKARUS Sales Team** | sales@ikarus.at | +43 1 589 95-500
**IKARUS Support Team** | support@ikarus.at | +43 1 589 95-400