

HarfangLab Guard feat. IKARUS

Endpoint Protection, Detection and Response-System entwickelt und gehostet in Europa

HarfangLab Guard feat. IKARUS ist eine umfassende europäische Endpoint-Security-Plattform, die Endpoint Protection (EPP), Endpoint Detection & Response (EDR) und optional Attack Surface Management (ASM) in einem einzigen Agenten vereint. Entwickelt und betrieben in Europa, erfüllt die Lösung Anforderungen von mittleren bis großen Unternehmen, Behörden und kritischen Infrastrukturen an Wirksamkeit, Transparenz und Datenhoheit.

Unterstützte Systeme

- ✓ Windows
- ✓ Linux
- ✓ macOS

Einzigartige Transparenz, Sicherheit und Daten-Souveränität

Organisationen behalten jederzeit die vollständige Kontrolle über alle Daten, die von HarfangLab Guard feat. IKARUS erhoben werden. Ein offenes Regelwerk in standardisierten Formaten wie YARA und Sigma schafft Whitebox-Transparenz: Security-Teams können Alarme nachvollziehen, verstehen und bei Bedarf anpassen.

EDR: Mehr Kontext, schnellere Reaktion

EDR (Endpoint Detection & Response) macht sicherheitsrelevante Aktivitäten auf Endpoints sichtbar, erkennt Anomalien und Angriffsmuster und ermöglicht schnelle Reaktionen – von der Analyse bis zur Remote-Incident-Response. Dadurch können Security-Teams Vorfälle priorisieren, effizient untersuchen und gezielt beheben.

In Kombination mit der integrierten IKARUS Malware Scan Engine blockiert HarfangLab Guard feat. IKARUS Malware zuverlässig bereits vor der Ausführung – und entlastet damit Systeme und Analyst:innen. Die Plattform erkennt selbst gezielte Angriffe, korreliert Anomalien zu belastbaren Alerts und bietet vollständige Nachvollziehbarkeit (Whitebox-Ansatz).

Unabhängig validiert

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

Deutsches IT-Sicherheitszertifikat
Zertifikatsnummer: BSI-DSZ-BSZ-0021-2025
Gültig bis: 07.12.2027
Updates bis: 07.12.2027

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

Prävention, Reaktion und Angriffsflächen-Management

Drei Module in einem schlanken Agenten

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

Mehrschichtige Malware-Erkennung blockiert Schadcode zuverlässig vor der Ausführung.

- ✓ Echtzeit-Erkennung von Malware, bevor Schaden entsteht
- ✓ Schutz auch in Offline- oder Air-gapped-Umgebungen
- ✓ Plattformübergreifende Malware-Erkennung
- ✓ Entlastung von Analysten und Systemen

Endpoint Detection & Response (EDR) – HarfangLab Technologie

EDR korreliert Endpoint-Signale zu Angriffsketten und ermöglicht schnelles Verständnis realer Angriffe – für schnelle Analysen und Reaktionen.

- ✓ Echtzeit Endpoint-Telemetrie (Prozesse, Netzwerk, Events)
- ✓ Anomalieerkennung & Attack-Chain Correlation
- ✓ Threat Hunting & Remote Incident Response
- ✓ Forensik-Timelines für Root-Cause-Analyse
- ✓ Threat-Intelligence-Enrichment (IOCs, Kontext)
- ✓ Agent Self-Protection gegen Deaktivierung/Manipulation

Attack Surface Management (ASM) – optionales Add-on

ASM schafft kontinuierliche Transparenz über reale Angriffsflächen und reduziert damit Risiken, bevor sie ausgenutzt werden – ohne zusätzliche Infrastruktur oder Netzwerk-Scans.

- ✓ CVE- & Exposure-Sicht pro Endpoint
- ✓ Erkennung von Shadow-IT & ungemanagten Assets
- ✓ Risiko-Priorisierung nach Kontext & Exploitability
- ✓ Agent-basiert, keine zusätzlichen Netzwerk-Scans

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

Architektur

HarfangLab Guard feat. IKARUS vereint die Abwehr und Isolation erkannter Bedrohungen mit tiefreichenden Analyse- und Reaktionsmöglichkeiten.

Der **Agent** untersucht Clients und Server auf Malware und Anomalien. Er enthält die gesamte Logik für die Bedrohungserkennung, sodass der lokale Schutz auch bei getrennter Verbindung aufrecht bleibt. Außerdem sammelt und überträgt er Telemetriedaten in Echtzeit an die Management-Konsole. Das optionale ASM nutzt dieselbe Telemetrie, um Exposures und CVEs sichtbar zu machen – ohne zusätzliche Infrastruktur. Der Umfang der gesammelten Daten kann individuell festgelegt und jederzeit eingesehen werden.

Flexible Betriebsmodelle – einheitlicher Funktionsumfang

- ✓ **EU-Cloud-Hosting** im Rechenzentrum in Österreich/Europa
- ✓ **On-Premises-Deployment** in Ihrer eigenen Infrastruktur
- ✓ **Air-gapped / offline-fähig** für isolierte Systeme
- ✓ **MDR-Option** Managed-Service-Partner

Die **IKARUS Malware Scan Engine** erweitert die Funktionen des Endpoint Detection and Response Systems um die Vorteile einer leistungsstarken Antiviren-Lösung: Malware wird, unabhängig von der Plattform, für die sie geschrieben wurde, sofort erkannt und noch vor ihrer Ausführung geblockt. Damit werden die Ressourcen des EDR-Systems und der Security-Analysten geschont und fokussiert. Ein zusätzlicher Antiviren-Client ist überflüssig.

Über die **Management-Konsole** konfigurieren Security-Teams Policies, untersuchen Vorfälle und leiten Remote-Response-Maßnahmen ein. Echtzeit-Warnungen können über alle betroffenen Endpunkte gleichzeitig bearbeitet oder Reaktionen automatisiert werden. Grafische Prozess- und Event-Ansichten unterstützen Forensik und Root-Cause-Analysen.

Schlank, effizient und skalierbar

Integration in bestehende SOC-Workflows

- ✓ **Konnektoren zu SIEM / SOAR / NDR / Threat Intelligence** sowie File-Analysis-Umgebungen
- ✓ **API-fähig / API-ready** (automatisierbar und anschlussfähig für eigene Use-Cases)

Für hohe Performance und Stabilität wurde der EDR-Agent in Rust entwickelt. Zusammen mit der IKARUS Malware Scan Engine, die mit Fokus auf Schnelligkeit und Verlässlichkeit entwickelt wurde, stellt HarfangLab Guard feat. IKARUS ein außerordentlich effizientes, skalierbares System dar. Die Kapazität einer Instanz oder einer Datenbank kann ohne Serviceunterbrechung erhöht werden. Auch die Installation von Agenten erfordert keinen Neustart, sodass Administratoren das Netzwerk unkompliziert erweitern und anpassen können.

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

Hauptmerkmale

Detection & Prävention

- ✓ **Bekannte und unbekannte Bedrohungen erkennen und blockieren:** IKARUS Malware Scan Engine plus IOC-/Anomalie-Erkennung verbindet starke Prävention mit EDR-Kontext. Detection-Logik im Agenten schützt auch bei unterbrochener Verbindung. Offenes Regelwerk macht Alerts nachvollziehbar
- ✓ **Selbstschutz und Manipulationsschutz:** Schutz vor Deinstallation, Deaktivierung und Manipulation; Umgehungsversuche werden erkannt und gemeldet. Konsole–Agent-Kommunikation ist verschlüsselt und zertifikatsbasiert.
- ✓ **Attack Surface Management (ASM) – optional:** Sicht auf Exposures und Schwachstellen pro Endpoint, inkl. ungemanagter Assets und Priorisierung nach Kontext/Exploitability. Nutzt Agent-Telemetrie – keine zusätzlichen Netzwerk-Scans erforderlich.

Investigation, Threat Hunting & Incident Response

- ✓ **Sicherheitsvorfälle untersuchen und beheben:** Alerts qualifizieren, Angriffspfade nachvollziehen und Threat Hunting durchführen. Endpoints isolieren, Dateien herunterladen, Prozesse/Tasks/Services stoppen und Systeme bereinigen.
- ✓ **Grafische Vorfallanalyse (Timelines):** Timelines mit Prozessen, Netzwerkverbindungen, Event Logs und Warnungen; Maßnahmen zur Untersuchung und Behebung direkt aus der Ansicht.
- ✓ **Telemetrie für Echtzeit-Ermittlungen:** Live oder anlassbezogen (z. B. bei Alerts) für Untersuchungen und IOC-Suche. Umfang und Granularität policy-basiert steuerbar.

Betrieb, Integrationen & Kontrolle

- ✓ **Individuelles Sicherheitsmanagement:** Whitelist-/Exception-Management reduziert False Positives; Dashboards, Reports und vorkonfigurierte Views für Alarme, Telemetrie, Analysen und Threat Hunting.
- ✓ **Threat-Intelligence-Integration:** Einbindung von YARA-/SIGMA-Regeln und IOCs; Feeds via Upload/API, Konnektoren (z. B. MISP) oder SOAR/Playbooks.
- ✓ **SIEM/SOAR & Interoperabilität:** Integration in bestehende SOC-Workflows über Konnektoren und Schnittstellen; Telemetrie kann für eigene Analytics und Use-Cases genutzt werden.

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

Persönliche Beratung, Live-Demo oder PoV anfragen:

IKARUS Security GmbH

Tel.: +43 1 58995-500
E-Mail: sales@ikarus.at

Über IKARUS

IKARUS Security entwickelt und betreibt seit 1986 führende Cybersicherheitslösungen. Die Eigenentwicklungen des Unternehmens konzentrieren sich auf die anerkannte IKARUS Malware Scan Engine, effiziente Cloud-Lösungen sowie den Schutz kritischer Infrastrukturen. Gemeinsam mit ausgewählten Technologiepartnern bietet IKARUS neben den Kerntechnologien eine breite Palette an Sicherheitsdienstleistungen für Unternehmen aller Größen und Branchen sowie für kritische Infrastrukturen an. Diese reichen von der modularen IKARUS Threat Intelligence Platform, die lokale und internationale Bedrohungsinformationen aggregiert und verarbeitet, über Incident Response Services und Advanced Threat Protection bis hin zur Integration innovativer OT Security Sensoren.

Über HarfangLab

HarfangLab ist ein französisches Cybersecurity-Unternehmen, das auf EDR-Technologien spezialisiert ist, die Cyberangriffe erkennen, neutralisieren und ein besseres Verständnis der IT-Infrastruktur ermöglichen. HarfangLab war das erste EDR, das von der französischen Behörde für Cybersicherheit ANSSI zertifiziert wurde, und verfügt heute über zahlreiche Kunden, darunter Verwaltungen, Unternehmen und internationale Organisationen, die in hochsensiblen Bereichen tätig sind. HarfangLabs Lösungen zeichnen sich durch ihre Offenheit und ihre nahtlose Integration mit anderen Sicherheitskomponenten, ihre Transparenz durch die Zugänglichkeit der verarbeiteten Daten und die strategische Autonomie durch die Wahl des Hostings – Cloud oder eigene Infrastruktur – aus.

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