

ZAŘÍZENÍ PRO NIS2 & ZKB COMPLIANCE

XRENN™ EdgeGuardian NIS2

rEvoluční AI strážce sítě

Lokální AI zařízení pro monitoring sítě, detekci incidentů a auditní reporting pro NÚKIB. Veškerá analýza probíhá na hraně vaší sítě — **100 % offline, bez cloudu, bez odesílání dat.**

100 % OFFLINE

100 % COMPLIANCE

ZERO CLOUD

MADE IN CZECH REPUBLIC (EU)

AI AUTONOMY (LLM + RAG)

**28.900 Kč**

Garance ceny bez DPH do konce roku 2026 (od 2027: 48.900 Kč)

< 48 h

Auditní report na stůl od zapojení

ISO 27001

ČSN ISO/IEC 27001:2023 — certifikovaný výrobce XRENN Labs s.r.o.

Proč právě offline zařízení

Povinnost, která už platí

Směrnice **NIS2 (EU 2022/2555)** a zákon **264/2025 Sb. (ZKB)** vyžadují průkaznou evidenci technických a organizačních opatření, hlášení incidentů a doložitelnou auditní stopu. Rok 2026 je kritický pro kontroly NÚKIB.

EdgeGuardian tuto evidenci vytváří automaticky — bez konzultantských hodin a bez ručního sběru podkladů.

Proč ne cloudové SIEM

- ✓ Vaše síťová data nikdy neopustí budovu — žádný přenos k třetí straně
- ✓ Žádná závislost na konektivitě, žádné měsíční poplatky za objem dat
- ✓ GDPR compliant, DPA součástí smlouvy, automatické maskování PII
- ✓ Volitelný režim Striktně OFFLINE — vzdálená správa (XSC) jen na vaše rozhodnutí

NASAZENÍ

Tři kroky k NIS2 compliance

01

Bleskové zapojení

Připojení k mirror portu switchu (SPAN/Mirror). Pasivní metoda — nulové riziko pro stabilitu sítě a nulová latence provozu.

02

Lokální AI analýza

Během pár minut vidíte „Síťový příběh“ v češtině. Systém lidsky vysvětlí, proč zablokoval tiskárnu nebo proč se kamera pokouší komunikovat do zahraničí.

03

Export reportů

PDF report s technickým i manažerským shrnutím, kryptograficky podepsaný (HMAC-SHA256) a připravený k doložení orgánům NÚKIB.

FUNKCE

Co zařízení dělá

Absolutní soukromí

Edge LLM + RAG bez odchodích dat. Lokální model, API i znalosti o vaší síti.

AI Defense 1.0

Detekce úniků firemních dat do veřejných AI, hrozby typu WormGPT a FraudGPT, ochrana proti Jailbreak / Prompt Injection.

Inventarizace zařízení

Fingerprinting všech aktiv, CVE mapování a risk scoring.

Real-time monitoring

Anomálie, DNS exfiltrace, brute-force útoky a neobvyklý provoz v reálném čase.

Honeypot Network

Volitelné kontejnery RTSP/Telnet/Modbus pro včasnou detekci průniků.

Klid pro management

Důkazy pro auditora dříve, než o ně požádá. Buďte připraveni, nikoli překvapeni.

Reporting pro NÚKIB

Co report obsahuje

- ✓ Technické shrnutí incidentů a zjištění za sledované období
- ✓ Manažerské shrnutí v češtině, čitelné pro netechnický management
- ✓ Citace konkrétních článků NIS2 / ZKB 264/2025 Sb. přímo v analýze
- ✓ Evidence technických a organizačních opatření
- ✓ NÚKIB-ready draft hlášení incidentu
- ✓ Podpis HMAC-SHA256 (SHA-2 origin) — doložitelná integrita exportu

GET /api/v1/compliance/reports/verify

```
{
  "status": "verified",
  "report_id": "audit-20260205-164619",
  "hash": "23fb7831...5f64588",
  "generated_at": "2026-02-05T16:46:19",
  "type": "audit",
  "reason": "The report is verified."
}
```

Ověření podpisu reportu je součástí API — auditor si integritu doloží kdykoliv.

API & integrace do SOC

- ✓ FastAPI & OpenAPI 3.0.1 (Swagger / Redoc)
- ✓ 54 endpointů, real-time webhooks pro incidenty
- ✓ Export auditních logů v CSV / JSON
- ✓ 2FA autentikace pro všechny uživatele
- ✓ Integrace do stávajících SIEM / SOAR nástrojů

GET /api/v1/monitoring/incidents

```
[{
  "id": 12,
  "title": "[NIS2] Possible Network Mapper Activity",
  "severity": "medium",
  "src_ip": "192.168.0.107",
  "source": "Suricata",
  "active": true
}]
```



Certifikovaný výrobce

XRENN Labs s.r.o. je držitelem certifikace **ČSN ISO/IEC 27001:2023** pro systém řízení bezpečnosti informací. Vývoj, výroba i podpora probíhají v České republice (EU).

< 30 s

Průměrná doba vysvětlení incidentu

> 90 %

Přesnost fingerprintingu zařízení

< 5 %

Míra halucinací LLM v RAGu

Cena a garance do konce roku 2026

STARTOVNÍ EDICE 2026 · SKLADEM

OD 1. 1. 2027

28.900 Kč bez DPH~~48.900 Kč bez DPH~~

Jednorázová investice do hardwaru s předinstalovaným softwarem a proprietární licencí. **Cena je garantována do 31. 12. 2026**; od roku 2027 činí cena 48.900 Kč bez DPH. Základní monitorovací a NIS2 funkce jsou bez měsíčních poplatků — filozofie nízkého TCO.

Technická specifikace

MASTER CPU	Raspberry Pi 5 (8 GB RAM), 4× Cortex-A76 @ 2.4 GHz
AI AKCELERACE	Vlastní TPU + eBPF Kernel Engine, offline LLM a hybridní RAG bez API
STORAGE	512 GB MicroSD Samsung EVO Plus
TERMOMANAGEMENT	Aktivní chlazení + pasivní hliníkový blok
EKO PROVOZ	Spotřeba 5 až 8 W/h — ideální pro provoz 24/7/365
BALENÍ	EdgeGuardian NIS2, napájecí adaptér, ethernet kabel, digitální dokumentace

Volitelná podpora & SLA

BASIC

- ✓ Měsíční aktualizace Suricata IDS/IPS signatur a patching OS
- ✓ Aktualizace reportovacích šablon dle NÚKIB a NIS2
- ✓ OpenAPI dokumentace a integrační manuály SIEM/SOAR

PRO

- ✓ AI Model Evolution — upgrade lokálního LLM a optimalizace RAG
- ✓ Hardware NBD Swap — náhradní zařízení Next Business Day
- ✓ Expert SOC Assistance — konzultace s L3 inženýry, podpora auditu

Pro kritickou infrastrukturu nabízíme zakázkové SLA 24/7/365 s reakcí do 4 hodin.

Přípravení na NIS2 compliance?

Auditní report do 48 hodin od zapojení. Bez závazků, bez cloudu, bez skrytých poplatků. Objednávka a technická konzultace: **xrenn.cz** · **xrenn.store** · **xrenn@xrenn.ai**

[Přejít do e-shopu →](#)

XRENN™ EdgeGuardian NIS2 je nástroj pro splnění technických a organizačních opatření dle NIS2/ZKB (264/2025 Sb.). Konečné posouzení souladu provádí provozovatel a auditorské orgány. Ceny jsou uvedeny bez DPH. Cenová garance 28.900 Kč bez DPH platí do 31. 12. 2026.