WEB SHIELD AI

Merchant content monitoring and underwriting for acquiring banks

Automated screening of merchant websites for prohibited content (Mastercard BRAM / Visa GBPP), transaction laundering controls and in-depth due diligence of high-risk merchants.

SaaS · ru / be / en · deterministic layer + AI

3
modules: Monitoring · InvestiGate · Onboarding

51
underwriting risk indicators

24/7
scheduled website crawling

ArtCloud LLC · Minsk, Belarus · shield.by

About the product

An acquiring bank is accountable to Visa and Mastercard for its merchants: their websites must not sell prohibited goods or services. Web Shield AI performs this control automatically — it crawls merchant websites around the clock, detects violations, captures evidence and helps the compliance officer make decisions, replacing manual monitoring and reducing the bank's regulatory and reputational risks.

Three modules

1. Monitoring — content monitoring

Scheduled crawling of merchant websites and detection of prohibited content with ru/be/en morphology and anti-obfuscation; AI classification and semantic detection (Premium); immutable evidence.

2. InvestiGate — underwriting and due diligence

In-depth screening of high-risk merchants: a case file with 51 risk indicators, a dynamic risk score, CREM, transaction laundering controls, PDF report.

3. Onboarding — application intake

Applications intake (manual, CSV, API, public form) → merchant profile and an underwriting case.

Two-stage analysis — the cost invariant

The inexpensive deterministic pass (Aho-Corasick + morphology) runs on every tier and every page. The expensive AI layer (LLM classification, semantic search, vision) runs only on the candidates produced by the first layer and only on Premium — heavy models never scan every page, so the economics stay under control.

01 Monitoring — content monitoring

Continuous screening of merchant websites for content prohibited by card scheme rules (Mastercard BRAM / Visa GBPP-style compliance).

How the pipeline works

1. **Crawl** — site traversal (httpx, robots.txt, per-domain throttle), multi-page BFS over internal links + sitemap, within the tier limits (depth/pages).
2. **Text extraction** — trafilatura, stripping navigation/footers; normalisation (NFC + casefold).
3. **Morphology** — ru (pymorphy3), be (UDPipe belarusian-hse), en — every word form of every stop phrase.
4. **Matching** — Aho-Corasick over the tenant's stop lists and categories; anti-obfuscation: spaced-out letters (c a s i n o), homoglyphs (a Latin "a" in a Cyrillic word), transliteration (kazino → казино).
5. **AI layer (Premium)** — an LLM classifies each hit (a real sale vs an incidental mention); semantic detection of violations worded without stop phrases (embeddings + Qdrant).
6. **Evidence** — an immutable HTML snapshot + a screenshot (Premium), append-only, bound to the scan moment.

What the officer gets

Hit review

Statuses (violation / false positive), remarks, activity log.

Scheduling

Recrawl frequency per site and per risk category.

Export

Alert Report in PDF and Excel following the customer's template.

Evidence base

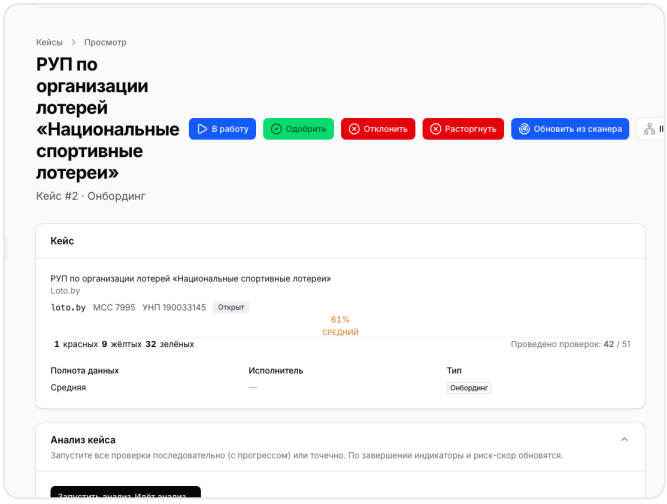
Immutable evidence (HTML + screenshot) is the bank's legal defence before the regulator: it records exactly what was on the merchant's website and when. Personal data is processed in line with Belarus Law No. 99-Z (and GDPR for EU traffic).

02 InvestiGate — underwriting and due diligence

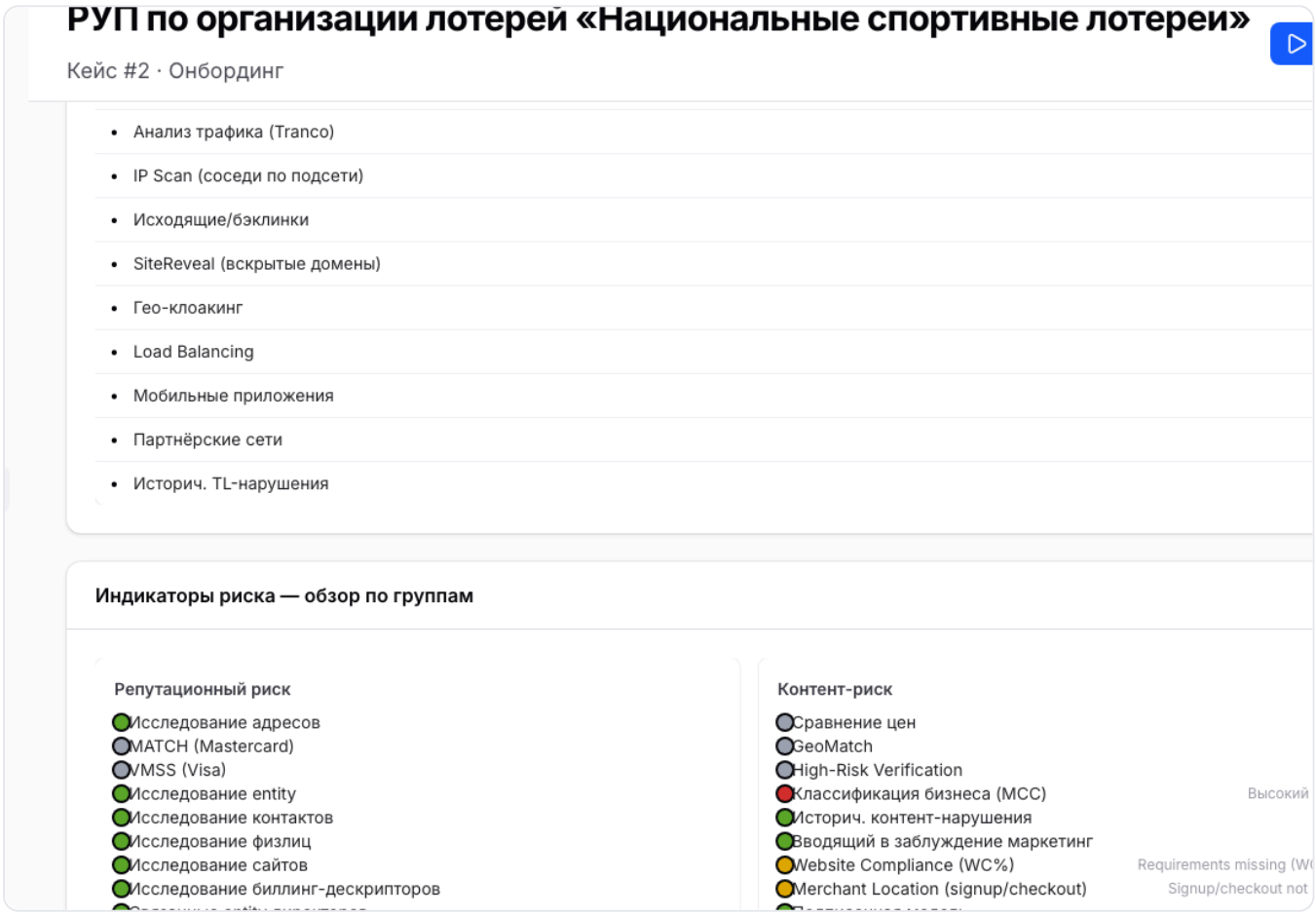
In-depth screening of high-risk merchants at onboarding and at the annual re-check: a single underwriting case file with a dynamic risk score and an evidence base.

What the case file contains

- ✓ **51 risk indicators** in 4 groups (reputation, content, laundering, transaction laundering) — traffic-light
- ✓ **Dynamic risk score** (subtractive model) + Low/Medium/High level
- ✓ **CREM** — credit exposure model (EtPR, scenarios, reserves, limits)
- ✓ **MCC Knowledge Base** — regulatory requirements (MRP/VIRP)
- ✓ **Analysis runner** — run all checks with progress, or one at a time
- ✓ **Recommendations checklist** and a multi-section **PDF report**



Case card: merchant brand, risk score, indicator summary, analysis runner

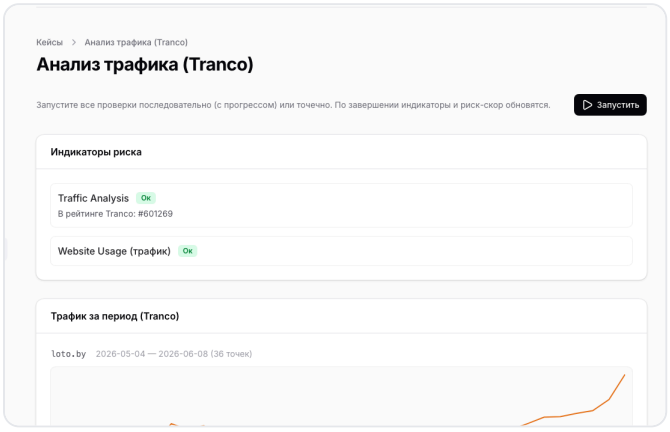


Risk indicator overview across 4 groups (traffic-light) + credit exposure (CREM)

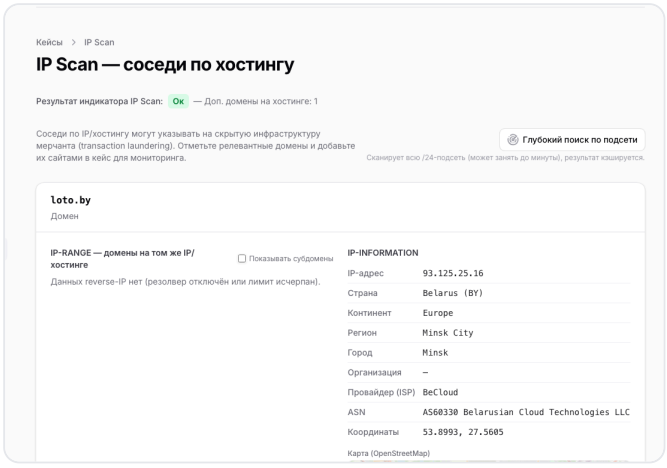
02 Transaction laundering controls

A deterministic TL contour uncovers the merchant's hidden infrastructure and front websites — without external paid data providers. Every check has its own detail page and feeds the case indicators.

- ✓ **IP Scan** — hosting neighbours by IP/subnet (reverse-IP), add straight to the case
- ✓ **Whois** — registrant cross-check (entity mismatch)
- ✓ **Domain and SSL age** — whois + Certificate Transparency
- ✓ **Traffic analysis** — Tranco ranking + spike detection
- ✓ **SiteReveal** — related domains uncovered and run against stop lists
- ✓ **Geo-cloaking** — different content per geo target
- ✓ **Load balancing, mobile apps, affiliate networks**
- ✓ **Test cards** and entry keywords (tax ID/name/email/phone/account)



Traffic analysis: Tranco rank history over a period + spike detection



IP Scan: subnet neighbours + IP information (geo/ASN) and a map

03 Onboarding — application intake

Merchant applications from any source, converted into a profile and an underwriting case.

Intake channels

Manual entry, CSV import, API ingest, a public application form on the website.

Merchant domain

Directors/UBO, addresses, documents, contacts (phone/email/account). Application → merchant + underwriting case in one click.

Platform

Multi-tenancy

Data isolation per client bank; RBAC (super_admin/admin/officer/auditor roles), 2FA.

Reliability

Activity audit trail, mail queue (Horizon), backups, health monitoring.

Languages and UI

Content scanning and UI in ru/be/en; a single compliance officer panel.

Compliance and protection

Regulatory fit

Mastercard BRAM and Visa GBPP-style controls. Immutable evidence — a defence before the regulator.

Data and privacy

Processing in line with Belarus Law No. 99-Z (and GDPR for EU traffic).

Tiers

Basic

The deterministic layer for everyone

- ✓ ru/be/en morphology + stop lists
- ✓ Anti-obfuscation (spacing/homoglyphs/transliteration)
- ✓ Multi-page crawl, recrawl scheduling
- ✓ HTML evidence, PDF/Excel export
- ✓ All modules: Monitoring · InvestiGate · Onboarding
- ✓ TL contour (IP Scan, whois, domain/SSL age, traffic…)

Premium + AI

Everything in Basic + the AI layer on candidates

- ✓ AI hit classification (LLM)
- ✓ Semantic violation detection (embeddings + Qdrant)
- ✓ Page screenshots in evidence
- ✓ SPA rendering and extended detections

Volumes (example)

BRAM/GBPP content — 3,000/month; transaction laundering controls — 3,000/month; in-depth high-risk screening — on demand. Subscription pricing model.

Request a demo

ArtCloud LLC · Minsk, Belarus
Website: **shield.by** · the "Request demo" form on the website