EMPIRICAL

Empirical Security builds precision AI tuned to your cybersecurity environment

Platform Overview

Empirical is the only exposure management vendor that publishes a false positive rate and measures performance. Our platform trains predictive models on near-real time exploitation telemetry and your enterprise's own data (assets, applications, controls, patching cadence) to produce calibrated probabilities of exploitation that you can measure, test, and defend to your board.

Why security teams choose Empirical

A common language for risk decisions

The Empirical global model grounds every prioritization decision in observable evidence. When someone asks "why are we fixing this one first?" The answer is a probability backed by real world exploitation telemetry, with critical indicators explaining the logic in real time.

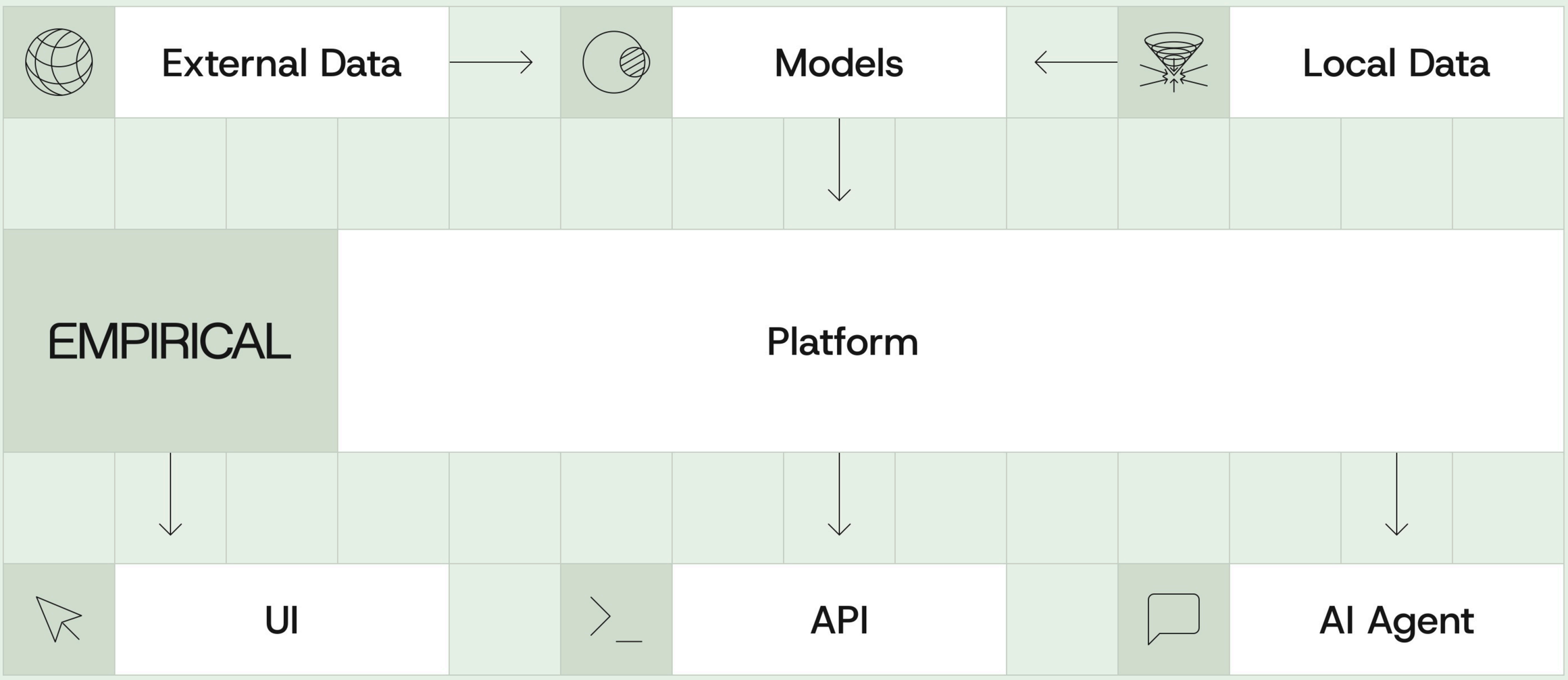
Your context changes the answer

A critical vulnerability behind a WAF with no internet exposure is not the same risk as a medium CVE on an unpatched, public-facing server running your payments stack. Generic models can't tell the difference. Our local model can because it trains on data only your environment produces.

We predict which vulnerabilities will be exploited in your environment.

CVSS measures severity, and EPSS predicts global exploitation probability, but neither tells you what will be exploited in your environment next month. Our models answer this crucial question. We demonstrate higher coverage and efficiency than traditional methods or off the shelf models. When fixing a limited set of vulnerabilities our predictions catch more of what actually gets exploited and waste less effort on what doesn't. We publish the data to prove our performance.

How It Works



See how your model would differ — book a walkthrough | empiricalsecurity.com | info@empiricalsecurity.com

EMPIRICAL

Platform Capabilities

Switch models instantly

Toggle between local, global, and EPSS views. See how each model scores the same CVE and understand why they diverge.

Full model transparency

Every data point contributing to a score is exposed. No black boxes. Inspect the features, question the output, trust the result.

Validate threats with exploitation evidence

Cross-reference any CVE against real-time exploitation indicators: active campaigns, malware associations, exploit maturity, attacker infrastructure.

AI agent for workflow automation

Ask our agent to triage findings, generate remediation plans, draft exception requests, or surface emerging threats grounded in the Empirical model's output, not hallucinated from irrelevant data.

Connect any security tool

Ingest from scanners, CNAPPs, EDR, CMDB, ticketing systems, and cloud platforms. The model improves with every source you connect.

17,000+ exploited-in-the-wild CVEs

The largest curated exploitation dataset in the industry. 12× CISA KEV. Built from the same ground-truth collection that powers EPSS.

Near-real time exploitation telemetry

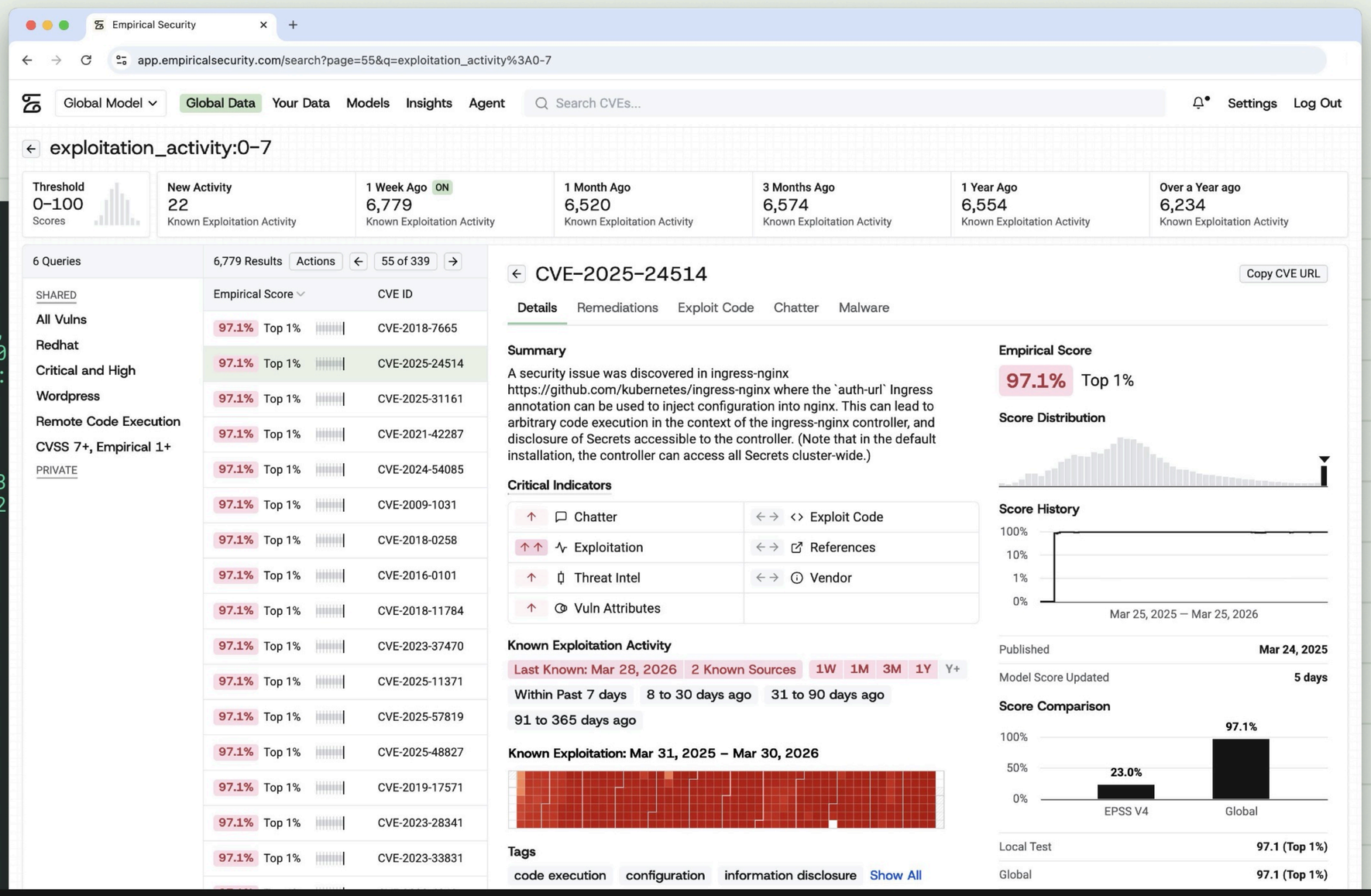
Models update with hourly exploitation signals. Not daily. Not weekly.
The threat landscape moves in hours. So does the model.

Forward-deployed data science team

Our team includes the creators of EPSS and the founders of risk-based vulnerability management. They work directly with customers to tune local models, validate results, and drive measurable risk reduction.

See how your model would differ

Try our models with your own local data and discover their impact on your cybersecurity environment.



API


```
{
  "identifier": "CVE-2023-49103",
  "reserved_at": "2023-11-21T06:0
  "published_at": "2023-11-21T06:

  "scores": {

    "local_model": {
      "score": 0.9091291982186883
      "percentile": 0.99618114602
      "computed_at": "2025-03-16

    },
    "global": {
      "score": 0.92099,
      "percentile": 0.99238,
      "computed_at": "2025-03-16

    },
    "epss_v4": {
      "score": 0.92099,
      "percentile": 0.99238,
      "computed_at": "2025-03-16

    },
  "platforms": [
```


See how your model would differ — book a walkthrough | empiricalsecurity.com | info@empiricalsecurity.com