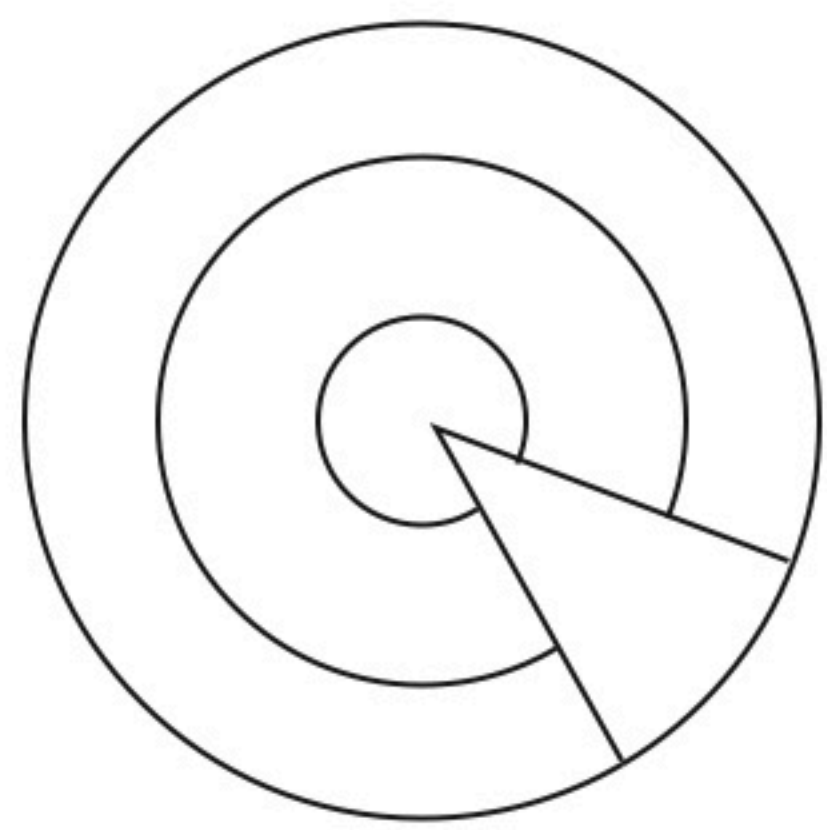


EMPIRICAL

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 shared language for risk decisions

The Empirical foundation 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.

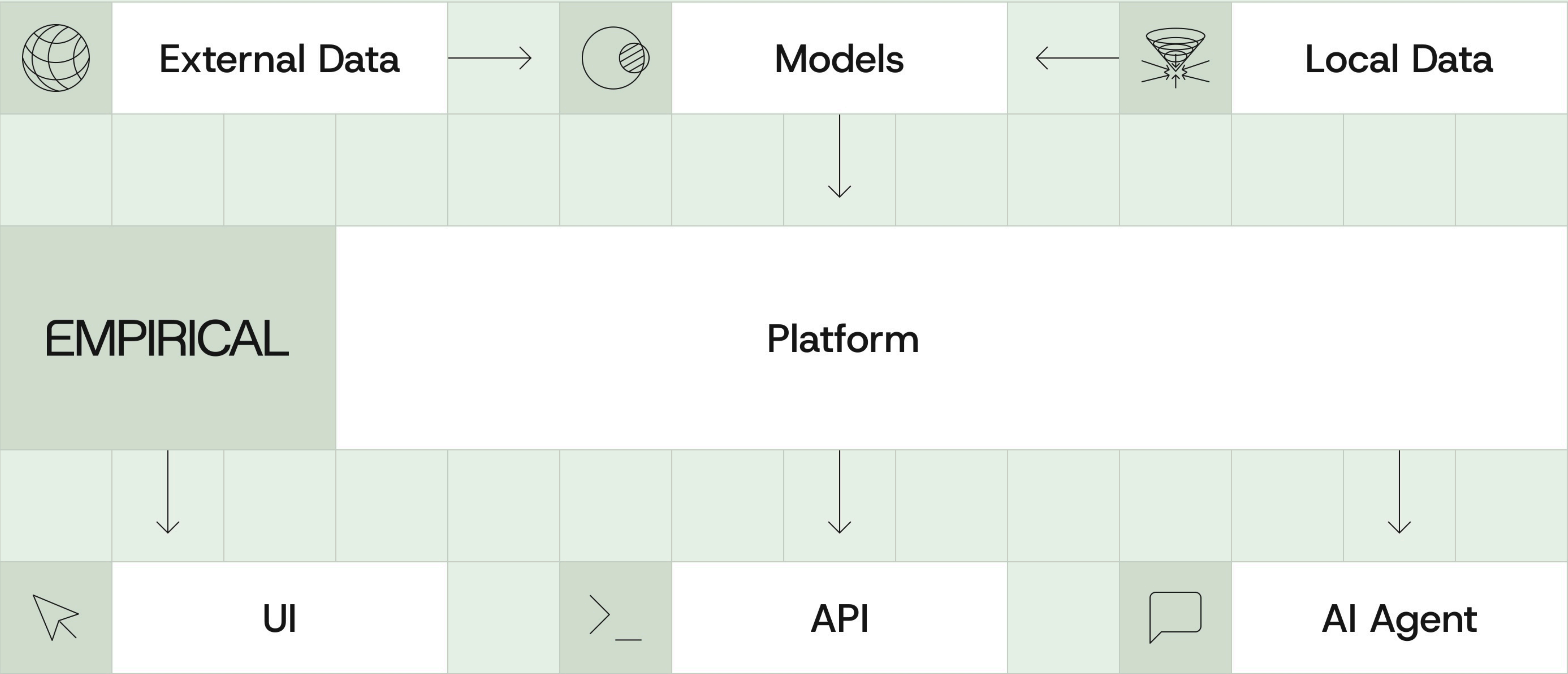
Your context changes the answer

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 radiant 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



Platform Capabilities

Switch models instantly Toggle between radiant, foundation, 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.	19,000+ 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": "2023-11-21T06:00:00Z",
  "published_at": "2023-11-21T06:00:00Z",
  "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": [

```

Empirical Security

app.empiralsecurity.com/search?page=55&q=exploitation_activity%3A0-7

Global Model Global Data Your Data Models Insights Agent Search CVEs... Settings Log Out

exploitation_activity:0-7

Threshold 0-100 Scores

New Activity 22 Known Exploitation Activity

1 Week Ago 6,779 ON Known Exploitation Activity

1 Month Ago 6,520 Known Exploitation Activity

3 Months Ago 6,574 Known Exploitation Activity

1 Year Ago 6,554 Known Exploitation Activity

Over a Year ago 6,234 Known Exploitation Activity

6 Queries

6,779 Results Actions 55 of 339

SHARED All Vulns Redhat Critical and High Wordpress Remote Code Execution CVSS 7+, Empirical 1+ PRIVATE

Empirical Score	CVE ID
97.1% Top 1%	CVE-2018-7665
97.1% Top 1%	CVE-2025-24514
97.1% Top 1%	CVE-2025-31161
97.1% Top 1%	CVE-2021-42287
97.1% Top 1%	CVE-2024-54085
97.1% Top 1%	CVE-2009-1031
97.1% Top 1%	CVE-2018-0258
97.1% Top 1%	CVE-2016-0101
97.1% Top 1%	CVE-2018-11784
97.1% Top 1%	CVE-2023-37470
97.1% Top 1%	CVE-2025-11371
97.1% Top 1%	CVE-2025-57819
97.1% Top 1%	CVE-2025-48827
97.1% Top 1%	CVE-2019-17571
97.1% Top 1%	CVE-2023-28341
97.1% Top 1%	CVE-2023-33831

CVE-2025-24514

Details Remediations Exploit Code Chatter Malware

Summary

A security issue was discovered in ingress-nginx https://github.com/kubernetes/ingress-nginx where the 'auth-url' Ingress annotation can be used to inject configuration into nginx. This can lead to arbitrary code execution in the context of the ingress-nginx controller, and disclosure of Secrets accessible to the controller. (Note that in the default installation, the controller can access all Secrets cluster-wide.)

Critical Indicators

Chatter	Exploit Code
Exploitation	References
Threat Intel	Vendor
Vuln Attributes	

Known Exploitation Activity

Last Known: Mar 28, 2026 2 Known Sources 1W 1M 3M 1Y Y+

Within Past 7 days 8 to 30 days ago 31 to 90 days ago 91 to 365 days ago

Known Exploitation: Mar 31, 2025 - Mar 30, 2026

Tags

code execution configuration information disclosure Show All

Empirical Score 97.1% Top 1%

Score Distribution

Score History

Published Mar 24, 2025

Model Score Updated 5 days

Score Comparison

EPSS V4	23.0%
Global	97.1%

Local Test 97.1 (Top 1%)

Global 97.1 (Top 1%)

