MIGGO × Grafana Labs

Miggo Security's Runtime Intelligence for Grafana Cloud

Real-Time Risk Decisions Powered by Your Own Telemetry

Runtime security is everywhere, from detection to protection, and depends on core system signals such as logs, metrics, traces, and profiles. Much of this telemetry already exists within most observability stacks. Yet, many runtime security approaches re-collect this data adding overhead, compute costs, and creating friction with platform teams.

By partnering with Grafana Labs, Miggo builds directly on existing production telemetry to determine what is truly exposed, what actually executes in production, and which vulnerabilities represent real, exploitable risk – without duplicating instrumentation or introducing operational overhead.

Real-Time Risk Decisions Powered by Your Own Telemetry

High-Impact Results for Security & Engineering Teams

60–99% Reduction
in critical vulnerability backlog noise.

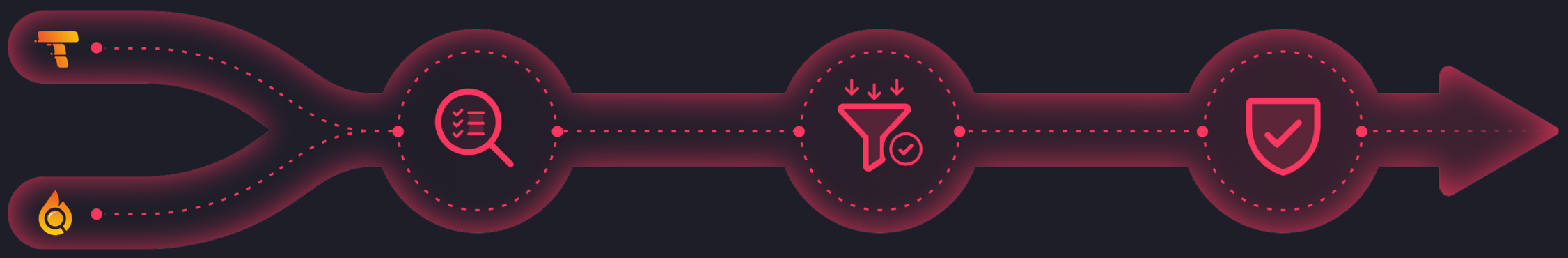
Evidence-Based Prioritization
grounded in actual runtime execution.

Faster Mitigation
of truly exploitable risk through WAF Copilot.

Zero Added Complexity
to your observability stack.

Reduce Friction
between security and engineering teams by providing evidence (e.g., traces, profiles) and reasoning for risk assessment.

Zero Added Complexity
for audit and compliance requirements by enabling comprehensive reporting of risk-specific assessments.



1 Collect
Grafana Cloud gathers live performance data from your application using Tempo and Pyroscope.

2 Analyze
Miggo securely pulls this data and uses its security tools to scan it for vulnerabilities.

3 Prioritize
Miggo ranks the vulnerabilities, showing the immediate danger to the live environment.

4 Mitigate
Utilize a virtual patch to protect instantly while developers work on a permanent fix.

Key Capabilities

Runtime BOM and Application Mapping

Transforms traces and profiles into visibility of services, APIs, AI components, dependencies, and exposure paths.

Vulnerability Pre-Mortem Analysis

Analyzes the precise runtime execution path a vulnerability would require, validating reachability, exposure, downstream impact, and blast radius before exploitation occurs.

Reachability & Exposure Validation

Identifies externally exposed vs. internally restricted components.

Grafana Labs

MIGGO

Better Together

Runtime Telemetry

Distributed Traces & Profiles

Production Visibility

Execution-Backed Prioritization

Reachability Evidence

Noise Reduction

Security Analysis

Vulnerability Validation

Attack Surface Intelligence

About MIGGO

Miggo Security delivers AI Runtime Defense through its application detection and response (ADR) solution, empowering enterprises to identify, mitigate and respond to application threats. Miggo enables organizations to secure traditional, cloud-native and AI-driven applications at scale, reducing exposure windows by up to 99% and cutting operational overhead by 30% or more. Miggo Security has been awarded Gartner Cool Vendor 2025 for AI Security and Frost & Sullivan's Product Innovation Award 2025, among others.

About Grafana Labs

Grafana Labs, the company behind the open observability cloud, is founded on the principles of open source, open standards, open ecosystems, and open culture. Grafana Cloud, their fully managed observability platform, is flexible and built for scale, enabling organizations to see, understand, and act on their data so they can move at the speed of their ambitions. Today, more than 25 million users and 7,000+ customers – including Anthropic, Bloomberg, NVIDIA, Microsoft, and Salesforce – rely on Grafana Labs to make their software run better.
Learn more at grafana.com.

Secure your applications today. Schedule a demo at **miggo.io**