



Continuous Observability for Security & Compliance

ZERO CODE CHANGES • LANGUAGE AGNOSTIC • BRING ANY WORKLOAD • ANY CLOUD • LOW PERFORMANCE OVERHEAD • PLUG INTO CI

What is DeepFactor?

DeepFactor is the industry's first Continuous Observability platform enabling Engineering and AppSec teams to find and triage RUNTIME security, privacy, and compliance risks in your applications—including 3rd party components—within the DevOps pipeline.

How Does It Work?

DeepFactor automatically observes **billions** of live telemetry events in every thread/process/container to detect anomalies during test, staging, and production.

DeepFactor requires zero code changes to the app, uses one command, works with any workload (container/Kubernetes/Docker or even traditional apps) and any cloud, is agnostic to the language in which the app is written, has low performance overhead, and plugs into any CI platform using DeepFactor's Observability-as-Code API.

Why Now?

Remediating risk in production is exponentially more expensive than resolving during development. Why take the risk and ship 'maybe' secure code to prod knowing today's appl are more complex (multiple languages, 3rd party components, cloud services, containers, microservices, etc.) and are released at a higher frequency than ever before?

- ✓ Observe billions of application events at runtime
- ✓ Detect anomalies to identify security & compliance risks
- ✓ Enable engineering teams to create secure & compliant apps

Why Runtime Visibility?

When considering adding security to your DevOps practices, think about it in two parts: static and runtime.

Here's an analogy to help clarify why adding comprehensive runtime visibility is critical.

When you go to buy a car, do you make the decision solely based on how it looks parked at the dealership? Probably not. You want to take it for a test drive since looking at a parked car is very different from test-driving it. It's not either or...it's both.

Static code analysis is like the parked car and it's different from observing a running application, which is the running car. And this is what DeepFactor delivers.

Who is DeepFactor?

DeepFactor was **created for developers by developers**. We have 100+ years of combined software development, security, and DevOps experience. Our leadership team has been key players for Citrix, Cisco, IBM, Qualys, HPE, and Micro Focus. We have offices located in the U.S. and India. Contact us today: hello@DeepFactor.io

Continuous Observability for Security & Compliance

What Insights Does DeepFactor Identify?

Deep Insights cover system call risks, data risks, behavior risks, DAST scans, and vulnerable dependencies to create high-fidelity alerts with actionable evidence.



CODE EXECUTION RISKS

Risks in process, memory, filesystem, and network behaviors determined by observing system and library calls



CUSTOM ALERTS

Alert developers during CI if in-house or 3rd party app deviates from expected process, memory, filesystem, and network behaviors defined by policies



DATA RISKS

Identity & credential tracking, weak encryption, unencrypted PII in DB or object storage, keys in env vars, data audit logs, unencrypted data in flight, etc.



OWASP ZAP SCAN RESULTS (WEB & API)

Results of built-in headless OWASP ZAP DAST Scanner



PRIVACY & COMPLIANCE RISKS

Risks mapped to GDPR, PCI, ISO27001 and other compliance frameworks



DYNAMIC DEPENDENCY ANALYSIS

Prioritized list of vulnerable dependencies based on actual runtime usage, touchpoints, and actionability; augments SCA tools and reduces alert fatigue



BILL OF MATERIALS

Catalog of 3rd party libraries and dependencies used by the app, including opensource and licensing; makes SOC2/other compliance processes a breeze



CHANGES BETWEEN RELEASES & ENVIRONMENTS

Deviations in ports, processes, metrics and configurations between versions and between environments