Oligo Runtime Security Platform

DETECT AND PREVENT SECURITY RISKS FOR
APPLICATIONS YOU BUILD, BUY, AND USE

The Need for Runtime Security

Despite significant investment in application and cloud security tooling, applications remain the most common data breach vector. Why is this the case?

While they have utility, traditional "shift-left" application security tools are point-in-time. These tools excel in identifying potential risks, but they fail to detect imminent risks and active exploits. Meanwhile, cloud security tools provide some visibility for production applications, but they fail to monitor the application layer, **leaving companies defenseless to exploits and attacks.**

The Oligo Solution: Modern Runtime Security For Your Applications

Oligo transforms runtime security with instant detection and prevention of exploits, as well as vulnerability prioritization and remediation based on actual execution status. With Oligo, security teams can:

- **Detect & Prevent Exploits in Real Time:** stop known and unknown attacks based on library profiling, pattern analysis, and crowdsourcing.
- **Prioritize Real Risks, Not Just Theoretical Ones:** reduce CVE backlogs 90% or more by focusing only on vulnerable dependencies actually executed in production.
- **Eliminate Alert Fatigue:** reduce noise by filtering out non-exploitable threats.

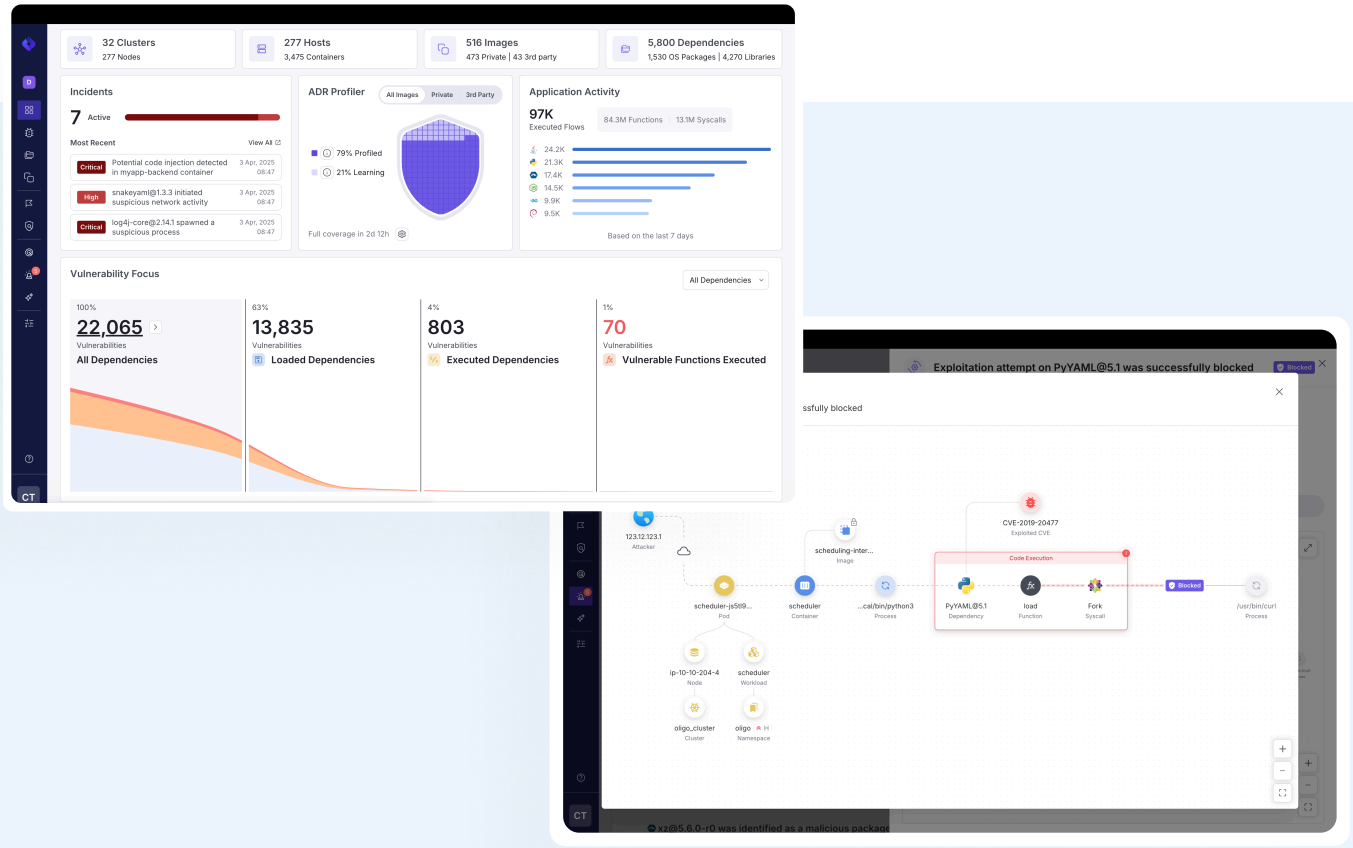
Key Capabilities

- **Cloud application detection and response (CADR):** detection and response for known CWEs, CVEs, as well as zero-day exploits at the application and workload level.
- **Workload threat detection (CWPP):** detection of suspicious and malicious workload events (malware/network/privileges/etc).
- **CVE backlog reduction:** focus only on the vulnerabilities that present an immediate attack vector: running vulnerable dependencies.
- **Real-time SCA + SBOM:** reference an actionable bill of materials of every library, dependency, and function that's used within the apps you build, buy, or use.
- **Secure AI Apps:** protect against open-source GenAI frameworks embedded within your apps, and monitor AI-generated code for malicious behavior.

Why Oligo?

Oligo is the only solution built with Deep Application Inspection (DAI), which observes activity at the kernel level and ties them to specific components within the running application. This sets Oligo apart from other runtime security approaches.

- Unlike other runtime tools, Oligo offers protection against app exploits - the first phase of an attack
- Unlike point-in-time scanners, Oligo detects which vulnerabilities pose an immediate risk
- Unlike legacy WAF and RAPSs, Oligo prevents exploits at the function level without any risk of taking down your application



Technical Specifications

The Oligo sensor is application-independent and easy to implement and upgrade. You can deploy it in just minutes. Because it is kernel-based, you don't have to modify or even restart your applications.

- **Deployment Model:** Helm-package (kubernetes), VM sensor
- **Integrations:** Ticketing/Helpdesk, SIEM/SOAR, ASPM, Cloud Security Platforms, DevSecOps tools
- **Performance impact:** ~1% CPU overhead
- **Supported environments:** on-prem / Cloud: Kubernetes, virtual machines

See Oligo For Yourself