Cloud Application Detection & Response (CADR): Stop Cloud Application Attacks in Real Time

Oligo CADR provides unified detection and response that correlates activity across applications, workloads, hosts, cloud environments, and networks. With real-time visibility into root cause, attack path, and impact, SOC and Product Security teams can stop attacks, minimize attack paths, and respond faster and more precisely to incidents.

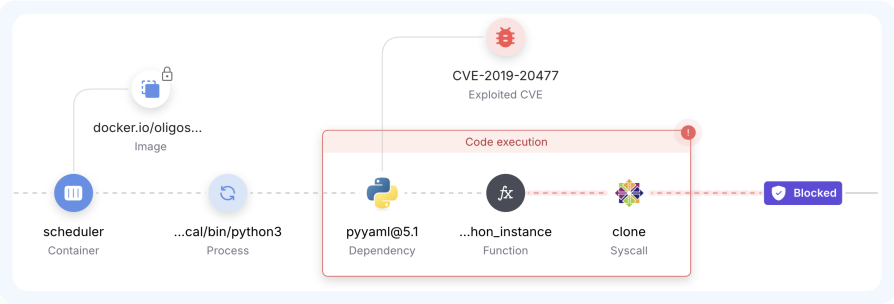
Why Other Approaches Don't Deliver True Runtime Protection

- **Static App Scanners:** don't see how applications behave in real time, miss active exploits, and flood teams with irrelevant vulnerabilities.
- **Web Application Firewalls:** rely on static rule sets and can be easily bypassed as legitimate traffic in the context of modern cloud applications.
- **Cloud Security Tools (CWPP, CNAPP):** focus on infrastructure only, lacks application context, and delivers false positives

The Result: Too many false positives, missed application exploits, and SOC teams left scrambling without the "how" or "why" of an attack.

How Oligo Delivers True Runtime Protection

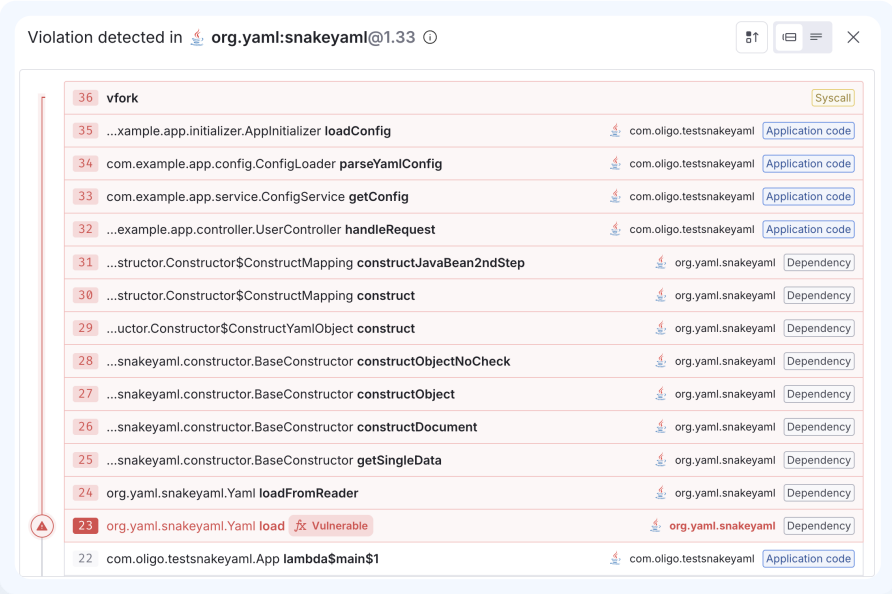
- **Real-time detection** across all layers where applications are hosted and run.
- **Contextual blocking of malicious syscalls,** preventing CVE exploits, zero-day attacks, supply chain compromise, and risks of intrusion into infrastructure.
- **Deep application visibility** that ties together root cause, attack path, and impact across the entire stack.



Key Features

- **Instant, Unified Detection:** Correlates signals across network, application, and infrastructure for accurate and rapid incident triage

- **Contextual Blocking of Malicious Behavior:** Sandbox syscalls from specific libraries—stopping supply chain, CVE exploits, and zero-day attacks before execution.
- **Zero-Day & Non-CVE Detection:** Behavioral profiling and pattern analysis to identify malicious activity without reliance on signatures or CVEs.
- **Lightweight Sensor:** Minimal performance impact: ~1% CPU and 300MB memory footprint, far leaner than traditional solutions.



Types of Attacks CADR Protects Against

- **Remote Code Execution (RCE):** detect exploitation attempts in real time and block execution.
- **Supply Chain Compromise:** Stop malicious packages and dependency hijacks at runtime.
- **Privilege Escalation & Lateral Movement:** Identify and contain attacker behavior before escalation spreads.
- **Living-off-the-Land & Fileless Attacks:** Behavioral analysis detects malicious use of legitimate tools.
- **Container Escapes & Cloud-native Exploits:** Protect Kubernetes and containerized workloads at runtime.

Why CISOs & SecOps Choose Oligo CADR

- Consolidates multiple point solutions into a single platform, reducing cost and complexity.
- Enriches SIEM and SOAR playbooks with application-layer context, completing the "SOC visibility picture"
- Delivers full attack picture, making incident response more accurate and faster with clear attack paths and root cause analysis.
- Ensures business continuity by stopping modern attacks without needing to take down the entire application.

See Oligo For Yourself