WHITEPAPER

Reimagining Application Threat Assessment, Detection & Response

DEEP APPLICATION INSPECTION PROVIDES CONTEXTUAL RUNTIME INSIGHTS

EXECUTIVE SUMMARY

Despite significant investments in shift-left practices, application security solutions, and cloud security tools, businesses of every size and industry continue to be plagued by costly and disruptive web application breaches stemming from supply chain attacks, zero-day vulnerabilities, and other software-related exploits. Around 38% of data breaches are attributed to the exploitation of known unpatched vulnerabilities or unknown zero-day vulnerabilities[1]. That's more than any other attack vector including compromised credentials and phishing attacks, and more than any other non-human-based attack vector.

Tracking, prioritizing, and mitigating software vulnerabilities is a significant challenge for most organizations. Tens of thousands of new CVEs are discovered annually, with each year's total surpassing the last. Development organizations and security teams are hard pressed to keep pace.

Traditional vulnerability scanning tools and runtime protection apps are notoriously ineffective

The central issue is that most organizations lack a clear understanding of which vulnerabilities are genuinely exploitable within their applications and runtime environments. Developers waste time and effort addressing CVEs that don't pose a legitimate threat to the business, which impacts development schedules and hinders business agility. SecOps teams squander time and resources patching vulnerabilities that pose no real-world risk, which delays the mitigation of truly exploitable vulnerabilities and leaves the door open for attackers.

[1] Mandiant M-Trends 2024 Special Report

Detecting and remediating application security incidents is equally challenging. Threat actors routinely exploit application vulnerabilities to penetrate systems and move laterally without detection.

The average time to exploit a vulnerability is five days[2], but the mean time to remediate known exploited vulnerabilities is several months.

Now is the time for application and cloud security leaders to take a fresh look at their systems and practices. The average cost of a breach involving known unpatched vulnerabilities or unknown zero-day vulnerabilities exceeds $4.3 million.[1] And the problem is about to get a lot worse with artificial intelligence and machine learning. AI will dramatically increase the speed, scale, and sophistication of attacks, empowering adversaries to adapt tactics and techniques, identify and exploit vulnerabilities, and evade detection with unprecedented agility and efficiency.

Oligo provides deep application inspection for instant detection and response

Oligo was specifically created to overcome the fundamental limitations and inefficiencies of traditional shift-left security approaches and conventional application and cloud security solutions. Oligo makes it fast and easy to discover genuinely exploitable vulnerabilities and block active exploits in any cloud-native application you build, buy, or use. The Oligo platform reduces your attack surface, accelerates threat detection and mitigation, and frees resources to focus on real threats and core business tasks.

INTRODUCTION

The Trouble with Shift-Left Solutions and Runtime Protection Tools

Today's development organizations and security teams use a variety of tools to identify application vulnerabilities and mitigate application-based threats. Traditional security offerings like Software Composition Analysis (SCA), Runtime Application Self-Protection (RASP), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), and Dynamic Application Security Testing (DAST) solutions help strengthen cybersecurity, but each of these tools comes with its own set of challenges and limitations.

[2] Google Cloud Blog, October 2024

Application and cloud security posture analysis tools

Oligo was specifically created to overcome the fundamental limitations and inefficiencies of traditional shift-left security approaches and conventional application and cloud security solutions. Oligo makes it fast and easy to discover genuinely exploitable vulnerabilities and block active exploits in any cloud-native application you build, buy, or use. The Oligo platform reduces your attack surface, accelerates threat detection and mitigation, and frees resources to focus on real threats and core business tasks.

Software composition analysis (SCA) solutions

SCA tools are designed to identify vulnerable components within an application's codebase, particularly open-source libraries and dependencies. They are inherently inefficient and impractical in today's world.

- **Lack of context:** SCA tools can identify vulnerabilities in software components, but they can't tell you if those vulnerabilities present a genuine risk. Is the vulnerable code loaded into memory? Is it called by an application? Is a threat actor actively exploiting it?

- **False positives:** SCA solutions generate a high number of false positives, overwhelming developers with alerts for vulnerabilities that may not pose a real threat.

- **Static analysis:** SCA tools primarily conduct static analysis; they do not account for dynamic behavior or interactions between components at runtime.

Dynamic Application Security Testing (DAST) solutions

DAST tools identify vulnerabilities in running applications by simulating real-world attacks. They can help mitigate risk but are inefficient point-in-time simulations.

- **Limited scope:** DAST solutions are designed to identify known vulnerabilities documented in CVE databases. They cannot detect undocumented vulnerabilities and cannot proactively identify and block live attacks.

- **Lack of context:** Like SCA tools, DAST solutions can identify vulnerabilities in production software components, but they can't tell you if those vulnerabilities pose a genuine risk to the business.

- **False positives:** Just like SCA tools, DAST solutions can overwhelm developers with false positives.

- **Performance impact:** DAST scans can adversely affect the performance of production applications.

Cloud security posture management (CSPM) platforms

CSPM solutions focus on assessing and improving the security posture of cloud environments by identifying infrastructure misconfigurations and compliance issues. Despite their benefits, CSPM solutions also have limitations.

- **Point-in-time visibility:** CSPM solutions often rely on periodic scans and cannot detect real-time changes or dynamic threats.

- **Contextual gaps:** While CSPM solutions can identify if a vulnerable component is running in a cloud environment (i.e., reachable), they cannot determine if the component is in use or being exploited.

- **Infrastructure-centric view:** CSPMs focus on infrastructure misconfigurations, and don't provide visibility at the application level where most attacks occur.

Runtime protection tools

Runtime application self-protection (RASP) tools

RASP tools aim to enhance application security by detecting and mitigating attacks in real-time, directly within the runtime environment. These tools are also fraught with inefficiencies and limitations.

- **Operational overhead:** RASP tools often require code changes and embedded instrumentation, which adds application development, integration, and maintenance cost and complexity.

- **Performance issues:** The in-line operation of RASP tools can introduce notable latency, impact application stability, and impair application performance.

- **Limited scope:** RASP tools are primarily designed to protect first-party software and typically don't offer adequate coverage for open-source libraries or third-party components.

Cloud workload protection platforms (CWPP) solutions

CWPP products are designed to monitor and safeguard cloud workloads. They can help identify runtime threats but, since their visibility is limited to the container/host-level, detected threats are often indicative of an already successful exploit.

- **Performance impact:** CWPP solutions can introduce latency and impact the performance of applications, especially when operating in-line.

- **Integration complexity:** CWPP products often require significant integration efforts, which adds cost and complexity.

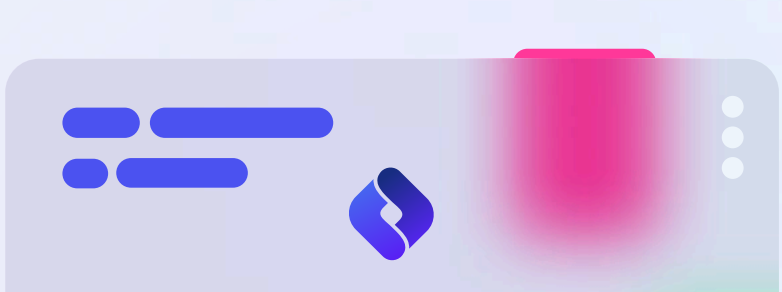
- **Limited coverage:** CWPP solutions may not provide sufficient protection for third-party components or open-source libraries.

Why Oligo?

We designed Oligo from the ground up to overcome the inherent inefficiencies and constraints of traditional shift-left security solutions and runtime protection tools. Oligo dramatically strengthens your security posture, simplifies vulnerability prioritization, and makes it possible to detect and prevent exploits within your applications—whether they are conducted against first-party code or third-party code.

Fix only what matters with advanced application security vulnerability management

Oligo is the first and only solution that provides deep insights into cloud-native applications and their dependencies so you can immediately identify exploitable vulnerabilities that pose a legitimate threat to your business.

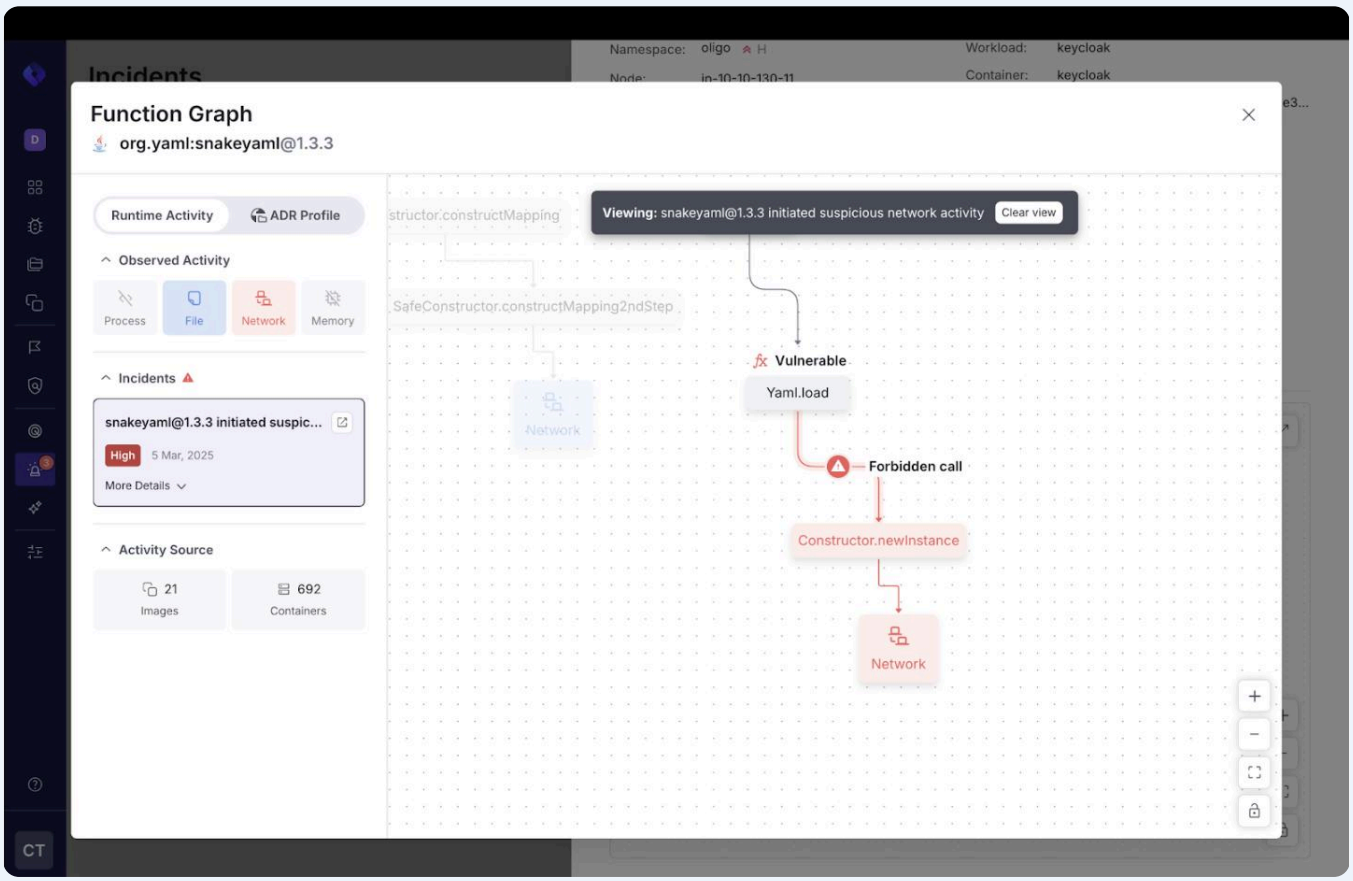


Stop attackers in their tracks with innovative application detection and response

With Oligo, you can detect and prevent application-based attacks automatically, in real-time, to stop adversaries from compromising your applications.

What Makes Oligo Special?

Oligo provides deep application inspection at runtime, with function-level call tracing to help you pinpoint application vulnerabilities and contain attacks before they impact your business. The platform addresses the "left side" of the development cycle by helping you efficiently discover and prioritize CVEs. It addresses the "right side" of the development cycle by helping you automatically detect and respond to application exploit attempts.



Function-level call tracing

With Oligo you can:

With Oligo, you can detect and prevent application-based attacks automatically, in real-time, to stop adversaries from compromising your applications.

- **Discover genuine exposure:** conclusively determine if vulnerable code is loaded to memory or called by an application.

- **Detect active exploit attempts:** intelligently identify activity symptomatic of an in-progress attack.

- **Preemptively stop attacks:** automatically block suspicious actions at the function level, without compromising the rest of the code base and application.

We designed Oligo to be lean and non-intrusive. Unlike traditional in-line AppSec and cloud security tools, Oligo runs alongside an application and does not impair its performance or affect its operation.

Oligo is also incredibly fast, easy, and cost-effective to deploy and scale. The solution requires no code changes or application restarts. It offers exceptional TCO and rapid ROI, delivering value within minutes.

Why Is This Important?

With Oligo, you can:

- **Gain unparalleled visibility** into your application security posture by definitively determining if vulnerable code is exploitable.

- **Contain risk** by automatically detecting and mitigating threats before adversaries can exploit them and do serious damage.

- **Appropriately focus** vulnerability remediation efforts based on tangible risk.

- **Save time**, avoid wasted effort, and free up staff to work on strategic tasks.

- **Improve readiness** and responsiveness by quickly assessing the real-world impact of a new CVE.

- **Increase transparency** and customer trust by providing accurate and timely CVE exposure information.

Oligo Use Cases

You can use Oligo to satisfy a variety of application security posture assessment and application detection and response requirements.

- **Real-time application detection and response:** detect and prevent malicious function calls and activity occurring within your apps in real-time, with workload context.

- **Application vulnerability management:** identify known supply chain threats, vulnerable libraries, and functions that are running to reduce CVE backlogs and prioritize fixes.

- **Real-time software bill of material (SBOM) and automated VEX generation:** generate SBOMs and AI-BOMs with contextual information and automatically create Vulnerability Exploitability eXchange reports.

- **Compliance and assurance:** meet software vulnerability assessment and reporting requirements for FedRAMP, PCI-DSS, NIST SSDF, GLBA, HIPAA, and other initiatives and regulations.

Oligo Architectural Overview

Oligo is designed to provide deep contextual insights into application behavior at runtime without impairing workload performance or operation. The solution is highly scalable and extensible, yet extremely easy to deploy and use.

A single platform with a common agent and uniform user interface, Oligo delivers advanced application security posture assessment functionality and innovative application detection and response (ADR) functionality, addressing a variety of use cases.

The Oligo platform includes:

Oligo Sensors

Non-intrusive, lightweight agents deployed on Linux VM instances or Kubernetes nodes

Oligo Scanner

Kubernetes scanner that collects metadata about running containers their alerts.

Oligo Cloud

A managed SaaS solution that gathers, aggregates, analyzes, and acts on sensor data

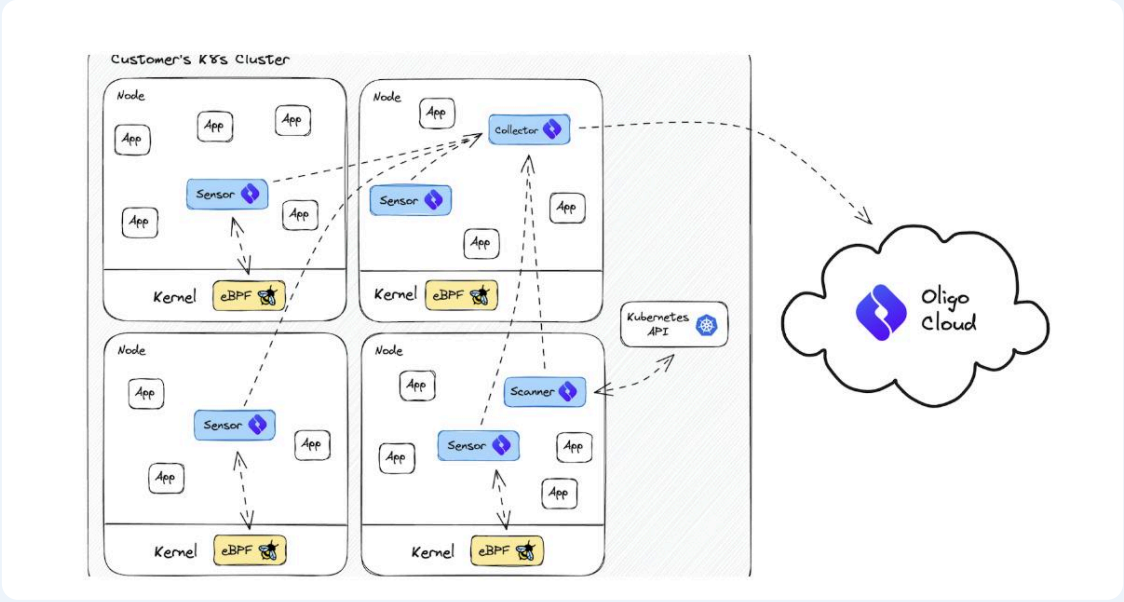
Oligo Collector

Aggregator that gathers Oligo Sensor data for communication with the Oligo Cloud

Oligo Console

A secure, browser-based user portal for detecting and investigating vulnerabilities and exploits

Oligo supports a RESTful API, webhooks, and offers integrations with a variety of third-party collaboration, incident tracking, and application security posture management (ASPM) tools.



Oligo Kubernetes Reference Architecture[3]

Oligo Sensor

The Oligo Sensor seamlessly monitors application libraries, tracking function calls and kernel-level activities in real-time. Unlike traditional in-line RASP and CWPP solutions that can impact application performance or stability, the Oligo Sensor runs as a DaemonSet with one sensor on each node (i.e. one sensor per dozens of applications), imposing minimal overhead. It also consumes relatively low CPU and memory resources, minimizing recurring public cloud-compute expenses.

The sensor is built on Linux eBPF (extended Berkeley Packet Filter), a novel technology used to safely extend the capabilities of the Linux kernel at runtime for observability, tracking, filtering, and other purposes. eBPF is field-proven and used by leading tech companies like Google, Netflix, Facebook, and Cloudflare.

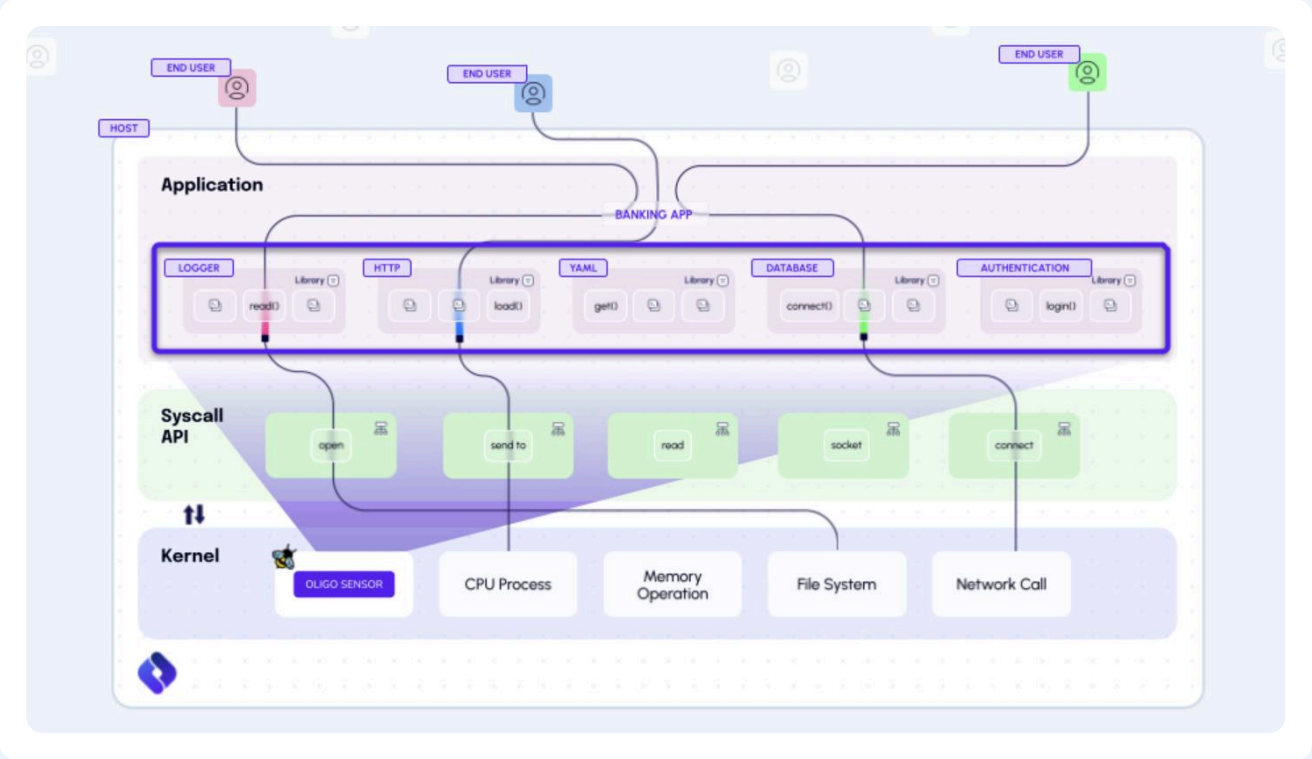
Network, security, and application performance monitoring vendors can attach eBPF programs to various kernel events to inspect or modify data passing through the kernel, without needing to recompile the kernel or reload kernel modules. Oligo uses eBPF to power its deep application inspection, which allows security and development teams to understand exactly how their code behaves in real time.

[3] In a VM implementation the Oligo Sensor is deployed directly on each virtual machine.

The Oligo Sensor dynamically tracks which application libraries are installed, loaded into memory, or executed on a particular VM instance or Kubernetes node. It continuously monitors application behavior, providing real-time observability into the application, its dependencies, and the base operating system (Debian, CentOS, Ubuntu, etc.).

The sensor monitors individual function calls to identify anomalous activity.
Supported detections include common container-level threats, and:

- **File management actions,** such as opening a file, reading, or writing to it
- **Networking and internet-access actions**
- **Process-related actions**, such as new process execution, process information, internal process communication, scheduler, threads, process control, and process tracing



Function-call observability

Learn more

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.

Oligo Cloud

Oligo Cloud is a managed SaaS solution that efficiently aggregates, analyzes, and acts on data gathered from Oligo Sensors. The cornerstone of Oligo Cloud is a comprehensive application behavior knowledge base maintained by **Oligo Research**, a team of world-class ethical hackers, AI security leaders, and application security experts. Collectively, the Oligo Research team has discovered hundreds of CVEs in some of the world's most prominent applications.

The extensive knowledge base encompasses open-source and commercial off-the-shelf software components. It includes CVEs from public vulnerability databases and repositories, as well as unique vulnerabilities discovered by the Oligo Research team.

Oligo uses AI to identify suspicious activity, even if that activity is not documented in a published CVE. The knowledge base maps CVEs to specific operating system packages and provides actionable insights, such as recommending patches to fix the vulnerability.

Detecting active exploits

Anomalous application activity is instantly flagged in the Oligo Dashboard. You can also automatically open a trouble ticket, create a Slack message, send out an email, or kick off other notification actions when unusual activity is detected.

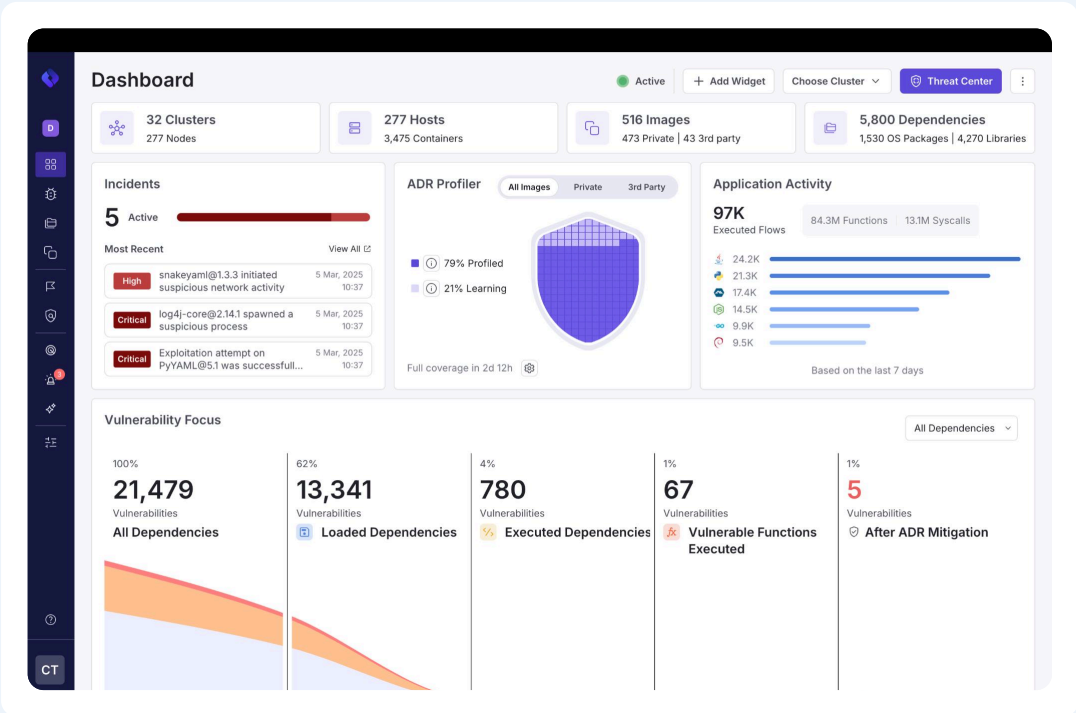
Remediating active exploits

Oligo Cloud intelligently blocks active exploits by automatically prohibiting applications from performing anomalous function calls symptomatic of an attack.

Oligo Console

The Oligo platform includes a secure, browser-based user interface that lets development and SecOps professionals efficiently identify and qualify application vulnerabilities and live application security incidents. The Oligo console provides summaries and detailed vulnerability reports, alerts and alert forwarding capabilities, exportable SBOMs and VEX reports with contextual information, and real-time incident reporting and insights.

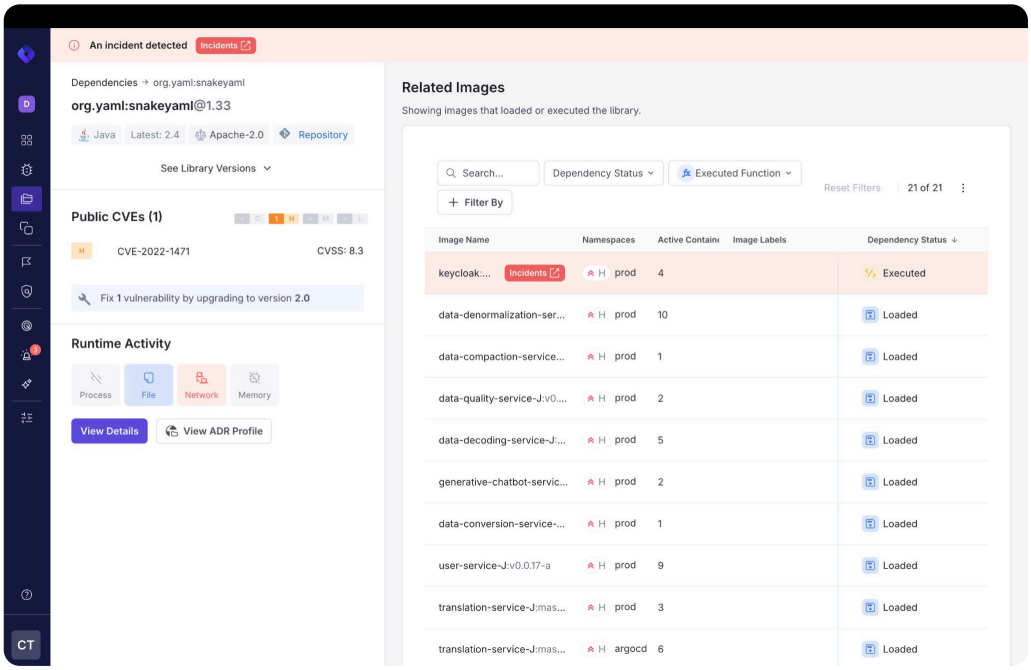
An intuitive dashboard lets you instantly assess your overall application security posture, identify active exploits, and view key threat intelligence data such as how many exploitable vulnerabilities are present in your runtime environment and how many vulnerable functions are being executed.



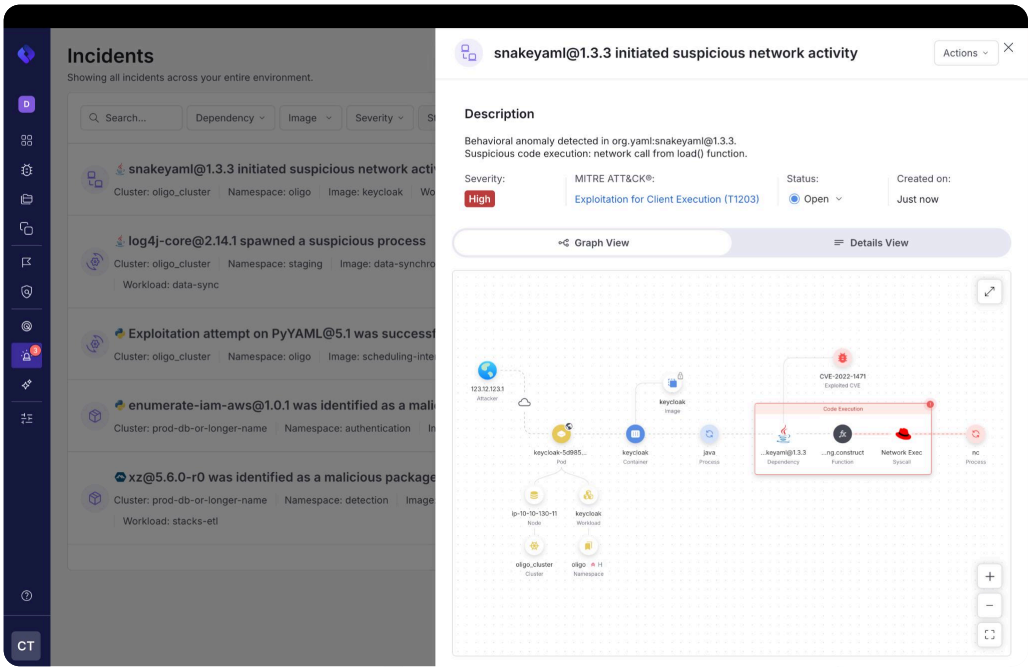
Oligo dashboard

You can drill down to get detailed information about individual dependencies and corresponding vulnerabilities.

You can also drill down to get detailed information about live incidents. Function call graphs and call stack listings make it easy to analyze and isolate in-progress attacks.



Detailed vulnerability reports



Real-time incident analysis and isolation

Identity and access management (IAM) options

The console supports a variety of standards-based IAM methods including single sign-on, multi-factor authentication, and passwordless authentication. It also supports SAML (Security Assertion Markup Language) and OIDC (OpenID Connect) for federated authentication using Microsoft Entra ID (formerly known as Azure Active Directory), Okta, and other identity providers.

Third-party integrations

You can automatically forward Oligo alerts and notifications to third-party tools and platforms including Microsoft Teams, Slack, Jira, and GitHub. Oligo also offers integrations for third-party ASPM tools including Armorcode, DevOcean, Ox Security, Seemplicity, and Stream Security.

Oligo Customer Success Stories

Oligo in action: Sage cuts vulnerability backlog by 90% in under an hour

Sage is the market leader for AI and ML-enhanced integrated solutions for accounting, payroll, and payments, supporting millions of entrepreneurs across the world. The solution provider's development organization was overwhelmed by vulnerability sprawl. They used Dependabot to track dependencies and identify CVEs but had no way to determine which CVEs posed real-world risk in production.

After evaluating several options, Sage deployed Oligo to improve observability and increase developer productivity. By identifying exploitable CVEs, Oligo's deep, contextual insights helped the development team slash their vulnerability backlog by 90% in under an hour. "Oligo has changed the way we work," says Senior Application Security Specialist, Javan Rasokat. "It means the developers have time to work on other, more important stuff".

Oligo in action: Mural accelerates zero-day response and risk reduction

Mural is the #1 visual work solution for the enterprise, trusted by 95% of the Fortune 500. The platform provider uses Oligo to efficiently identify, quantify, and mitigate zero-day vulnerabilities. "With Oligo we've been able to quickly assess the impact of zero-day vulnerabilities and accurately classify a CVE's exploitation risk in our environment," explains Maanul Shrivastava, Head of Application Security at Mural. "We've been able to re-prioritize exploitable issues for remediation, validate when a fix has been deployed to production, and make recommendations on migrating or upgrading infrastructure and technology."

When an alarming CVE makes headlines, Oligo makes it easy for Shrivastava and his team to reassure customers that Mural has it covered. "Customers want to know quickly whether these issues could have a security impact for them. With Oligo, I can show them that there isn't a risk and help them understand exactly why that risk isn't present."

CONCLUSION AND NEXT STEPS

The explosive growth of vulnerabilities in cloud-native software has created seemingly insurmountable challenges for development and security teams. Despite major investments in scanning tools and runtime protection platforms, most organizations lack a comprehensive understanding of which vulnerabilities are genuinely exploitable in their applications and runtime environments. To add to this, most organizations struggle to detect and remediate modern application-based attacks.

Oligo is the first and only solution that provides deep application inspection at runtime, delivering real-time visibility into library and function-level activity. With Oligo, development and security teams can accurately pinpoint where code vulnerabilities exist and if they are in use, providing a clear picture of true application risk. The Oligo platform also continuously monitors application components to detect anomalies and stop malicious behavior before adversaries disrupt business-critical services or exfiltrate confidential data.

To learn how Oligo can help your company strengthen its application security posture, improve productivity, and reduce risk, contact us today.

About Oligo

Oligo protects applications against attackers with the industry's leading Application Detection and Response platform. With deep application inspection through real-time monitoring and context-aware analysis, Oligo enables customers to instantly see all the vulnerabilities in their environments, identify those that matter most, and stop application-based attacks in their tracks. https://www.oligo.security/

Unlock More Value Today with Oligo

oligo

Interested in how Oligo can help you detect application breaches, protect yourself from unknown threats, and slash vulnerability backlogs? Talk to us today to get started—we'd love to show you how Oligo can unlock value from your security and development teams.

See Oligo in Action