SOLUTION BRIEF

The Business Case for Oligo

The Oligo Application Defense Platform doesn't just give the best visibility in application security—it delivers more value, faster, than any other runtime AppSec solution.

Oligo gives security teams and developers what they need to do their job effectively: real-time visibility and visual, contextual proof about risks and incidents in all their applications, including third-party commercial software.

Driving ROI from the Oligo Application Defense Platform

Security teams using Oligo have fewer "fire drills," quicker incident response times, and maintain visibility over application attacks and reachable vulnerabilities in real time.

Easy Deployment, Scalable, Low TCO

Unlike many other runtime approaches (including RASP), the Oligo Application Defense Platform is simple to deploy and maintain, even at scale.

Oligo Benefits

BY THE NUMBERS

- **Up to 99%** of vulnerabilities deprioritized
- **99%+** reduction in time to detect exploits
- **99.9%+** less time spent validating vulnerabilities
- **10x** faster overall zero-day response & triage
- **100x** faster vulnerability customer assurance

"The most surprising aspect of Oligo for OneTrust was how quickly we were able to get it operational. Oligo told us, it won't take more than a week or two—and it truly didn't!

It's remarkable: I've worked in the industry for over 20 years, and I've seen a number of technologies that say the same thing: *Oh, don't worry about it. It'll be implemented in a very short period of time...* but then it takes forever. So this was one of the best surprises: we were able to operationalize and implement Oligo very quickly, and it delivered value immediately."

Igor Zavulunov
VP of Information Security onetrust

BY THE NUMBERS

Deployment & Maintenance

<14

Days To **Fully Deploy** Across The Environment

<5

Minutes To **Actionable Results** After Deployment

<0.1

FTE To Maintain Oligo Post-Deployment

One Platform, Two Solutions

OLIGO ADR	OLIGO FOCUS
Real-time detection tells you which of your applications may **be under attack right now**—with full, visual proof security teams need to validate and respond to the threat.	**Real-time reachability** tells you what vulnerable libraries and functions are **exposed and exploitable**—with full, visual proof developers need to trust their alerts.
First- and third-party applications (no source code required)	
Identify risks from CVEs, shadow vulnerabilities, and supply chain compromises	
Detect risk in open-source dependencies, OS packages, first-party code	

How Oligo Delivers Value

REAL-WORLD SCENARIO #1

Application Breach

Can you detect an application breach the moment it begins?

Without ADR, an application breach takes an average of 180 days to detect. In that time, attackers exploit resources and steal data, including sensitive personal information or company secrets.

Oligo ADR uses real-time behavioral analysis to identify anomalies in application components. **When anomalies indicating exploitation occur, the Oligo platform instantly alerts security teams with visual proof of the anomalous behavior.**

REAL-WORLD SCENARIO #2

Zero-Day Response

When a new zero-day hits, how fast can you tell your teams—and your customers—that their software is safe?

A typical security team for a mid-sized organization will respond to several zero-day "fire drills" each year. At enterprise organizations, dozens of zero-day vulnerabilities each year may require response and triage. **Oligo instantly detects zero-day exposure *and* exploitation**, so security teams can respond urgently to applications under attack, followed by those with an executed vulnerable function that could be attacked at any time.

Oligo customers praise the platform for making it possible to reassure customers faster about their exposure to zero-day vulnerabilities—**improving customer retention with ultra-fast proof that applications are not under attack or exposed to a threat.**

REAL-WORLD SCENARIO #3

Backlog/Noise Reduction

Does developer pushback cost your team time and credibility?

SCA products produce huge numbers of findings, but since most are unreachable false positives, developers do their best to ignore them. With real-time reachability from Oligo Focus, **Oligo customers can de-prioritize 70-99% of their vulnerabilities as non-reachable.**

Other products on the market use static reachability algorithms that can only generate hypothetical findings that won't be trusted by developers. Oligo uses *real-time* reachability to monitor the behavior of applications at runtime and in production. With Oligo, **developers get visual proof of the vulnerable executed path, cutting vulnerability validation requests by over 99%.**

REAL-WORLD SCENARIO #4

Shadow Vulnerabilities

Can you protect against attackers exploiting unknown threats?

AppSec tools typically only detect known vulnerabilities with a CVE. But what about vulnerabilities that are under dispute, or haven't yet been disclosed or even discovered? When attackers exploit these vulnerabilities, **they've remained totally undetectable—until now.**

Oligo ADR goes beyond CVEs to detect anomalous behavior that indicates an attack in progress, even when attackers exploit disputed or pre-disclosure vulnerabilities. Oligo could detect the XZ Utils backdoor without any rule changes, even before the supply chain compromise was discovered. **With Oligo, once-undetectable attacks now trigger instant security alerts.**

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