Zero Day Response

OLIGO DETECTS EXPLOITABILITY AND INDICATORS OF COMPROMISE

THE CHALLENGE

Detection and Response

Difficult to detect and even harder to prevent, zero-day vulnerabilities - and the exploits that follow - can feel like a **no-win scenario for security teams**. When zero-day vulnerabilities are discovered in commonly used software components that underlie a huge number of applications, understanding the risk picture and minimizing exposure becomes a high-stakes "fire drill" that stops other work from taking place while responders take action.

THE OLIGO SOLUTION

Discover Active Application Exploitation with Oligo

Even before security teams look for which applications are vulnerable to a new zero-day vulnerability, there's a more important question - one which most teams have previously been unable to answer.

What's already being exploited right now?

If attackers are already leveraging a zero-day against your applications, **it's critical to know what's happening immediately.**

The Oligo Application Defense Platform monitors and observes your applications in real time, and detects whenever libraries are behaving unusually versus their baseline behavioral profile. Using information gathered about the new zero-day vulnerability, the Oligo platform can **determine whether any compromise already exists** and help you identify exactly which dependency is vulnerable.

EXPLOIT INSIGHTS

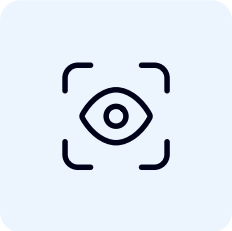
Pinpoint Zero-Day Exploitability with Oligo

Once you've determined that you're not being actively exploited already, the next question on your security teams' mind is: **where is this vulnerability present in our applications - and where can it actually be exploited?**

Typical static scanning tools will simply find every instance of the vulnerable package that exists anywhere in your applications. Many of these findings **(typically 90-99%)** will be "dormant dependencies" that show up as false positives in static scanners, but are never actually loaded or executed at runtime.

The Oligo Application Defense Platform monitors your applications in real time, with visibility into every library and even individual vulnerable functions. Using Oligo, you can see exactly where a **new zero-day vulnerability uses a vulnerable function** that is loaded and executed in your application in the real world - indicating that you are currently exposed to a potential attack.

The Oligo platform can trace back exposed vulnerabilities to their original repository, and can determine whether the exposed vulnerability is contained in a direct or indirect dependency, enabling smarter, faster response that can stop time-consuming "fire drills" by giving security teams all the information they need to guide remediation steps.



ZERO-DAY TRACKING

Track Zero-Day Vulnerabilities In Third-Party Applications

Zero-day risks can come not only from the applications you build internally, but also from the third-party applications your teams buy or use. Without access to source code, **static scanning tools are dead in the water** - totally unable to observe or understand the risks in the third-party applications that your containers depend on.

Oligo **does not require access to source code** in order to monitor and observe applications and their components. If a vulnerable library or function is exposed and exploitable - or being actively exploited - the Oligo platform will alert you and track down the origin of the risky dependency, with proof you can take to your vendor to ensure that they take swift action to remediate.

SWIFT SETUP

Fast Deployment, Valuable Insights

The Oligo Application Defense Platform deploys in **just a few hours**, and can be maintained easily with low technical overhead (<1%) as well as low maintenance requirements (<¼ FTE).

Don't let the next zero-day create havoc for your security teams. With Oligo, you can know exactly **what your exposure is to new zero-days**, even in third-party applications - and identify instantly when applications are already compromised.