June 2026

NAVY SBIR TRANSITION PROGRAM

SPOTLIGHT

Company: ObjectSecurity LLC
Website: www.objectsecurity.com
POC: Ulrich Lang, CEO
Phone: 650-515-3391
Address: 845 15th Street #320
San Diego, California 92101

BinLens: ObjectSecurity delivers cybersecurity capability with applications across military, government

By Matthew Schilling

The U.S. Navy faces a persistent cybersecurity challenge: how to identify vulnerabilities in complex, mission-critical software, often without access to source code and within highly restricted, air-gapped environments. Traditional tools fall short. Some, like static analysis and software bill of materials (SBOM) approaches, are fast but noisy, or are limited to already-published vulnerabilities. Others, like fuzzing, can uncover deeper issues but require significant time, resources, and manual effort, sometimes running for weeks without clear results.

ObjectSecurity LLC is helping to close that gap with BinLens, a binary vulnerability analysis tool that enables faster, deeper, and more actionable insights into software risk. Founded in 2009 in San Diego, ObjectSecurity specializes in high-assurance cybersecurity technology for complex and embedded environments.

Developed through several Small Business Innovation Research Program (SBIR) contracts, starting with a Phase I from the Office of Naval Research in 2018, BinLens allows analysts to identify critical vulnerabilities, including previously unknown, or "zero-day" threats, directly within compiled software.

ObjectSecurity has navigated the SBIR "valley of death," matured BinLens to technology readiness level 9, and successfully transitioned into critical defense applications. In January 2026 the Naval Air Warfare Center Aircraft Division (NAWCAD) awarded ObjectSecurity a five-year contract for a license of BinLens.

Photo credit: Petty Officer 2nd Class Malachi Lakey

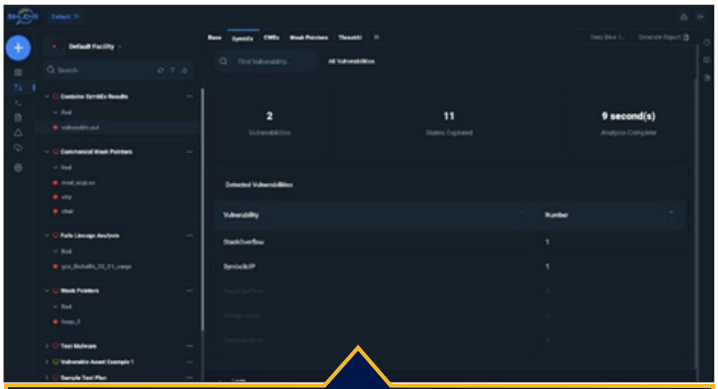
Naval and other military systems run on complex, compiled binaries with specialized cybersecurity demands.

At the core of BinLens is a technique called symbolic execution, a binary vulnerability testing technique that assigns symbolic values to various inputs. These symbolic values highlight which inputs cause different parts of a program to execute and enable analysts to more easily track software's constraints and vulnerabilities. ObjectSecurity CEO Ulrich Lang calls it a form of "fancy math" that automatically evaluates what happens to multiple combinations of values in the binary.

Rather than testing inputs one by one, as fuzzing does, or relying on known vulnerability signatures, BinLens analyzes how entire ranges of inputs behave within a program. The result is

a more efficient path to identifying high-impact vulnerabilities, with significantly fewer false positives.

"What sets our product apart is that it is orders of magnitude faster than fuzzing," Lang explains, "and when we do find something with the symbolic execution tool, there's a much higher probability it's a legitimate vulnerability compared to conventional static analysis."



The BinLens dashboard shows symbolic execution toolkit and vulnerability assessment results.

BinLens' increased visibility into vulnerabilities, compliance issues, and hidden behaviors allows its users to better understand and manage risk across mission-critical systems, but to better understand BinLens, it is helpful to look back at its beginnings.

At its inception, BinLens was known under its SBIR topic title RedBox: Red team in a Box. In software testing, a "red team" refers to a group acting as a simulated adversary, seeking potential vulnerabilities or security risks. Redbox was originally conceived to automate and streamline this process under the constraints of complex, compiled binaries.

In addition to its depth and efficiency, BinLens stands out for its ability to automatically detect novel threats and maintain a low false positive rate. Traditional cybersecurity programs often rely on known indicators, essentially digital wanted posters to identify vulnerabilities. While effective for known threats, this approach cannot detect novel vulnerabilities such as zero-day exploits.

Symbolic execution enables BinLens to detect zero-day vulnerabilities because it conducts analysis without relying on external databases of known threats. This independence is crucial for military systems that rely on proprietary or classified code.

Existing vulnerability detection methods can also resemble finding a needle in a haystack. As Lang explained, "The bulk of tools today just flag anything that may or may not be an actual vulnerability. You don't have time to look through 5,000 things and figure out which ones are real and high impact." That high volume noise often results in high numbers of false positives.

The speed, accuracy, and efficiency of BinLens — especially when compared to fuzzing approaches — help explain why multiple military agencies have already invested in the technology, with more adoption likely in the next few years.

Thanks in part to COVID-19 relief funding, ObjectSecurity developed a Redbox prototype and provided it to the Navy for evaluation. Internal testing verified a consistent capability for detecting vulnerabilities within the Navy's uniquely challenging binary ecosystem. Following the success of the RedBox SBIR prototype in 2021, ObjectSecurity commercialized the capability into the BinLens product.

In Naval applications, BinLens primarily supports aviation cybersecurity and automated vulnerability assessment. However, the Defense Advanced Research Projects Agency (DARPA), the Defense Threat Reduction Agency (DTRA) and the U.S. Army all recognized additional potential for the technology, with each agency awarding ObjectSecurity SBIR contracts in 2022-2024.

DARPA seeks to use BinLens to enable third parties to confirm that embedded software performs its intended functions safely and reliably. The U.S. Army sees potential for enhancing the cybersecurity of Army vehicular systems, and DTRA is testing BinLens capabilities in development, security, and operations (DevSecOps) and data management.

Throughout the process ObjectSecurity has benefited from support provided by the Navy SBIR Transition Program (Navy STP). Lang highlighted the program's role in helping the company navigate the decentralized nature of government opportunities and identify relevant points of contact.

"One of the big issues we face is the decentralized nature of how information from the government is distributed," Lang said. "The weekly tracker Navy STP sends out has been very useful in finding opportunities that are actually relevant." Market Research Analysis Reports also provided valuable insight and access to potential customers, helping ObjectSecurity connect with stakeholders across the military.

Looking ahead, ObjectSecurity continues to enhance BinLens with new capabilities, including agentic artificial intelligence features designed to further support cyber operations. These include a large language model to drive analysis and a chatbot feature that allows users to analyze results with ease.

These advancements enable more intuitive, conversational interaction with the platform while supporting automated orchestration of complex analysis workflows. By reducing analyst workload and accelerating vulnerability discovery, these capabilities are intended to act as a force multiplier for military cyber teams.

As cyber threats continue to evolve, the ability to perform deep binary analysis in a timely manner will remain critical to keeping the Navy's fleet and other military systems secure and mission ready. Through BinLens, ObjectSecurity provides the Navy and other users with a powerful capability to improve software assurance, reduce cyber risk, and support mission readiness around the globe in some of the most challenging operational environments.

For more information on ObjectSecurity and BinLens, visit https://objectsecurity.com/binlens/.