Automated Vulnerability Detection and AI Model Hardening

for Mission-Critical Environments

DISA TEM Presentation - May 1, 2025

Agenda

- ObjectSecurity Company Introduction
- FortiLayer™ Introduction and Technical Demo
- BinLens™ Overview and Technical Demo
- Open Discussion and Q&A

Intro to Our Team

Ulrich Lang, PhD – Founder and CEO

Trevor Thomas – Lead Software Engineer

Stephen Brennan – AI/ML Researcher

Connor Forman – DoD Account Manager

ObjectSecurity Company Overview

We provide precision vulnerability detection for defense and critical infrastructure.

- Founded in 2000 (Dr. Lang PhD spinout UK, US 2009).
- R&D tech/product dev. $10M+ gov't R&D funded, numerous patents, awards…
- For more than 20 years we've pioneered successes with DARPA, Office of Naval Research, and other DOD organizations in the following fields:

Binary Vulnerability Analysis	AI/ML Trust Analysis	5G Vulnerability Analysis	Supply Chain Risk Analysis	Zero Trust Access Policy Automation

BinLens™ 3.2
DARPA and ONR SBIR development

FortiLayer™
USAF Phase II SBIR development

ObjectSecurity
Secure technology

FortiLayer – Safeguards Your AI Models

- **Automate** deep security analysis of AI models to identify vulnerabilities and mitigate risks
- **Optimize** fine-tuning of models by enhancing accuracy and training speed, reducing time to deployment
- **Rigorous** performance, sensitivity, and robustness testing of AI/ML models
- **Rapid patching** of models to improve accuracy and mitigate security issues efficiently
- **Layer-wise** deep understanding of model internals and behavior with explainability analysis

Results from layer-level model performance analysis.

Object Security
Secure technology

FortiLayer – Optimizes AI Performance

Performance 	Identifies specific architectural or pipeline-level slowdowns in training or inference
	Pinpoints performance choke points that could degrade real-time decision-making or lead to mission delays
Accuracy 	Evaluates how well the AI system meets its intended performance goals using standardized benchmarks
	Ensures models used in mission-critical systems deliver reliable results under expected conditions (i.e. testing against custom datasets)
Security 	Tests resilience to unexpected, noisy, or malicious inputs (e.g. adversarial attacks, edge cases)
	Highlights model architectural weaknesses for targeted correction

Object Security
Secure technology

FortiLayer – Builds Trustworthy AI

IP Compliance	Scans for copyright, license, and provenance metadata across source code, datasets, and trained models
	Ensures compliance with open-source and proprietary content — reducing legal and supply chain risk in acquisitions or third-party reuse
Explainability	Provides transparency into how the model makes decisions
	Includes saliency maps, weak neuron analysis, and overfitting detection
Compliance	Maps analysis results to compliance frameworks (e.g., NIST RMF, MITRE ATLAS)
	Automatically generates reports for tracking dataset usage, model compliance scoring etc. for documentation

Object Security
Secure technology

Demo

BinLens™ – Automate. Detect. Secure.

- BinLens helps vulnerability researchers, product security teams, and device buyers who need to find **unpublished, potential zero-day vulnerabilities** in binary code at a low-cost point.

- Automates key manual reverse engineering tasks like **symbolic execution**, disassembly, and decompilation to find potential vulnerabilities. Unlike traditional tools, it doesn't rely solely on known vulnerabilities (i.e. CVEs)

- Offers flexible deployment options for installation in air-gapped on-prem or cloud-based instances

Object Security
Secure technology

Why Symbolic Execution Matters

- BinLens employs **symbolic execution** to explore, detect, and report vulnerable program states.

- Evaluate the behavior of the binary program, detecting memory safety violations and other undefined behaviors with a level of precision traditional tools cannot match.

BinLens outperforms solutions that:

- require source code to detect vulnerabilities
- only scan network traffic
- detect known, published vulnerabilities
- needs connectivity to internet, cannot be used by Defense or Intel Agencies
- produce high false-positive rates
- are manual/expensive/slow

Object Security
Secure technology

BinLens – Operational Benefits

Risk Reduction

Identifies *unpublished* vulnerabilities (zero-days) in compiled binaries — not just known CVEs

Traditional tools rely on SBOMs and known-vuln databases; BinLens detects novel logic flaws and misuses the static tools aren't designed to catch

Impact: Reduces operational risk from inherited third-party or contractor-supplied software/firmware

Time Savings

Automates deep binary analysis that would take hours or days manually

Symbolic execution replaces the need for manual reverse engineering

Typical findings surface in minutes-to-hours versus days

Impact: Faster triage and decision-making for red teams, ATO approvals, and procurement teams validating vendor software

Object Security
Secure technology

BinLens – Resource Optimization

Lower Analyst Effort

- Low false-positives, automatically prioritizes and explains issues at the function-level
- No need to correlate raw disassembly with vulnerability patterns
- Clear outputs: CWE tags, function call chains, paths to execution
- **Impact:** Less time spent by analysts reviewing noise or duplicating work across teams

Cost Efficiency

- Reduces need for highly specialized reverse engineering talent on every project
- Enables junior analysts or generalists to perform deeper assessments
- Reduces over-reliance on scarce, expensive SME hours
- **Impact:** Greater capability without growing the headcount or expensive Pen Test contracts

Object Security
Secure technology

BinLens – Enterprise Readiness

Operational Integration 	API integration into existing CI/CD pipelines seamlessly
	Works with air-gapped or classified systems
	Exports to Ghidra, Splunk, dashboards, JSON for ticketing
	Impact: Analysis becomes part of the process, not a one-off
Scalable Use 	Supports many architectures — from embedded firmware to complex ELF/PE applications
	No source code required, can be used across different mission environments (ground, air, space, or maritime systems)
	Impact: Broad applicability without major customization per platform
Compliance & Governance 	Helps teams meet latest NIST guidance, software supply chain mandates, and supports SBOM validation
	Supports mission-critical software assurance and ATO documentation
	Impact: Easier to pass audits and support Red Team reviews, while maintaining accountability and security for inherited code

Object Security
Secure technology

Demo

Key Takeaways

FortiLayer

BINLENS

Build trust into AI Models

- Identify vulnerabilities and performance bottlenecks in AI models
- Accelerate safe deployment with explainability, accuracy, and IP compliance

Secure binaries without source code

- Detect unpublished vulnerabilities in firmware and binaries, automate deep reverse engineering with symbolic execution
- Support Red Teams, DevSecOps and CI/CD pipelines, and Threat Hunters operating across security levels
- Available on Tradewinds and Platform One Solutions Marketplaces today

Object Security
Secure technology

Thank You

Trevor Thomas
trevor@objectsecurity.com

Stephen Brennan
stephen@objectsecurity.com

Connor Forman
connor@objectsecurity.com

For more information, please connect with us at: objectsecurity.com/contact