oxsecurity

The OX Active ASPM Platform

See Everything. Focus on What Matters. Mitigate Risk at Scale.

As the pace of application development continues to get faster, the necessity to proactively detect and mitigate security threats at every phase of the development cycle becomes essential. Despite the implementation of AppSec measures, security and development teams have grown frustrated by the lack of visibility and manual processes associated with the fragmented collections of tools commonly used today.

The OX Active ASPM platform addresses these frustrations by delivering comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. It also empowers organizations to take the first step toward eliminating manual AppSec practices while confidently enabling scalable and secure development.

The platform helps security and development teams to:

Obtain **complete coverage** and bridge security gaps with flexible scanning options, providing continuous visibility across source control, CI/CD, registry, and cloud environments.

Monitor vulnerabilities in real-time with our proprietary Pipeline Bill of Materials (PBOM), which tracks software lineage from inception to release.

Efficiently **prioritize risk** based on threat, environment, and business context and improve mean response time by continuously targeting the top 5% most critical vulnerabilities.

Prevent risk at scale and intercept security issues before reaching production by **automating response** and **remediation efforts** with no-code workflows.

Go beyond compliance requirements to ensure you're proactively identifying and addressing security gaps during development, not just checking compliance boxes.

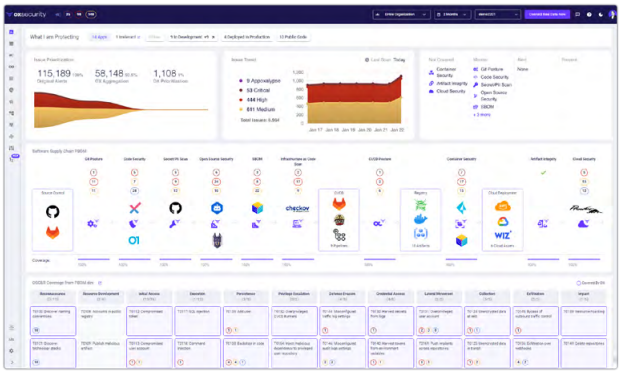
Supported Use Cases

- Application Security Posture Management
- Single Source of Truth
- Software Supply Chain Security
- Shift Left
- Repo & CI/CD Posture
- CI/CD Workflow (Automated Response)
- Production Integrity
- Maturity Assessment, Compliance & SBOM

INTERESTED IN LEARNING MORE? VISIT: WWW.OX.SECURITY/BOOK-A-DEMO/

Beyond ASPM – A Comprehensive AppSec Platform

FEATURES INCLUDE:



Continuous End-to-End Coverage: Native scanners seamlessly integrate with commercial tools or the user's source control, CI/CD, registry, and cloud environments, reducing the need for manual oversight and analysis, and eliminating the need for multiple tools that may result in coverage gaps and technical debt.

Attack Path Analysis: Comprehensive attack path analysis enables users to visualize and quickly address security concerns from a single screen, significantly speeding up response time and improving efficiency in managing security tasks.

Contextualized Prioritization: Effectively assess exploitability, reachability, and impact while reducing noise by over 95%. OX priortization provides comprehensive Dockerfile insights, including SBOM, SCA, and plaintext secrets detection in code, containers, and logs. Users also benefit from detailed open-source security analysis, advanced taint analysis, and data flow.

Pipeline Bill of Materials (PBOM): Tracks code, pipelines, artifacts, container images, runtime assets, and applications. In addition to standard SBOM capabilities, PBOM ensures the integrity of every build, verifies that all apps in production are secure, and minimizes the attack surface.

No-Code Workflows: Simplifies remediation with a drag-and-drop interface, automates ticketing and notifications, and enforces policies to maintain security in production. OX goes beyond automation, enabling you to respond to emerging risks quickly.

OSC&R: Our proprietary OSC&R framework, developed in collaboration with experts from Google, Microsoft, and GitLab, provides a comprehensive model to understand software supply chain risks. Focused on critical attacker techniques and behaviors, this ATT&CK-like open framework helps security and development teams contextualize risk and stay abreast of the latest attack trends.

OX Security
Active ASPM Platform