OX Security: Scanning Public Images

Unmask hidden risks in your software supply chain.

Public Image Security

Public container images are widely used in cloud-native development but introduce unmanaged risks into the software supply chain.

OX Security's **Scanning Public Images** feature identifies images in use across clusters and registries, scans them for vulnerabilities, and enriches findings with metadata such as provenance, integrity, and usage.

Unlike registry-only tools, OX extracts image data directly from the deployment environment. Vulnerabilities tied to each image are consolidated into a single issue, reducing noise and supporting faster remediation.

Key Capabilities:

Comprehensive Discovery

Identifies public container images across Kubernetes clusters, registries, and runtime environments to eliminate blind spots.

Contextual Risk Intelligence

Provides metadata on provenance, trust indicators, usage, and integrity validation to prioritize risk effectively.

One Image. One Issue. One Fix.

Consolidates vulnerabilities across scans into a single actionable issue per image—reducing alert fatigue and streamlining remediation.

Artifact Integrity Monitoring

Flags unknown or unverified images running in the environment.

Seamless Workflow Integration

Surfaces Issues, SBOM data, and artifacts that are then aggregated and correlated in the OX platform for unified tracking.

How It Works

OX Security connects to your cloud-native environment and extracts container image data—including image names, tags, and hashes—from where they are defined and deployed.

Public images are scanned through a specialized process that not only detects vulnerabilities but also enriches findings with:

- **Vulnerability detection**
- **Provenance classification** (official, verified publisher, sponsored OSS)
- **Integrity validation** (expected vs. actual SHA)
- **Popularity and usage data** (stars, pull counts)
- **Full profile details** (tags, versions, publish dates)

The results are consolidated into one issue per image, thereby minimizing alert duplication, improving accuracy, and accelerating risk remediation.

Use Cases

Secure Cloud-native Development:

Ensure base images and dependencies aren't introducing hidden risks.

Accelerate Remediation:

Upgrade one image instead of chasing dozens of fragmented alerts.

Enforce Supply Chain Integrity:

Detect tampered, outdated, or malicious images before they run.

Governance and Compliance:

Maintain complete visibility into open-source and third-party code components.

Designed for Real AppSec Teams

Security and development teams face a shared problem: public images fall between ownership lines. Developers pull them, security can't always track them, and no one has full visibility. With OX, Dev and AppSec teams can work better together to:

- Make public image security a priority
- Consolidate findings to reduce triage effort
- Quickly identify clear, singular remediation paths
- Eliminate the "assumed safe" mindset that increases organizational risk

The results are consolidated into one issue per image, thereby minimizing alert duplication, improving accuracy, and accelerating risk remediation.

Why OX's Public Image Scanning Stands Apart

Unlike siloed tools that only scan registries or runtime, OX delivers:

- Environment-based detection, not just registry scans
- Metadata enrichment for improved prioritization
- Single consolidated issue per image
- Integration into OX's unified AppSec workflows

The results are consolidated into one issue per image, thereby minimizing alert duplication, improving accuracy, and accelerating risk remediation.

About OX Security

For AppSec and development teams that struggle with wasted resources caused by generic prioritization of security issues, OX Security is the only unified application security posture management (ASPM) platform that leverages proprietary Code Projection technology. Code projection dynamically and accurately prioritizes risks based on reachability, exploitability, and real-world impact.

Unlike traditional tools that rely on static data and generic prioritization, OX Security projects code into runtime context, enabling deep, evidence-based insights from design to runtime. This ensures teams focus only on the critical 5% of risks that matter, eliminating 95% of irrelevant issues, improving collaboration, and reducing costly runtime fixes.