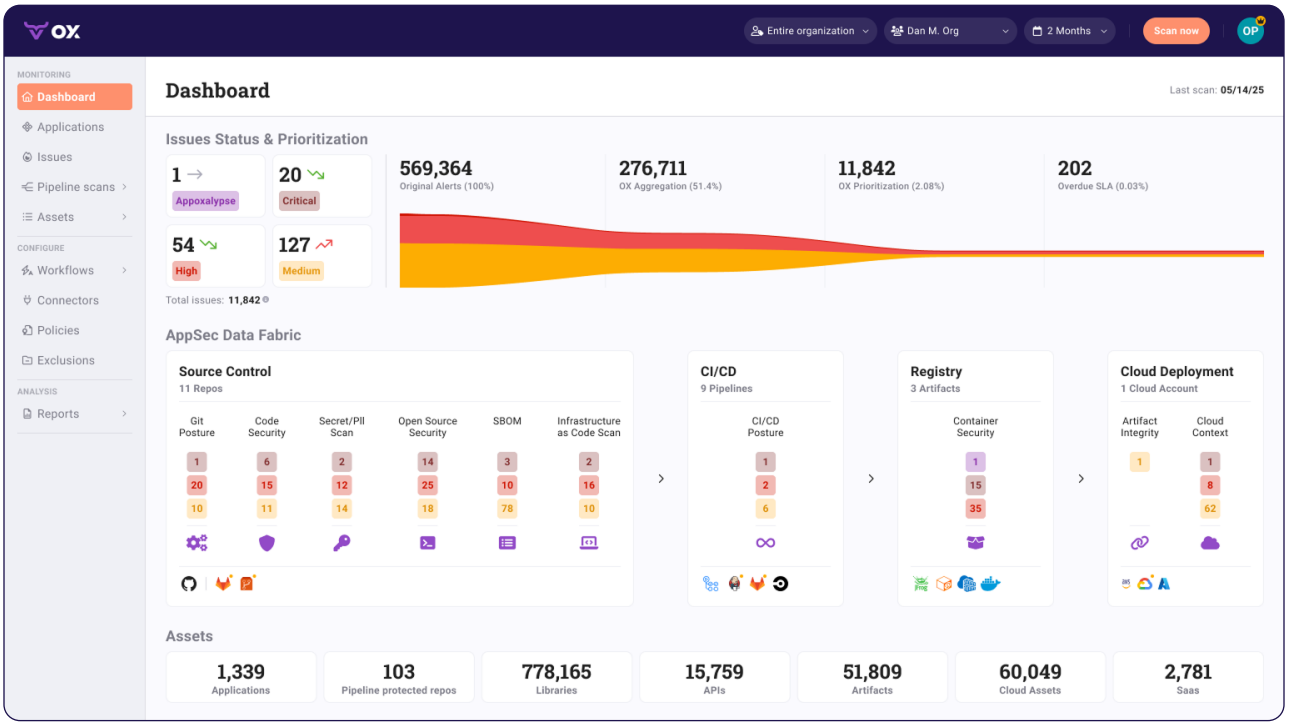
There's no platform that has more features for application security practitioners than OX. Their product provides every kind of scanner, asset mapping, and integration that a team could want. Most recently they also announced VibeSec, a collection of tools for bringing security policies and cloud context into AI coding tools. Whether you're using OX to ingest third party vulnerability findings to layer in code to cloud visibility, or as an all-in-one application security testing solution, OX has the use case covered.

OX offers deep integrations across your application security stack, monitoring code from developer IDE out to production. They offer every kind of application security scanning, mapping findings out to their deployed state, and prioritizing based on numerous details about the finding itself and the runtime environment.



Prioritization is where OX's feature set really shines, using details such as what databases you're using alongside AI exploitation simulation in order to determine the priority of patching a finding. For cloud security teams, OX also provides agentless cloud asset scanning, vulnerability management, and CSPM scanning. OX extends additional runtime context through integrations with dedicated CADR providers, allowing even more robust prioritization insights.

The Benefits of OX

Vibe Code with Context

OX embeds security context - runtime, infrastructure, and policies - into AI coding environments, preventing vulnerabilities from being generated.

Secure Your Entire Stack

OX provides every scanner and integration an application security team needs to ensure the entire environment is covered.

Map Your Application to Deployment

OX maps pieces of code through to their containers and running APIs to enable accurate prioritization and remediation.