

Xygeni Strengths vs. Competitors



Xygeni Differentiators

End-to-End Application Security

Xygeni delivers full coverage across the entire Software Development Lifecycle (SDLC). Unlike solutions that stop at vulnerability detection, our platform extends into identifying **malware across every SDLC phase**, including application code, third-party packages, container images, pipelines, IaC, configuration files, processes, and other critical assets. This enables proper end-to-end protection, eliminating blind spots competitors often leave unaddressed.

Xygeni MEW (Malware Early Warning)

The platform includes this exclusive system capable of detecting **malicious packages in real time**, offering a level of preventive protection rarely found in other application security technologies.

CI/CD Security

Protecting **Continuous Integration / Continuous Delivery (CI/CD)** environments is a core pillar of Xygeni, since modern pipelines have become prime attack vectors. As organizations accelerate their development cycles, pipelines, tools, plugins, and CI/CD systems become critical exposure points, ranging from **insecure pipeline configurations** and **exposed repository credentials to malicious dependencies or plugins** integrated without proper verification. CI/CD orchestration tools can also be vulnerable to privilege escalation, code injection, or excessive-permission abuse, which amplifies risk.

Higher-precision SAST (Static Application Security Testing)

Our technology delivers a **much lower false-positive rate** than competitors, allowing teams to focus on real vulnerabilities and save resources. Accuracy ensures remediation efforts are efficient and relevant. Beyond vulnerability detection (OWASP Top 10 and more), Xygeni's SAST can detect malicious code within application code, one of the few SAST solutions worldwide with this capability.

Advanced SCA (Software Composition Analysis)

Xygeni provides differentiators such as **remediation risk** scoring, **breaking-change** identification, and analysis of critical metrics like **reachability** and **exploitability**. This results in **sharper prioritization** and better-informed risk-management decisions.

Advanced secrets management across the SDLC

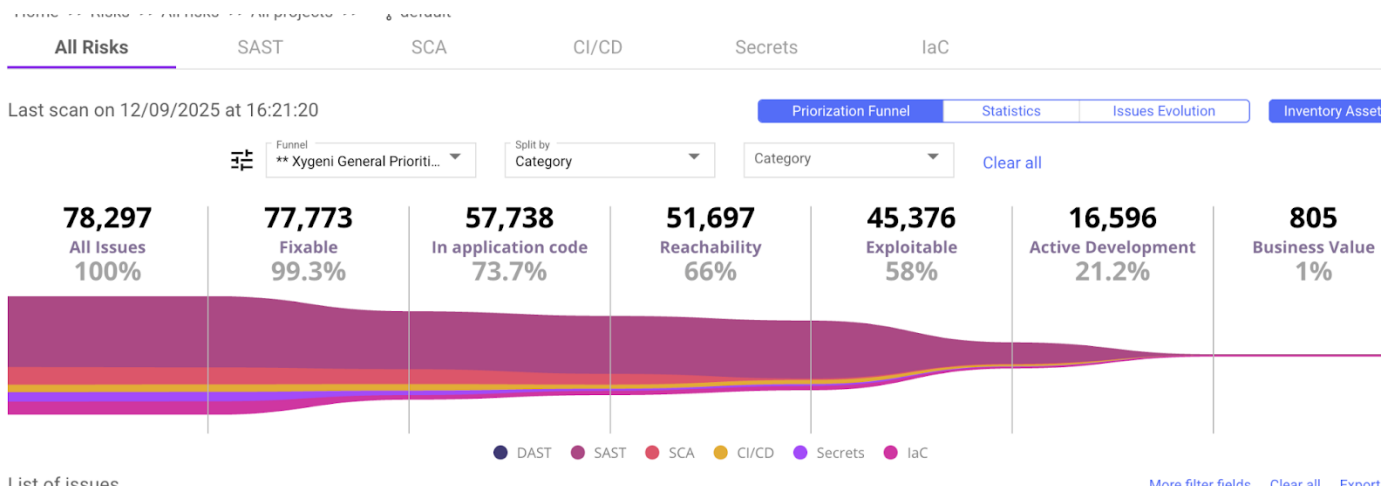
Unlike most solutions that only detect exposed secrets in certain phases or formats, **Xygeni uniquely identifies secrets at any point in the SDLC** and in **any file type or repository**, ensuring complete coverage of this critical risk. Beyond detection, the platform offers a standout capability: **automatic verification and revocation of compromised secrets**, immediately eliminating misuse risk and drastically reducing exposure time. This not only prevents leaks of credentials, API keys, or certificates, but also ensures an **automated, effective response**, integrating with identity and access management systems to protect the software supply chain end-to-end.

Anomaly Detection

The platform features an advanced system that identifies **unusual behavior** patterns across users, assets, or pipelines. This predictive approach boosts the ability to detect intrusion attempts, misuse, or uncatalogued risks, increasing resilience to unknown threats.

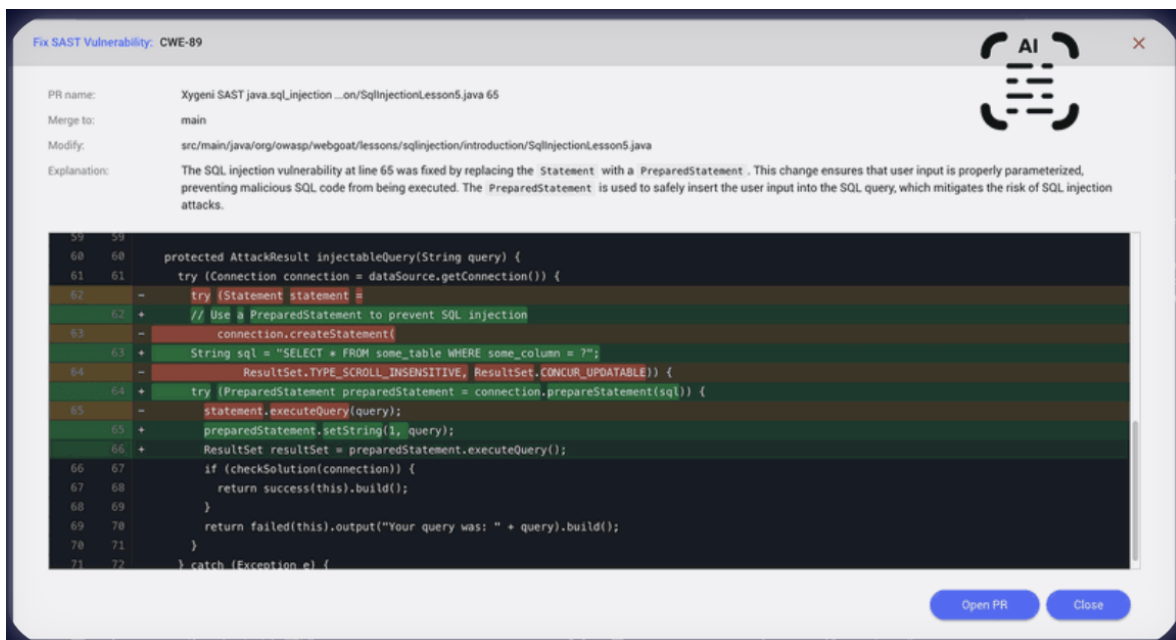
Intelligent, Customizable Prioritization

Xygeni lets each organization configure a fully adaptable risk-prioritization system. This ensures efforts focus on the issues with the **highest business impact**.



AI-Assisted Auto-Remediation

The platform enables **automatic remediation** across SAST, SCA, secrets management, and other critical vectors using AI. It also includes an **auto-remediation bot** that speeds response, reduces exposure time, and minimizes the operational load on security and development teams.

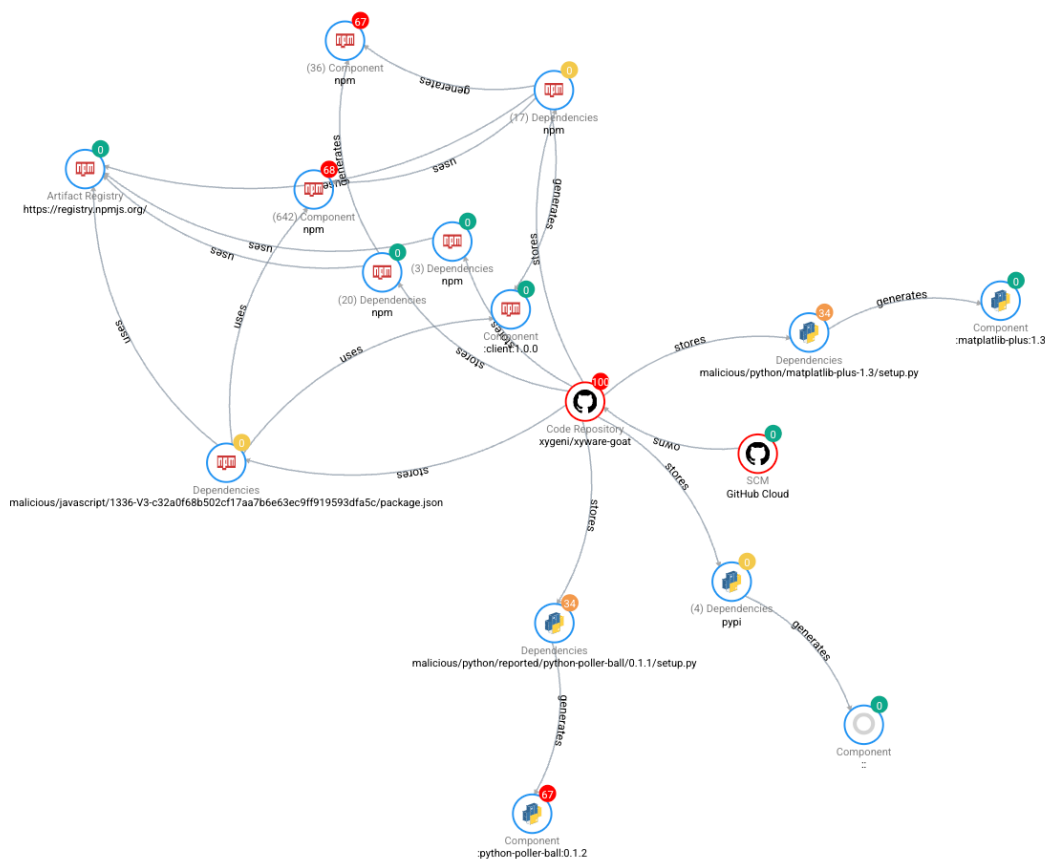


Map of all Assets Across the Software Lifecycle

Xygeni provides an **exhaustive map of all assets across the software lifecycle, delivering complete visibility and control over the organization's technology landscape. Unlike solutions that only monitor source code or dependencies, our platform extends visibility to every component of the development ecosystem, enabling broader, more accurate risk detection.** This includes:

- **Code repositories**, both public and private, may contain accidental vulnerabilities, insecure configurations, or exposed secrets.
- **Software components and external libraries** are a major attack vector due to inherited vulnerabilities or malicious dependencies.
- **CI/CD pipelines**, which orchestrate build and deployment and, if compromised, allow attackers to inject malicious code into the supply chain.
- **Plugins and extensions**, which if not rigorously controlled, can become backdoors or malware vectors within the development ecosystem.
- **Integration and orchestration tools** (e.g., Jenkins, GitHub Actions, GitLab CI, Azure DevOps) which require careful management of configurations, permissions, and secrets to prevent abuse and privilege escalation.
- **Users and service accounts** have their activity logged in detail, allowing for the identification of who introduced a security issue, when, and in what context.

Thanks to this total visibility, Xygeni not only provides an up-to-date, centralized asset inventory, but also enables early anomaly detection and the application of security policies tailored to each SDLC element, strengthening resilience across the entire supply chain.



Detailed audit log

The solution maintains a **complete, transparent history** of assets and users, precisely identifying who introduced a security issue, when, and where in the process. This ensures traceability, individual accountability, and regulatory compliance.

Pioneering, award-winning ASPM (Application Security Posture Management)

Xygeni is internationally recognized as a pioneer in **ASPM**, having received several global awards for the platform's advanced capabilities. Unlike solutions that fragment security information, Xygeni offers a **unified visualization layer from code to cloud**, enabling a 360° view of the entire application ecosystem. The platform not only centralizes its own security findings, but also **ingests data from other AppSec tools**, correlates it, and presents it in a single, integrated dashboard. Application security thus becomes a **cohesive, prioritized, intelligible system** for both technical and business teams. Beyond global risk visibility, Xygeni includes differentiators such as **intelligent vulnerability prioritization** and **automatic remediation of findings ingested from external tools**, maximizing efficiency and enabling rapid, precise action against threats.

Build Security

A solution designed to **protect the software build process** within CI/CD pipelines, ensuring integrity, traceability, and trust in generated artifacts. The platform collects and verifies, in real time, all build evidence, from source code, dependencies, and configurations to security reports and final artifacts, using cryptographic signatures and automatic attestations aligned with standards like **SLSA**. This ensures no component has been tampered with; the solution can even **detect attempts to use modified (tampered) artifacts**, introducing gates that block delivery if alterations are detected, and securely storing all proofs and records for future audits.

Code privacy and deployment flexibility

A standout advantage of Xygeni's SaaS platform is that it **does not require uploading source code to the cloud** to perform security analysis. All inspections and analyses **run locally**, guaranteeing complete code confidentiality and eliminating risks associated with transferring or storing code in third-party environments. The only data sent to the cloud are **encrypted security results**, i.e., detected vulnerabilities, reinforcing privacy and IP protection. Additionally, for organizations that require complete infrastructure control due to internal policy or regulation, **Xygeni also offers an on-premises version**, providing the same functional coverage deployed within the customer's own environment. This SaaS/On-Prem duality offers maximum adoption flexibility, adapting to diverse security and compliance requirements.