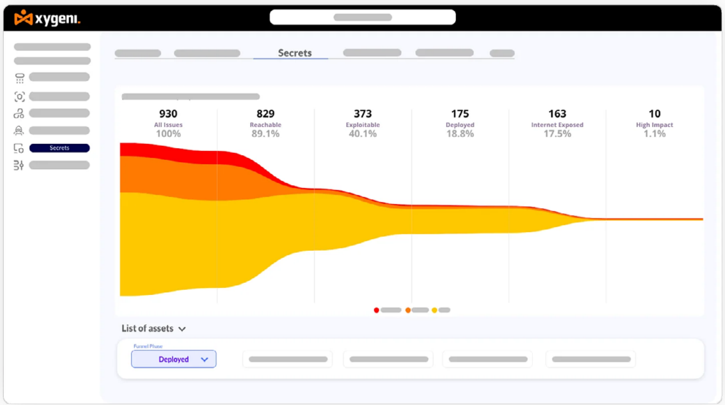
SCA - Open Source Security

Solution Brief

Modern SCA with Reachability, [Auto] Remediation and Malware Early Warning

Minimize risks and protect your applications with Xygeni Early Malware Detection. Focus on exploitable vulnerabilities with reachability analysis and reduce false positives. Our real-time monitoring detects and mitigates threats in your dependencies before they impact your software.



About Xygeni

Xygeni specializes in enhancing software development security and efficiency with our Application Security Posture Management (ASPM) platform. We offer complete control over application risks, a unified security view from code to cloud, and eliminate noise to prioritize risks effectively. Our advanced malware detection and early warning system makes Xygeni a leader in protecting applications from emerging threats, ensuring rapid and secure software delivery.

Recent reports reveal that nearly three-quarters of codebases now contain high-risk open-source components. **Vulnerabilities have soared from 48% to 74% in just one year.** Even more concerning, 91% of these components are at least 10 versions outdated, significantly heightening security risks. The rise of malicious open-source packages has been meteoric, with growth rates exceeding 300% year-over-year, resulting in over 245K malicious packages detected in 2023. It's time to take action!

Xygeni's Software Composition Analysis (SCA) goes beyond basic vulnerability detection by introducing reachability and exploitability analysis to help you focus on what truly matters. While other tools overwhelm teams with alerts, Xygeni prioritizes vulnerabilities based on actual impact, ensuring your team spends less time chasing false positives.

With auto-remediation, Xygeni reduces the time and effort required to secure your software. Automatically generate pull requests with fixes for known vulnerabilities, accelerating your remediation process and keeping your projects safe and compliant.

Our real-time monitoring spans multiple public registries, ensuring all dependencies are continuously scanned and verified for safety and integrity—giving you full visibility and control over your open-source software supply chain.

700K malicious packages detected last year

Open Source Security

Solution Brief

Advanced Detection of Risky Dependencies and Vulnerabilities

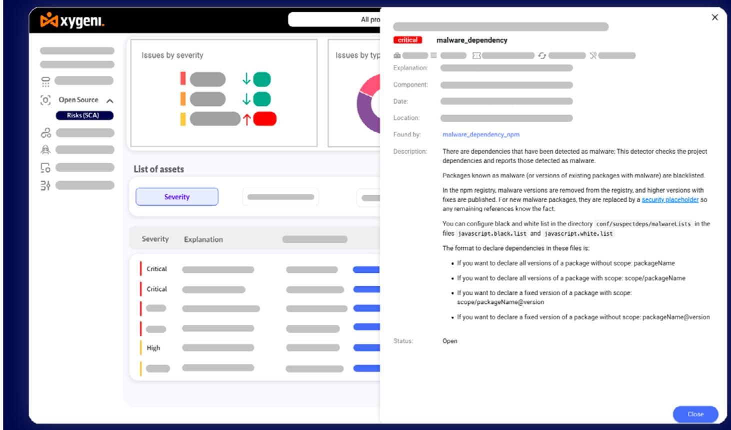
Xygeni's Suspect Dependencies Scanner helps detect and mitigate supply chain attacks by identifying risks like typosquatting, dependency confusion, and suspicious installation scripts. By analyzing the dependency graph, Xygeni ensures your software remains protected from compromised components.

When a dependency is flagged as suspicious, Xygeni provides detailed remediation strategies, including version pinning, whitelisting, and blocking risky scripts, preventing threats from infiltrating your projects.

Overview of Supported Risky Dependency Detectors

Xygeni's scanners offer comprehensive detection across multiple ecosystems, allowing security teams to identify and respond to evolving threats with precision.

Types of Suspect Dependency Detector



critical malware_dependency

Explanation:

Component:

Date:

Location:

Found by: malware_dependency_npm

Description: There are dependencies that have been detected as malware; This detector checks the project dependencies and reports those detected as malware.

Packages known as malware (or versions of existing packages with malware) are blacklisted.

In the npm registry, malware versions are removed from the registry, and higher versions with fixes are published. For new malware packages, they are replaced by a security placeholder so any remaining references know the fact.

You can configure black and white list in the directory `conf/suspectdeps/malwareLists` in the files `javascript.black.list` and `javascript.white.list`

The format to declare dependencies in these files is:

- If you want to declare all versions of a package without scope: packageName
- If you want to declare all versions of a package with scope: scope/packageName
- If you want to declare a fixed version of a package with scope: scope/packageName@version
- If you want to declare a fixed version of a package without scope: packageName@version

Status: Open

- **Anomalous Dependencies:** Detects unusual dependencies that may indicate security risks.
- **Dependency Confusion:** Identifies internal package names that could be mistaken for public repository versions.
- **Known Vulnerabilities:** Flags dependencies with documented security flaws. Xygeni integrates databases such as NVD, OSV, Github advisory and others.
- **Malware:** Detects dependencies containing known malware threats.
- **Suspicious Scripts:** Identifies scripts that may execute unauthorized or harmful actions.
- **Typosquatting:** Catches malicious packages with deceptively similar names.
- **Unscoped Internal Components:** Flags unscoped NPM components at risk of public exposure.

Simplify Open Source Licensing

Xygeni scans and assesses licenses to prevent legal issues and ensure compliance with policies and regulations, so you can use open-source software with confidence.

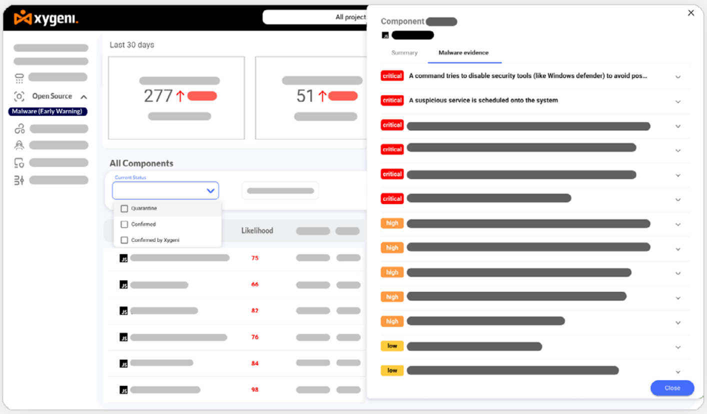
Keep Your Software Updated and Secure

Xygeni monitors and flags outdated components, ensuring you run the most secure versions to reduce risks and improve performance.

Malware Early Detection, Blocking, and Notification

As soon as new packages are published, Xygeni conducts a real-time scan to detect and block malware based on code behavior analysis, alleviating the need for extensive and urgent post-build remediation. Our systematic process sounds like this:

1. Continuous Scanning:



critical A command tries to disable security tools (like Windows defender) to avoid pos...

critical A suspicious service is scheduled onto the system

- **Public Registries Monitored:** The service continuously scans multiple public registries like NPM, Maven, PyPI, etc.
- **Immediate Notification to Affected Users:** As soon as a potential threat is detected, the system immediately notifies the affected users, enabling rapid response to mitigate risks. Notifications can be raised through standard Xygeni mechanisms such as email, messaging platforms, and webhooks.

2. Quarantine:

- Automatic Blocking of Zero-Day Malware: Upon detection, suspicious packages are automatically quarantined. The customer can use this information to implement guardrails in their CI/CD to prevent the packages from entering the development environment or the broader software supply chain.

3. Review and Confirmation:

- Code Review by Security Researchers: A security research team reviews the quarantined package to verify the threat.
- Confirmation by Public Registry: If confirmed by our internal team, we communicate it to the public registry, which should confirm the finding and validate the threat level and the nature of the malware or vulnerability.

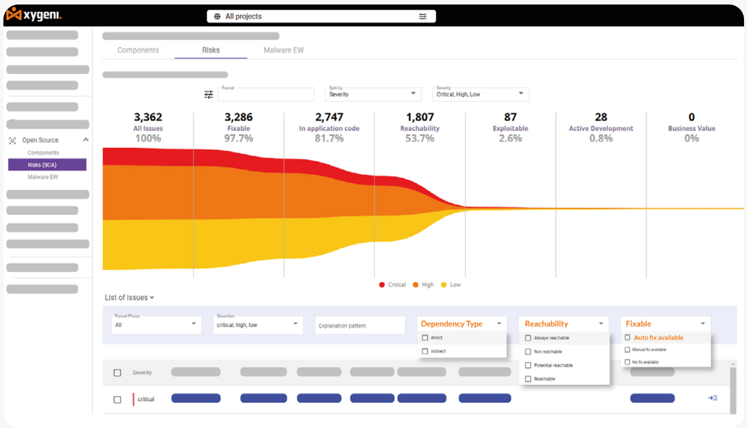
4. Disposal and Public Disclosure:

- Disposal: Once a threat is confirmed, the appropriate measures are taken to dispose of the threat safely, ensuring it does not re-enter the ecosystem.
- Public Disclosure: The usual details about the malware and its disposal are publicly disclosed through the product, Xygeni blog, or the package registry to inform the wider community and prevent further spread.

Open Source Security

Solution Brief

Prioritize What Truly Matters with Reachability Analysis



Most security tools generate overwhelming alerts without assessing whether vulnerabilities are actively exploitable. **Xygeni's Reachability Analysis** changes that by identifying whether a vulnerability is actually reachable in your application, ensuring teams focus only on real threats.

By analyzing code execution paths and dependency usage, Xygeni cuts false positives by up to 70%, ensuring remediation efforts are directed at issues that genuinely pose a risk.

Combined with EPSS (Exploit Prediction Scoring System), Xygeni also prioritizes vulnerabilities based on likelihood of exploitation, allowing security teams to allocate resources efficiently.

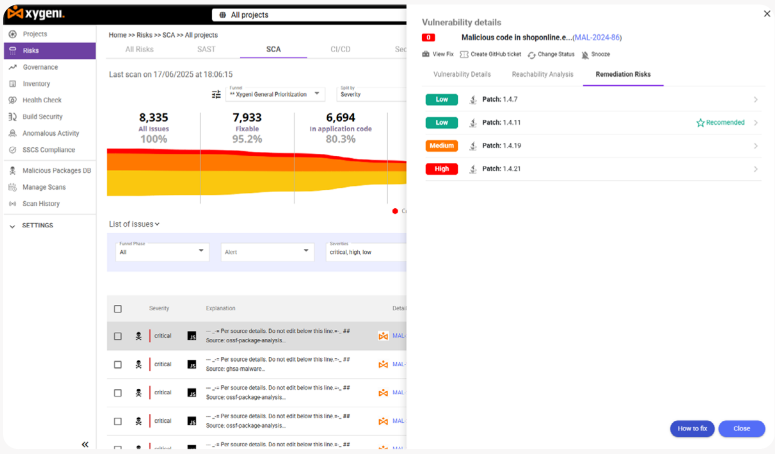
With Xygeni's Reachability Analysis, you gain:

- **Call Graph Tracing:** Accurately maps how vulnerabilities propagate through dependencies.
- **EPSS-Based Prioritization:** Scores vulnerabilities based on real-world exploitability likelihood..
- **Dependency-Level Reachability:** Distinguishes between used and unused components to reduce unnecessary fixes.
- **Continuous Monitoring & CI/CD Integration:** Ensures real-time evaluation of vulnerabilities as your code evolves.

Remediation Risk: Fix Smarter, Not Riskier

Not every upgrade is the right upgrade. Xygeni-SAST goes beyond detection by showing the risks behind each fix. For every vulnerable dependency, you can compare patch options and see:

- **Fixed risks:** vulnerabilities that disappear with the update.
- **New risks:** issues that the upgrade could introduce.
- **Breaking changes:** version jumps that may disrupt your code.



Severity	Explanation
critical	---_-= Per source details. Do not edit below this line.=-_ ## Source: ossf-package-analysis...
critical	---_-= Per source details. Do not edit below this line.=-_ ## Source: ghsa-malware...
critical	---_-= Per source details. Do not edit below this line.=-_ ## Source: ossf-package-analysis...
critical	---_-= Per source details. Do not edit below this line.=-_ ## Source: ossf-package-analysis...

Low	Patch: 1.4.7	
Low	Patch: 1.4.11	Recomended
Medium	Patch: 1.4.19	
High	Patch: 1.4.21	

With this insight, your team chooses the safest patch path, eliminating vulnerabilities without adding noise or new problems.

Accelerate Security with Auto-Remediation

Fixing vulnerabilities manually is time-consuming and slows down development. Xygeni's Auto-Remediation transforms the process by automatically generating fixes for detected vulnerabilities, allowing teams to secure applications without disrupting workflows.

Our AutoFix in Bulk feature goes even further—enabling teams to apply multiple fixes at once for vulnerabilities across different dependencies, reducing remediation time and effort.

How It Works:

1.Automated Fix Suggestions: Xygeni analyzes vulnerabilities and provides suggested fixes directly in your workflow.
2. Bulk AutoFix: Apply multiple remediations in one action, significantly cutting down security debt.
3. Seamless CI/CD Integration: Automate fixes without slowing down development, ensuring security is embedded into your pipelines.
4. Pull Request Generation : Automatically creates PRs with patched versions for rapid implementation.

With Xygeni's Auto-Remediation, organizations can eliminate security risks faster, free up developer resources, and keep applications secure without manual effort.

SBOM and VDR capabilities

Regulatory Requirements for SBOMs:

In response to growing cybersecurity threats, regulatory bodies worldwide are increasingly mandating using Software Bill of Materials (SBOMs). SBOMs provide essential visibility into the components of software applications, facilitating better vulnerability management and compliance with security standards.

Requiring SBOMs are:

1. **Executive Order 14028 (United States):** Federal agencies must require SBOMs from software suppliers.
2. **NIST Guidelines (United States):** Supports SBOM adoption for supply chain security, aligned with EO 14028.
3. **EU Cybersecurity Strategy (Europe):** Promotes transparency and security, encouraging SBOM use.
4. **Cybersecurity Maturity Model Certification (CMMC) (United States):** Defense contractors are encouraged to adopt SBOMs.
5. **FDA Guidance on Cybersecurity (United States):** Recommends SBOMs in medical device submissions.
6. **ISO/IEC Standards:** Considering SBOMs in software security practices.
7. **Automotive Cybersecurity Regulations (Global):** Emerging rules include SBOMs for connected vehicles.
8. **Energy Sector Regulations (Global):** Regulatory Bodies like NERC explore SBOMs to protect critical infrastructure.

Xygeni's Support for SPDX and CycloneDX Standards:

SPDX is a widely recognized standard that enhances transparency by detailing the components and licenses within software packages. Xygeni's compatibility with SPDX allows clients to document and communicate their software contents effectively, meeting global compliance and transparency requirements. Additionally, as a supporter of CycloneDX, a lightweight SBOM standard ideal for application security and software supply chain analysis, Xygeni champions a practical approach to SBOM management. This dual-format support empowers our clients to choose the most suitable standard based on their specific operational needs and preferences.

Integration of Vulnerability Disclosure Reports (VDR):

Xygeni enhances software security management by integrating Vulnerability Disclosure Reports (VDR) into its SBOM generation process. Our VDR provides a comprehensive overview of all known vulnerabilities within a product and its dependencies, analyzes their potential impacts, and outlines remediation strategies. Additionally, VDRs aid in compliance with stringent cybersecurity standards and simplify the remediation process.

Ease of Use:

Xygeni stands out as a user-friendly platform that facilitates the generation of Software Bill of Materials (SBOMs) through both its Command Line Interface (CLI) and Web User Interface (WebUI). This dual-interface approach ensures that Xygeni is accessible to a wide range of users—from developers who may prefer the direct control offered by CLI operations to security professionals who appreciate the intuitive navigation and visual insights provided by a WebUI. By simplifying the SBOM generation process, Xygeni helps users efficiently identify and manage software components, making it an essential tool for modern software development and security management.

Integration into CI/CD Pipelines:

The true power of Xygeni lies in its seamless integration into Continuous Integration/Continuous Deployment (CI/CD) pipelines. This integration is crucial for automating the generation of SBOMs, which ensures that every software build is accompanied by a real-time, up-to-date bill of materials. Automating this process with Xygeni saves time, reduces the potential for human error, and enhances security practices by enabling immediate risk assessment and vulnerability management. This capability allows teams to address potential security issues at the earliest possible stage—often before the software reaches production.

Comprehensive Scans & Security Gates

Xygeni not only supports full system scans but also allows for targeted scanning of specific components or changes, making it ideal for comprehensive security audits and incremental updates. The tool's capability to perform security gate scans further enhances its utility, enabling teams to apply rigorous security checks at critical points within the CI/CD pipeline. These scans can trigger alerts for critical issues requiring immediate attention, facilitating swift and informed responses to emerging threats.

Secure Your Code with Xygeni-SCA

Detect vulnerabilities, block malicious code, and protect your applications—all in one powerful solution.

- **No credit card needed**
- **Quick setup, instant results**

Start your free trial

Get in touch today!

www.xygeni.io
https://www.linkedin.com/company/xygeni
https://twitter.com/xygeni