Open Source Security

Solution Brief

Secure Your Open Source Dependencies against Vulnerabilities and Malicious Code

Minimize risks and protect your applications from malicious packages with Xygeni Early Malware Detection. Prioritize and address the vulnerabilities that matter most. Our comprehensive solution offers real-time monitoring of your dependencies to detect and mitigate threats before they impact your software.

About Company

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have soared from 48% to 74% in just one year.** Even more concerning, 91% of these components are at least 10 versions outdated, significantly heightening security risks.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 against these threats!

Given these challenges, Xygeni's Open Source Security solution is essential. It scans and blocks harmful packages upon publication, dramatically reducing the risk of malware and vulnerabilities infiltrating your systems. Our comprehensive monitoring spans multiple public registries, ensuring all dependencies are scrutinized for safety and integrity. Xygeni also enhances your team's ability to maintain secure and reliable software projects by contextually prioritizing critical issues and facilitating streamlined remediation processes.

245K malicious packages detected last year

Open Source Security

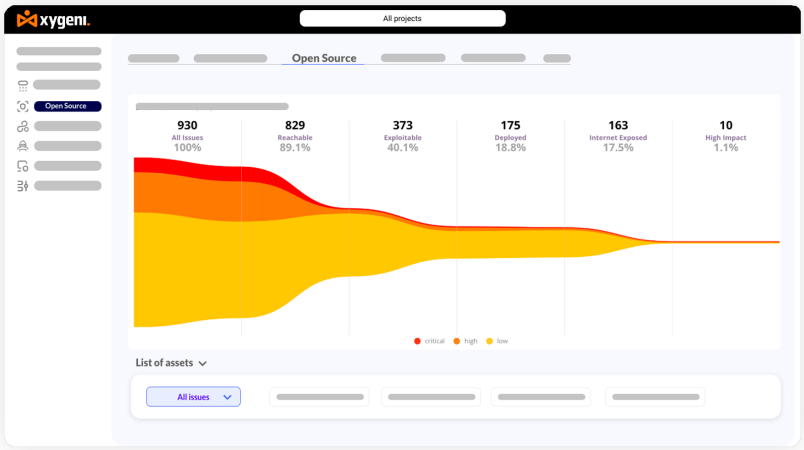
Solution Brief

Comprehensive Component Identification

At the heart of Xygeni's Open Source Security is our advanced capability to precisely identify and catalog every open-source component in your software projects. This thorough approach provides complete visibility into your software's architecture, enabling a detailed assessment of your project's security posture and compliance status. Your team can make better decisions by understanding exactly what makes up your software.

Strategic Approach for Risk Prioritization with ASPM

Xygeni's software security platform excels in identifying and prioritizing vulnerabilities that pose the most significant risks to your software projects. By systematically analyzing the severity and potential impact of each identified vulnerability, Xygeni enables organizations to focus their resources on mitigating the most critical issues first. Our prioritization is driven by a combination of factors such as vulnerability severity, exploitability, exposure, the potential impact on business operations, and any other custom property defined by customers. Some key features of Xygeni's prioritization process are:



1. Continuous Scanning: Xygeni assesses each vulnerability based on its severity and the affected component's context. This approach ensures that vulnerabilities are not just evaluated in isolation but are considered within the broader scope of the system's architecture.

2. Context-Aware Prioritization: Understanding that not all vulnerabilities are created equal, Xygeni prioritizes issues based on their operational and strategic impact. This means vulnerabilities that could lead to significant security breaches are flagged and addressed first.

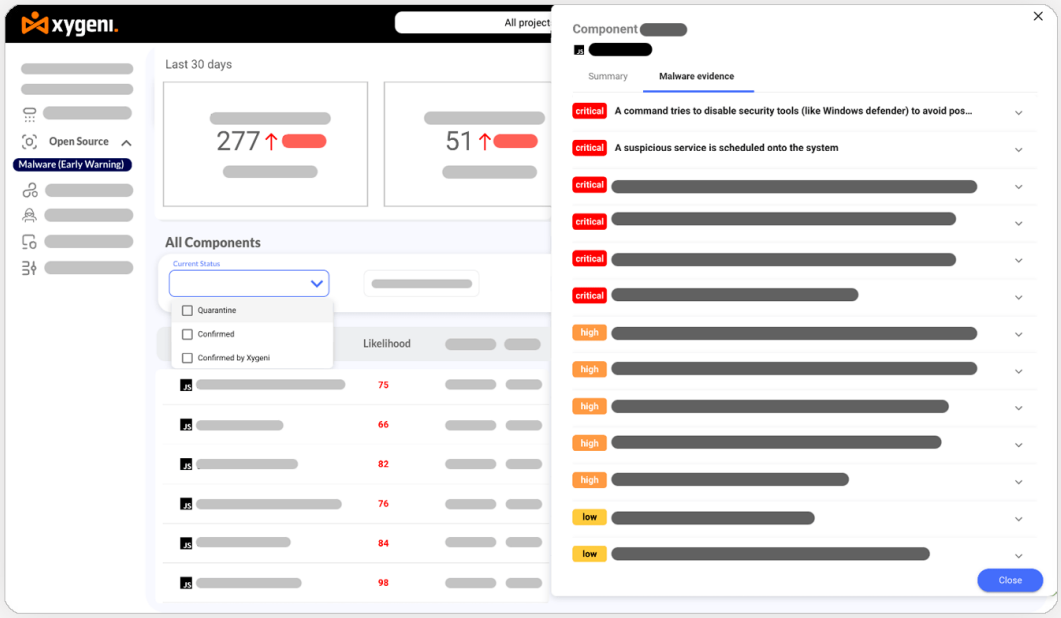
3 Customizable Risk Metrics: Xygeni allows organizations to customize how risks are scored and prioritized, aligning the prioritization process with their specific security policies and compliance requirements. This customization capability ensures that the security efforts perfectly sync with organizational priorities and risk

Open Source Security

Solution Brief

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:

- 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

Open Source Security

Solution Brief

Simplify Open Source Licensing

Xygeni makes navigating the complexities of open-source licensing easy. Our scanning capabilities assess each component's license, helping your team avoid legal issues and ensure compliance with both organizational policies and external regulations. With Xygeni, you can confidently use open-source software, knowing that all licensing requirements are met.

Keep Your Software Updated and Secure

Xygeni actively monitors and identifies outdated or obsolete components in your software projects. By ensuring your projects always utilize the latest and most secure versions, Xygeni not only reduces potential security risks but also boosts software performance and compatibility.

Advanced Detection of Suspect Dependencies

Xygeni's Suspect Dependencies Scanner is crucial for identifying and managing suspect dependencies that could be targets for supply-chain attacks. By analyzing the dependency graph, our product can detect issues such as typo-squatting, dependency confusion, and suspicious installation scripts that may indicate a compromise. If a component is recognized as suspicious, Xygeni provides detailed mitigation and remediation strategies to help safely remove or isolate the threat. This includes recommendations for version pinning, using whitelisted components, and blocking suspicious installation scripts. (see more details below)

Optimized and Accelerated Remediation Workflows

Prioritizing vulnerabilities that pose the highest risk ensures that remediation efforts are concentrated where they are most needed, optimizing resource allocation and reducing the time and effort spent on lower-risk vulnerabilities. Moreover, Xygeni simplifies the remediation of open-source vulnerabilities by integrating directly into developers' existing workflows and issue-tracking systems. This seamless integration provides all the necessary context for each vulnerability right within the tools developers already use, facilitating efficient and effective remediation.

Enhance Transparency and Compliance with SBOM and VDR Generation

Xygeni Open Source Security empowers organizations to maintain complete transparency over their software components with our SBOM generation feature. SBOM facilitates compliance with regulatory requirements and enhances supply chain security by providing a detailed inventory of all software dependencies. Additionally, our Vulnerability Disclosure Report (VDR) generation capability ensures that all stakeholders know potential vulnerabilities, enabling proactive risk management and reinforcing trust throughout the development lifecycle. (see more details below)

Effective Vulnerability Management

Xygeni enhances your software's security by continuously scanning and analyzing open-source components for vulnerabilities. By connecting directly with the National Vulnerability Database (NVD), other vertical vulnerabilities databases and security advisories, and using Common Vulnerabilities and Exposures (CVE) information, Xygeni ensures fast and accurate detection of potential security issues to protect your software applications promptly and efficiently.

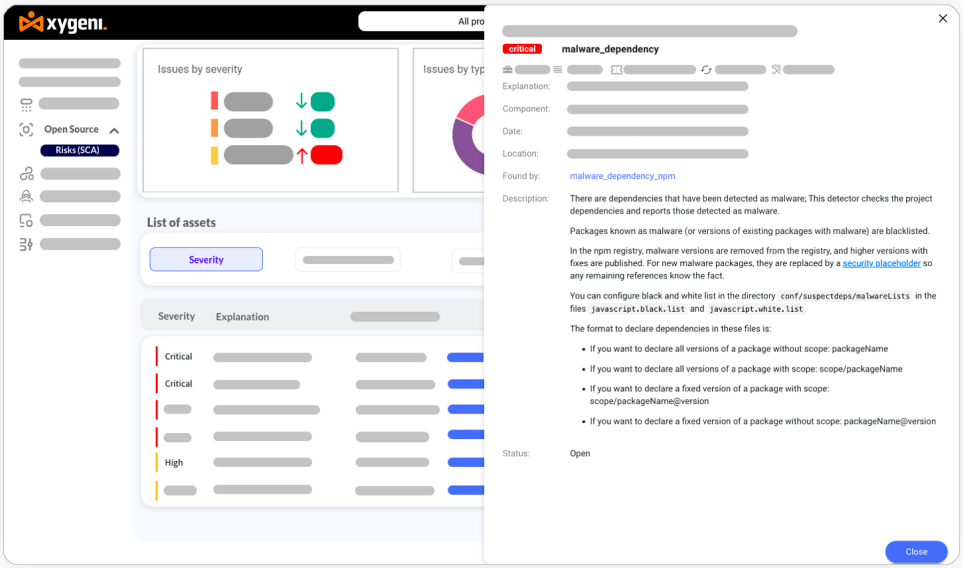
Open Source Security

Solution Brief

Overview of Supported Open Source Suspect Dependency Detectors

Xygeni provides a comprehensive range of detectors tailored to the unique characteristics of various software ecosystems, ensuring comprehensive coverage and precise detection of suspect dependencies, among others:

Types of Suspect Dependency Detector



- **Anomalous Dependencies:** Identifies unusual or unexpected dependencies within the context of the project, which may signal a security concern.
- **Dependency Confusion:** This feature detects cases where internal package names may be confused with similarly named packages from public repositories, potentially leading to security breaches.
- **Known Vulnerabilities:** Flags dependencies that contain recognized security vulnerabilities.
- **Malware:** Looks for dependencies known to contain malware, providing critical security alerts to prevent potential harm.
- **Suspicious Scripts:** Monitors for scripts within dependencies that might perform unauthorized or harmful actions.
- **Typosquatting:** Aims to catch potentially malicious typosquatting attempts where package names are slightly altered to trick users into installing them.
- **Unscoped Internal Components:** This is a special detector for NPM that identifies unscoped internal components and thus might be at risk of being publicly exposed or confused with external packages.

Open Source Security

Solution Brief

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):** Issued in 2021, this executive order mandates federal agencies to require SBOMs from their software suppliers.
2. **NIST Guidelines (United States):** The National Institute of Standards and Technology provides guidelines that support the implementation of SBOMs to enhance software supply chain security, aligning with the requirements of Executive Order 14028.
3. **EU Cybersecurity Strategy (Europe):** While not mandating SBOMs directly, the strategy emphasizes enhancing software transparency and security, which supports using SBOMs to manage software supply chain risks.
4. **Cybersecurity Maturity Model Certification (CMMC) (United States):** CMMC affects defense contractors and includes practices encouraging the adoption of SBOMs to protect sensitive defense information.
5. **FDA Guidance on Cybersecurity (United States):** The Food and Drug Administration recommends including SBOMs in premarket submissions for medical devices, highlighting their role in managing cybersecurity risks.
6. **ISO/IEC Standards:** Various standards from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are considering SBOMs as part of software security and risk management practices.
7. **Automotive Cybersecurity Regulations (Global):** Emerging regulations in the automotive sector are beginning to include requirements for SBOMs to ensure the safety and security of connected vehicles.
8. **Energy Sector Regulations (Global):** Regulatory bodies in the energy sector, such as the North American Electric Reliability Corporation (NERC), are exploring requirements for SBOMs to secure the increasingly digitized energy infrastructure.

Open Source Security

Solution Brief

Xygeni OSS: SBOM and VDR Capabilities

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.

Book Your Demo Now - Transform Your Approach to Cybersecurity!