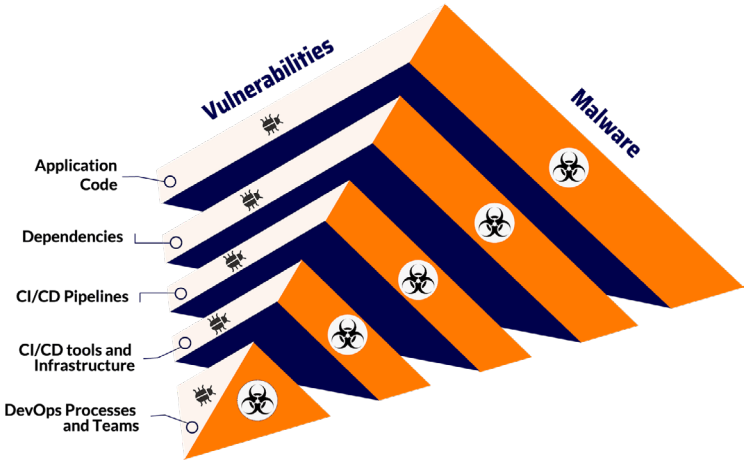
Malware Across DevOps

Solution Brief

Xygeni Malware Protection Across DevOps

Real-Time Detection & Automated Defense Against Malware in Your DevOps Pipelines

Xygeni detects and blocks malware in real time across code, dependencies, CI/CD, infrastructure, and DevOps workflows, stopping zero-day threats, backdoors, and supply chain attacks before they spread.



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.

Malicious open-source packages are surging, with 778,500+ identified since 2019, fueling dependency-based attacks. Backdoors, trojans, and zero-day exploits now infiltrate open-source components, CI/CD pipelines, and infrastructure, evading security.

Attackers inject malware at every stage of the software supply chain, compromising applications before deployment and exploiting dependencies, build systems, and misconfigured CI/CD pipelines.

Xygeni delivers real-time threat detection and automated blocking, stopping malicious dependencies, unauthorized code changes, and pipeline attacks before they spread. Our multi-layered security engine ensures full visibility from code to deployment, securing your software supply chain.

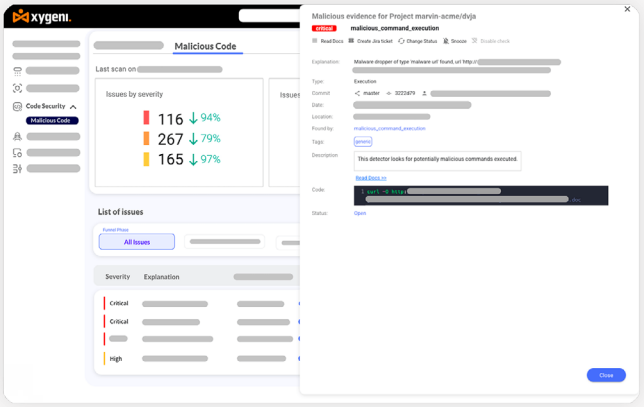
Stay ahead of threats with Xygeni's proactive malware detection and automated defense—protecting your entire DevOps ecosystem.

$60B
The Cost of SSC Attacks this year

Malware Across DevOps

Solution Brief

Detect Malware in Application Code



Find and eliminate malicious code before deployment.

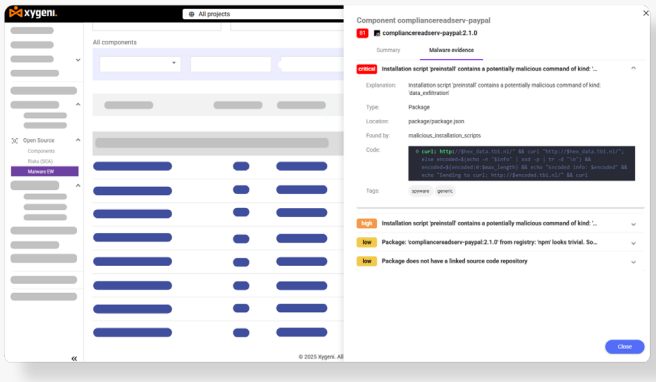
Advanced SAST for Malware Detection:
Xygeni enhances traditional Static Application Security Testing (SAST) by incorporating malware detection capabilities. It scans source code for backdoors, trojans, obfuscated scripts, and unauthorized modifications, ensuring that malicious code does not go undetected before deployment.

1.9% of GitHub PoC exploit repositories are malicious, aiming to exfiltrate data or deploy malware.

Block Malicious Packages & Dependencies

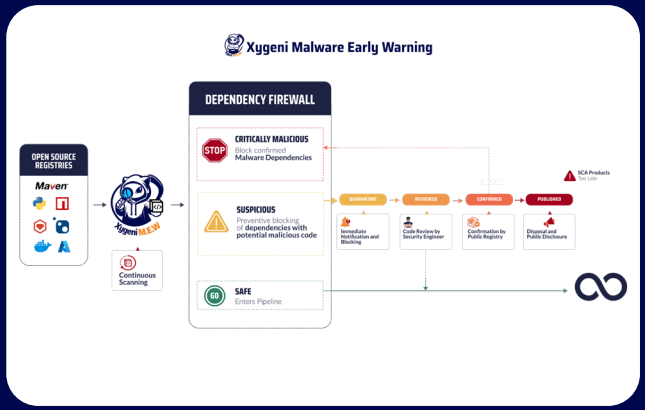
Stop malware at the source—before it enters your software.

- **Real-Time Malware Detection:** Analyzes thousands of new open-source packages daily to block zero-day malware instantly.
- **Dependency Firewall:** Provides early warnings, quarantines suspicious packages, and blocks malware by scanning NPM, PyPI, Maven, NuGet, and RubyGems for infected dependencies before use.



Malicious open-source packages surged 156% last year, reaching 512,847.

Early Warning System for Zero-Day Threats



Xygeni's Early Warning System provides real-time threat intelligence, continuously scanning public repositories to detect and block zero-day malware before it can infiltrate your supply chain.

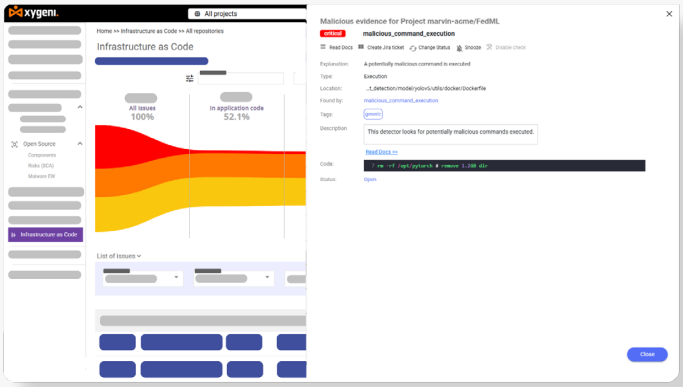
1. **Continuous Monitoring & Identification:** Tracks new packages in real-time, analyzing metadata and anomalies to flag malware threats.
2. **Early Warning Alerts:** Notifies DevOps teams about any potential malware impacting their applications upon malware publication.
3. **Research & Confirmation:** Validates flagged threats through deeper security analysis, reducing false positives.
4. **Registry Notification:** Reports verified malicious packages to public registries, helping prevent further distribution.

Malware Across DevOps

Solution Brief

Secure CI/CD Pipelines from Malware Attacks

Secure CI/CD pipelines from malware attacks by preventing threats before deployment, ensuring integrity, and blocking compromised artifacts.



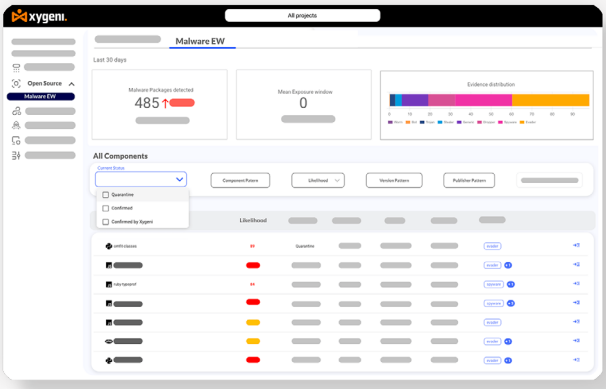
- **Reverse Shell Prevention:** Blocks reverse shell attacks that grant attackers unauthorized remote access within CI/CD pipelines.
- **Malware Download Blocking:** Detects and stops malicious payload downloads, preventing the execution of trojans, backdoors, and other hidden threats.
- **Infrastructure as Code (IaC) Security:** Scans Terraform, CloudFormation, Kubernetes, and Helm configurations for malicious commands.

The software supply chain experienced an attack approximately every 48 hours in 2024.

Strengthen DevOps Processes & Teams Against Threats

Gain visibility and control over your software supply chain to detect anomalies, prevent unauthorized access, and maintain software integrity.

- **Collaborator & Publisher Analysis:** Tracks maintainer reputation, package ownership changes, and suspicious releases to prevent supply chain infiltration.
- **Anomaly Detection:** Identifies unusual actions within CI/CD pipelines that attempt to exploit misconfigurations for infiltration.
- **Code Tampering Protection:** Detects unauthorized modifications in source code, build artifacts, and deployment scripts.
- **Historical Malware Lookup:** Provides full records of previously identified malicious packages for forensic investigation.



34% of data breaches stem from insider threats—making privilege monitoring and maintainer reputation tracking critical.

Malware Across DevOps

Solution Brief

Xygeni's Advanced Malware Malware Detectors

Comprehensive threat detection across code, dependencies, CI/CD, infrastructure, and DevOps environments.

Code Security Malware Detectors

- **Decoded & Decrypted Code Execution –** Identifies hidden malware that executes only after decryption.
- **Downloaded Code Execution –** Detects malicious scripts retrieved during runtime.
- **Malicious Command Execution –** Blocks unauthorized shell commands and remote access attempts.
- **Obfuscated Code Execution –** Flags attempts to hide malicious logic through code obfuscation.
- **Silent Execution & Registry Code Injection –** Prevents stealth malware from executing without detection.

Package & Dependency Security Detectors

- **Malicious Installation Scripts –** Detects scripts designed to introduce malware through package installations.
- **System Registry Tampering –** Prevents modifications that enable persistence mechanisms.
- **Masquerade File Type–** Identifies files disguised as legitimate software components.
- **Suspicious URL & Request Detection –** Blocks outbound connections to known malicious sites.

Code Tampering & Critical File Modification Detectors

- **Build & Workflow File Modification –** Detects unauthorized changes in CI/CD pipeline configurations.
- **Configuration & Env File Tampering –** Flags alterations in .env files and system configurations.
- **Security Policy & Tool Configuration Modification –** Prevents unauthorized security tool reconfigurations.
- **Infrastructure as Code (IaC) Modification –** Detects changes in Terraform, Kubernetes, and CloudFormation templates.

Unusual Activity & Behavioral Anomaly Detectors

- **CI/CD Token Misuse –** Detects token scope changes and unprotected credentials.
- **Repository Security Alerts –** Monitors for anomalous forks, unauthorized publicizations, and unexpected deletions.
- **Branch Protection Bypasses–** Flags unsigned commits, force pushes, and changes to status check requirements.
- **Jenkins & CI/CD Security Events –** Identifies failed logins, unauthorized plugin installations, and unusual long-running builds.

xygeni.

Stop Malware in Your DevOps

Detect, Block & Prevent Malicious Code Across Your SDLC

- **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