

Malicious Package Protection

Identify and remediate dangerous or suspicious open source code in your applications with deep package scanning and the industry's largest database of malicious packages.



Industry Challenge

The rise in malicious code in open source software (OSS) is increasing the frequency and severity of software supply chain attacks. The trend is clear:

- ↳ **92%** increase in the number of identified malicious packages in the wild from 2022 to 2024¹
- ↳ **68%** increase in supply-chain-related breaches between 2023 and 2024²
- ↳ **76%** of CISOs – concerned about the dangers of malicious packages³
- ↳ **\$4.63 million** – average cost of a software supply chain compromise, 8.3% higher than the average cost of a data breach due to other causes⁴

Checkmarx can help you mitigate this critical attack vector.

Protect Your Organization From Malicious Packages

Malicious packages can expose your organization and your customers to data exfiltration, intellectual property theft, system compromise and control, operational disruption, financial loss, reputation damage, and compliance violations.

Checkmarx' Malicious Package Protection enables your teams to quickly identify and eliminate the dangers of malicious and suspicious open source packages throughout the software development lifecycle (SDLC).

Key Benefits of Checkmarx Malicious Package Protection

- ↳ **Unmatched OSS Risk Visibility**
Prevent malicious threats by leveraging the industry's largest malicious packages database and deepest scanning capabilities.
- ↳ **Efficient & Prioritized Remediation**
Focus the efforts of your security and development teams on the biggest threats facing your organization.
- ↳ **A Safer Development Environment**
Automatically identify and block malicious or suspicious packages before they are installed in the dev environment or pushed to code repositories.



Key Features

▾ Comprehensive Scanning

Checkmarx detects malicious packages in manifest files, binaries, and containers.*

▾ Deep Malicious Package Detection

Checkmarx detects all OSS packages in use, including dependencies of other packages (transitive dependency scanning), to identify any that contain malware or exhibit suspicious behavior.

▾ Unparalleled Malicious Package Database

Checkmarx has the industry's largest database of malicious packages. The combination of our dedicated AppSec research team and proprietary automated technologies has identified more than 385,000 malicious packages to date.

▾ Package Reliability Metrics

Checkmarx rates the trustworthiness of each open source package included in your applications by package legitimacy, behavioral integrity, and contributor reputation.

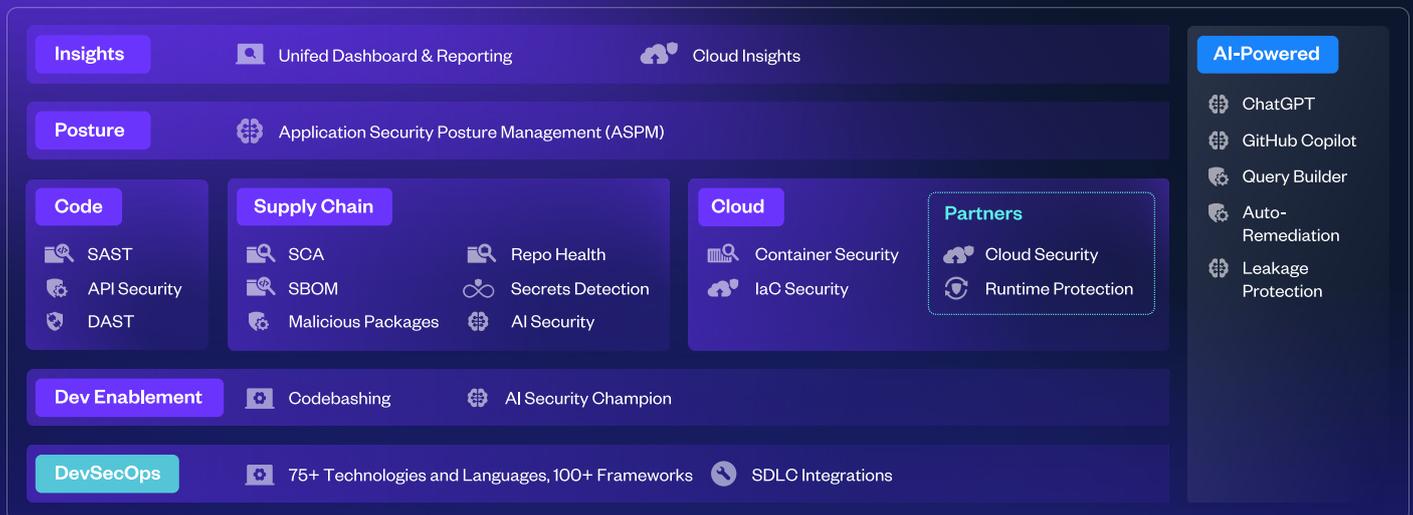
▾ Automated Policy Actions

Out-of-the-box and user-defined policies automatically take effect when malicious packages are detected. This includes sending alerts, generating incident reports, preventing pull requests and/or breaking builds.

Part of a Complete AppSec Solution

Malicious Package Protection is offered as part of the Checkmarx One platform. Checkmarx One provides a unified, enterprise-scale AppSec platform with everything you need to secure your applications. You can take advantage of the capabilities you're ready to use today, while remaining poised to address your needs of tomorrow.

Checkmarx One



*Scanning for malicious packages in containers requires the purchase of our Container Security product.

Checkmarx

Checkmarx is the leader in application security and ensures that enterprises worldwide can secure their application development from code to cloud. Our consolidated platform and services address the needs of enterprises by improving security and reducing TCO, while simultaneously building trust between AppSec, developers, and CISOs. At Checkmarx, we believe it's not just about finding risk, but remediating it across the entire application footprint and software supply chain with one seamless process for all relevant stakeholders.

We are honored to serve more than 1,800 customers, which includes 40 percent of all Fortune 100 companies including Siemens, Airbus, Salesforce, Stellantis, Adidas, Walmart and Sanofi.