

ThirdWatch

Third-party software, including open source, is increasingly important for developers. But you can inherit vulnerabilities and other risks from these software libraries.

ThirdWatch gives security and dev teams visibility into risks from third-party software and helps mitigate those risks.

Vulnerability Monitoring for Development Teams

Cyber security has become a critical business objective for every company, since a high-profile data breach can force any business into a survival situation on the global stage.

Companies that develop software, whether for their own internal use or for their customers, should pay special attention to make sure their code is secure. But developers often neglect to consider third-party code they rely on, and are unaware when vulnerabilities are identified.

ThirdWatch solves this problem by notifying developers about security issues in software libraries they depend on.

- Identifies vulnerable third-party software your organization is using, including open source
- Gives developers and management visibility into software dependencies and their risk profile
- Integrates with Cytenna's vulnerability database, the most comprehensive and up-to-date vulnerability source
- Helps developers address security risks and determine when upgrades are available
- Identifies licenses for open-source components, and flags compliance issues
- Integrates with your build environment and trouble-ticketing system

How ThirdWatch Works:



Inventory Tracking

ThirdWatch helps your development team keep track of the third party libraries that your organization uses. ThirdWatch plugs into popular build tools for Java, .Net, Python, and other languages, so that software dependencies can be easily discovered and tracked.

Always Watching

Behind the scenes, ThirdWatch monitors thousands of vendors and open source projects for the latest information about vulnerabilities and security risks. The system reports any security issues that are relevant, based on the third-party libraries that you are using. In addition, ThirdWatch identifies the licenses for your open source libraries, and flags any conflicts based on your licensing policies.

Alerts and Mitigation

ThirdWatch will send alerts to the appropriate staff members when a new security issue arises. The system also helps developers choose the best mitigation strategy, and integrates with trouble-ticketing systems, so vulnerability management is simple from start to finish.

Key Features

- **Comprehensive coverage** – We maintain one of the largest vulnerability databases in the industry. In particular, we provide the most comprehensive coverage of open source security issues.
- **Real-time coverage** – ThirdWatch continually monitors for new and updated software vulnerabilities.
- **Inventory Discovery** – The system makes it simple to identify and track the open source libraries you use..
- **License Checking** – ThirdWatch identifies the licenses used by your open source libraries, and lets you know if there are any conflicts with your licensing policies.
- **Alerts and Reporting** – When new security issues arise, ThirdWatch alerts the right people. Reports can be generated in a wide variety of formats.
- **Workflow Integration** – ThirdWatch helps developers to assess security issues and choose mitigation strategies. The system can also generate and track trouble tickets