MEND Azure DevOps

Mend for Azure Repos Integration

Integrated security and compliance made easy

In modern software development, security is in high demand yet in short supply. To make security more efficient and cost effective, organizations have shifted the burden of security to developers. For this shift left to be successful, organizations need developer-first security tooling that integrates with native environments to make security invisible for developers.

Mend for Azure Repos integrates seamlessly with Azure DevOps Repos, giving developers a tool they love to use because it improves software security without slowing software development. This integration empowers developers to move beyond just scanning to focus on the remediation of open source vulnerabilities and license compliance issues.

Native Repository Integration

Mend for Azure Repos integrates with developers' native Azure DevOps Repos environment to scan repositories as part of a Mend account. Mend detects all open source components and displays any open source security vulnerabilities or license compliance issues directly within Azure Repos.

Mend for Azure Repos provides developers with remediation information on vulnerable and outdated open source components and generates comprehensive up-to-date reports in the Issues tab and the security dashboard of the scanned project. Scanned projects can also be viewed in the Mend portal.

Key Capabilities

The Mend for Azure Repos integration gives developers full-spectrum application security that includes automated remediation, not just more alerts.

Automate Fix Merge Requests and Dependency Updates

Mend Remediate automatically opens fix merge requests for vulnerable open source components in the repository, upgrading them to the lowest non-vulnerable version.

Enforce Policies

Policies are automatically enforced in the repository for each merge request. The status and results of each scan appear on the Commits page.

Key Benefits

Shift left
Scanning at the repository shifts security left while still enforcing policies and requiring all developers to scan their code.

Feedback on demand
Developers receive feedback when they are still working on their code, making defects easier to remediate.

No context switching
Developers don't need to leave Azure DevOps Repos to consume and act upon scan results.

Differential results
Alerts occur only if a pull request introduces new errors. Positive feedback is given to developers when a pull request resolves vulnerabilities.

Automated remediation
Security vulnerabilities can be automatically prioritized and remediated.

Merge with Confidence

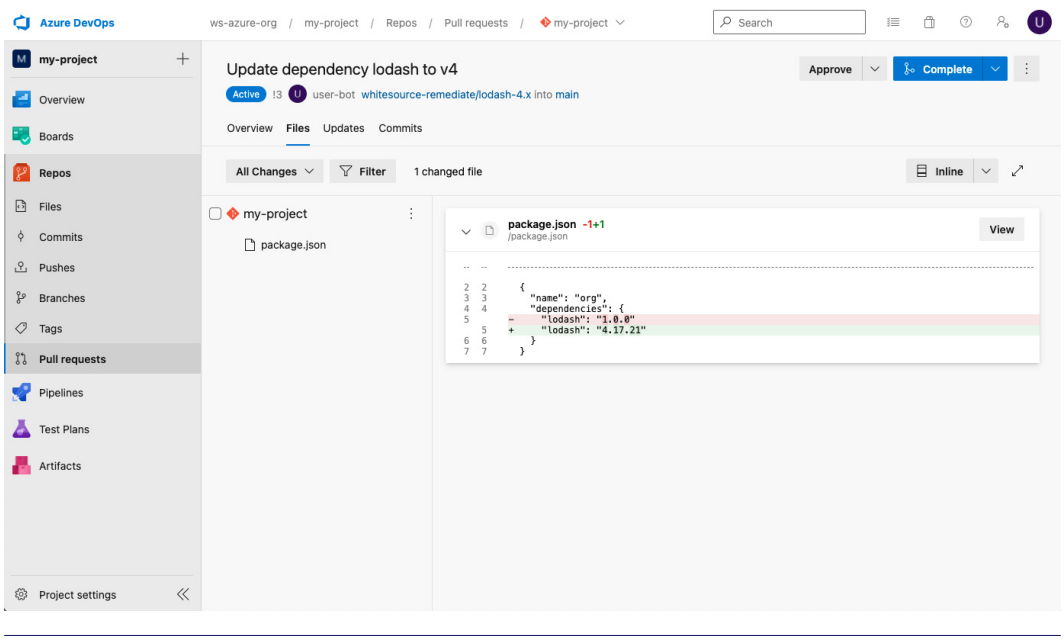
Using crowdsourced data, Mend Merge Confidence shows how likely an open source component can be updated without breaking the build. Merge Confidence includes data on upgrade age, adoption, and compatibility to create a "confidence" score.

Scan for IaC Misconfigurations

Protect production environments and provide security for the cloud, containers, and Kubernetes directly from Azure Repos.

Hosted in the Cloud

The integration is fully cloud-based, so there is no need to worry about configuring or managing hardware. Simply create an account and go.



With Mend for Azure Repos, scan results and actionable remediation advice are viewable directly within the repository, so developers never have to leave their native development environment.

About Mend

Mend helps organizations accelerate the development of secure software at scale. We provide automated tools that bridge the security knowledge gap, integrating easily into the software development life cycle and going beyond detection with a remediation-first approach. Mend is built on the most comprehensive vulnerability database in the industry, providing the widest coverage for threats and attack vectors. Our solution helps enterprises reduce risk and increase the productivity of their security and development teams. For more information, visit www.Mend.io

Related Resources

Learn more at www.mend.io