

# Assessing adoption of code security features

## In this article

- About adoption of code security features
- Viewing the enablement of code security features for an organization
- Viewing the enablement of code security features for an enterprise
- Interpreting and acting on the enablement data

You can use security overview to see which teams and repositories have already enabled code security features, and identify any that are not yet protected.

## Who can use this feature

Security overview for an organization is available to all members of the organization. The views and data displayed are determined by your role in the organization, and by your permissions for individual repositories within the organization. For more information, see "[About security overview](#)."

Security overview for an enterprise shows organization owners and security managers data for the organizations they have access to. Enterprise owners can only view data for organizations where they are added as an organization owner or security manager. For more information, see "[Managing your role in an organization owned by your enterprise](#)."

All enterprises and their organizations have a security overview. If you use GitHub Advanced Security features, which are free for public repositories, you will see additional information. For more information, see "[About GitHub Advanced Security](#)."

## About adoption of code security features

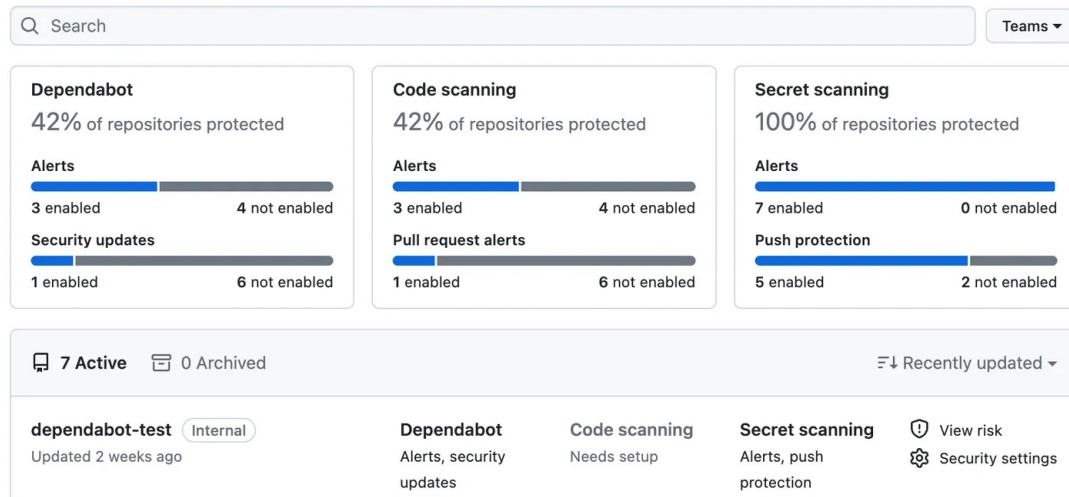
You can use security overview to see which repositories and teams have already enabled each code security feature, and where people need more encouragement to adopt these features. The "Security coverage" view shows a summary and detailed information on feature enablement for an organization. You can filter the view to show a subset of repositories using the "enabled" and "not enabled" links, the "Teams" dropdown menu, and a search field in the page header.

## Security coverage

[Give feedback](#)

Enablement of security features for repositories across the organization.

Organization members can only view repositories where they have admin privileges.




You can download a CSV file of the data displayed on the "Security coverage" page. This data file can be used for efforts like security research and in-depth data analysis, and can integrate easily with external datasets. For more information, see ["Exporting data from the risk and coverage pages."](#)


## Viewing the enablement of code security features for an organization [↗](#)

The information shown by security overview varies according to your access to repositories and organizations, and according to whether GitHub Advanced Security is used by those repositories and organizations. For more information, see ["About security overview."](#)

In the list of repositories, the "Paused" label under "Dependabot" indicates repositories for which Dependabot updates are paused. For information about inactivity criteria, see ["About Dependabot security updates"](#) and ["About Dependabot version updates,"](#) for security and version updates, respectively.

- 1 On GitHub.com, navigate to the main page of the organization.
- 2 Under your organization name, click  **Security**.



- 3 To display the "Security coverage" view, in the sidebar, click  **Coverage**.
- 4 Use options in the page summary to filter results to show the repositories you want to assess. The list of repositories and metrics displayed on the page automatically update to match your current selection. For more information on filtering, see ["Filtering alerts in security overview."](#)
  - Use the **Teams** dropdown to show information only for the repositories owned by one or more teams. For more information, see ["Managing team access to an organization repository."](#)
  - Click **NUMBER enabled** or **NUMBER not enabled** in the header for any feature to show only the repositories with that feature enabled or not enabled.
  - At the top of the list of repositories, click **NUMBER Archived** to show only

repositories that are archived.

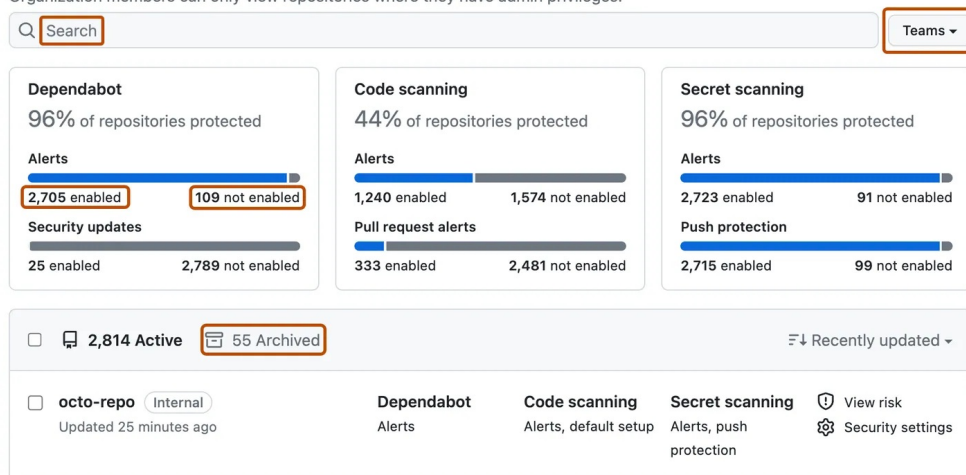
- Click in the search box to add further filters to the repositories displayed.

## Security coverage

[Give feedback](#)

Enablement of security features for repositories across the organization.

Organization members can only view repositories where they have admin privileges.



- 5 Optionally, click **Security settings** to enable code security features for a repository and click **Save security settings** to confirm the changes. If a feature is not shown, it has more complex configuration requirements and you need to use the repository settings dialog. For more information, see "[Securing your repository](#)."
- 6 Optionally, select some or all of the repositories that match your current search and click **Security settings** in the table header to display a side panel where you can enable security features for the selected repositories. When you've finished, click **Apply changes** to confirm the changes. For more information, see "[Enabling security features for multiple repositories](#)."

**Note:** For both the single and multiple repository enablement settings, enabling code scanning will override any existing code scanning configurations for the selected repositories, including any previous query suite selections and workflows for advanced setups.

## Viewing the enablement of code security features for an enterprise

You can view data to assess the enablement of code security features across organizations in an enterprise. The information shown by security overview varies according to your access to repositories and organizations, and according to whether GitHub Advanced Security is used by those repositories and organizations. For more information, see "[About security overview](#)."

In the enterprise-level view, you can view data about the enablement of features, but you cannot enable or disable features. For more information about enabling features, see "[Enabling security features for multiple repositories](#)."

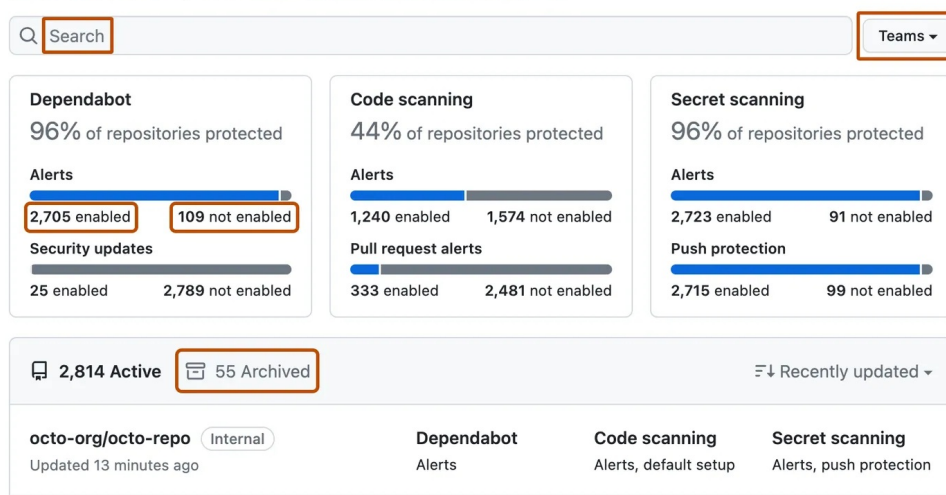
**Tip:** You can use the `org:` filter in the search field to filter the data by organization. For more information, see "[Filtering alerts in security overview](#)."

- 1 Navigate to GitHub.com.
- 2 In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.

- 3 In the list of enterprises, click the enterprise you want to view.
- 4 In the left sidebar, click ⓘ **Code Security**.
- 5 To display the "Security coverage" view, in the sidebar, click **Coverage**.
- 6 Use options in the page summary to filter results to show the repositories you want to assess. The list of repositories and metrics displayed on the page automatically update to match your current selection. For more information on filtering, see "[Filtering alerts in security overview](#)."
  - Use the **Teams** dropdown to show information only for the repositories owned by one or more teams. For more information, see "[Managing team access to an organization repository](#)."
  - Click **NUMBER enabled** or **NUMBER not enabled** in the header for any feature to show only the repositories with that feature enabled or not enabled.
  - At the top of the list of repositories, click **NUMBER Archived** to show only repositories that are archived.
  - Click in the search box to add further filters to the repositories displayed.

## Security coverage

Enablement of security features for repositories across the enterprise.



## Interpreting and acting on the enablement data [↗](#)

Some code security features can and should be enabled on all repositories. For example, secret scanning alerts and push protection. These features reduce the risk of a security leak no matter what information is stored in the repository. If you see repositories that don't already use these features, you should either enable them or discuss an enablement plan with the team who owns the repository. For information on enabling features for a whole organization, see "[Managing security and analysis settings for your organization](#)."

Other features are not available for use in all repositories. For example, there would be no point in enabling Dependabot or code scanning for repositories that only use ecosystems or languages that are unsupported. As such, it's normal to have some repositories where these features are not enabled.

Your enterprise may also have configured policies to limit the use of some code security features. For more information, see "[Enforcing policies for code security and analysis for your enterprise](#)."

Legal