

About security overview

In this article

About security overview

About security overview for organizations

About security overview for enterprises

Permission to view data in security overview

Further reading

You can view summaries of alerts for repositories owned by your organization and identify areas of high security risk. You can also monitor adoption of code security features across your organization.

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 you will see additional information. For more information, see "[About GitHub Advanced Security](#)."

About security overview

Security overview provides high-level summaries of the security status of an organization or enterprise and makes it easy to identify repositories that require intervention. You can also use security overview to see which repositories have enabled specific security features and to configure any available security features that are not currently in use.

Security overview shows which security features are enabled for repositories, and includes repository and alert-focused views so you can quickly investigate security issues and take action to remediate them.

- Risk and coverage information about Dependabot features and alerts is shown for all repositories.
- Risk and coverage information for GitHub Advanced Security features, such as code scanning and secret scanning, is shown for enterprises that use GitHub Advanced Security.

For more information, see "[About Dependabot alerts](#)" and "[About GitHub Advanced Security](#)."

The views are interactive with filters that allow you to look at the aggregated data in

detail and identify sources of high risk or low feature coverage. As you apply multiple filters to focus on narrower areas of interest, all data and metrics across the view change to reflect your current selection. For more information, see "[Filtering alerts in security overview](#)."

There are also dedicated views for each type of security alert that you can use to limit your analysis to a specific set of alerts, and then narrow the results further with a range of filters specific to each view. For example, in the secret scanning alert view, you can use the "Secret type" filter to view only secret scanning alerts for a specific secret, like a GitHub personal access token.

Note: Security overview displays active alerts raised by security features. If there are no alerts shown in security overview for a repository, undetected security vulnerabilities or code errors may still exist or the feature may not be enabled for that repository.

About security overview for organizations

The application security team at your company can use the different views for both broad and specific analyses of your organization's security status. For example, the team can use the "Security coverage" view to monitor the adoption of features across your organization or by a specific team as you roll out GitHub Advanced Security, or use the "Security risk" view to identify repositories with more than five open secret scanning alerts. You can also use security overview to find a set of repositories and enable or disable security features for them all at the same time. For more information, see "[Enabling security features for multiple repositories](#)."

You can find security overview on the **Security** tab for any organization that's owned by an enterprise. Each view shows a summary of the data that you have access to. As you add filters, all data and metrics across the view change to reflect the repositories or alerts that you've selected. For information about permissions, see "[Permission to view data in security overview](#)."

Security overview has multiple views that provide different ways to explore enablement and alert data.

- Use "Security coverage" to assess the adoption of code security features across repositories in the organization.
- Use "Security risk" to assess the risk from security alerts of all types for one or more repositories in the organization.
- Use the individual security alert views to identify your risk from specific vulnerable dependencies, code weaknesses, or leaked secrets.

For more information about these views, see "[Assessing adoption of code security features](#)" and "[Assessing your code security risk](#)."

About security overview for enterprises

You can find security overview on the **Code Security** tab for your enterprise. Each page displays aggregated and repository-specific security information for your enterprise.

As with security overview for organizations, security overview for enterprises has multiple views that provide different ways to explore enablement and alert data.

- Use the "Security coverage" view to assess the adoption of code security features across organizations in the enterprise.
- Use the "Security risk" view to assess the risk from security alerts of all types across organizations in the enterprise.
- Use the individual security alert views to identify your risk from specific vulnerable

dependencies, code weaknesses, or leaked secrets.



For information about permissions, see "[Permission to view data in security overview](#)."

Permission to view data in security overview

If you are an owner or security manager for an organization, you can see data for all the repositories in the organization in all views. You can see the data in the organization-level security overview, or see data for all organizations where you are an owner or security manager in the enterprise-level security overview.

If you are an enterprise owner, you will need to join an organization as an organization owner to view data for the organization's repositories in either the organization-level or enterprise-level overview. For more information, see "[Managing your role in an organization owned by your enterprise](#)."

If you are an organization member, you can view security overview for the organization and see data for repositories where you have access. You can view this data in the organization-level overview, but you cannot access the enterprise-level overview.

Organization member with	Risk and alerts views	Coverage view
 access for one or more repositories	View data for those repositories	View data for those repositories
 access for one or more repositories	View code scanning and Dependabot data for those repositories	No access for those repositories
Security alert access for one or more repositories	View all security alert data for those repositories	No access for those repositories
Custom organization role with permission to view one or more types of security alert	View allowed alert data for all repositories in all views	No access

For more information about access to security alerts and related views, see "[Managing security and analysis settings for your repository](#)" and "[About custom repository roles](#)."

Further reading

- "[Securing your repository](#)"
- "[Securing your organization](#)"
- "[Introduction to adopting GitHub Advanced Security at scale](#)"

Legal