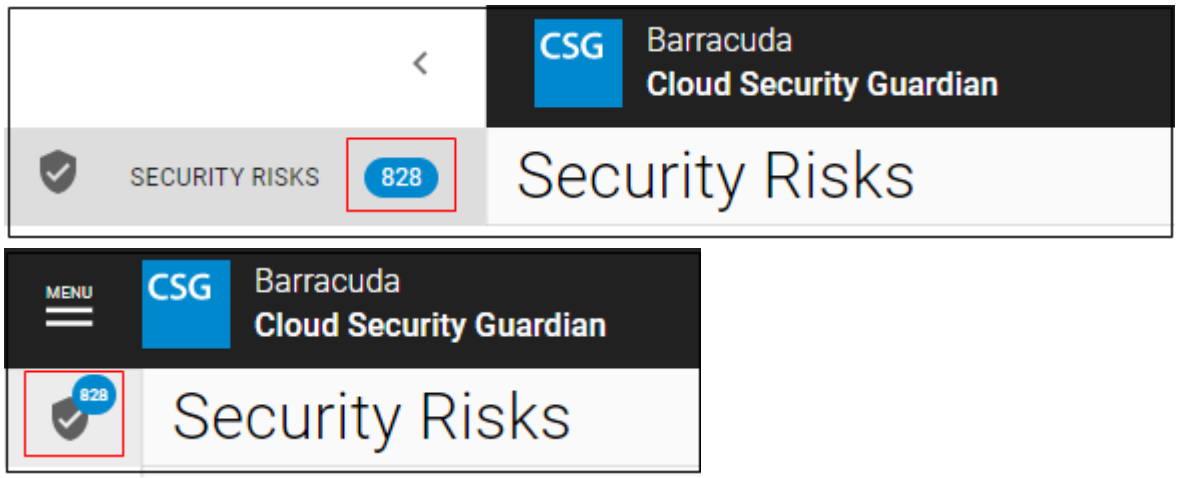
Security Risks

https://campus.barracuda.com/doc/93196211/

Every twelve hours, Barracuda Cloud Security Guardian scans your infrastructure for risks. It detects items which do not pass the standards in your policies. When it detects these failed items that need your attention, it highlights them on the **Security Risks** page.

You can think of this page as an inbox or a to-do list, where you can assess and address outstanding risks. The number of outstanding risks in your infrastructure displays in the menu pick for the Security Risks page. Navigate to the **Security Risks** page to assess the outstanding risks and either *remediate* them or *suppress* them.



Reviewing Security Risks

On the **Security Risks** page, the left panel displays outstanding risks – resources that have failed conditions in your policies – ranked from most to least severe, and grouped by cloud connection, security standard, and control. The number displayed for each entry in this list relates to the number of risks in that group.

Filtering Security Risks

Use the filters at the top of the page to choose certain values you want to include in the table on this page. This information on filtering applies to the **Security Risks** and **Security Findings** pages.

- Use the **Search** field to find a control title or description.
- Select specific settings in other search fields. Select **All** to select everything in that menu. Select **None** to clear all of the selections in that menu.
- After you make your selection for each field, either tab to the next field or click elsewhere on

the screen to apply your section to the table.

- **Sharing between pages** – The filter settings you choose are shared between the **Security Risks** and **Security Findings** pages. When you switch between these pages, your filter settings are automatically applied. You can alter the filter settings or remove all filters by clicking **Clear Filters**.
- **Bookmarking your filters** – When you have set the filters you want to use, create a bookmark in your browser. When you open that bookmark, your filters are automatically applied.
- **Sharing with a colleague** – To share your filter settings with an colleague who has access to your account, copy the URL in the address bar of your browser and share it. When your colleague opens the link you sent, they will see that page with the same filters you selected.

As described above, scans are performed automatically every hour. If you choose, you can perform an on-demand scan at any time by clicking **Scan** . To refresh the results in your browser without scanning the system, click **Refresh** . You might want to perform an on-demand scan, for example, after you update your policies. If you make your policies more strict, you can expect to see a higher number of security risks on this page. If you make your policies more lenient, you can expect the number of risks to decrease.

Explore the risks in the right panel. Click a resource to see the details of the failure.

- **Source** – Either Azure Security Center or AWS Security Hub.
- **See all findings from this source** – Click the link to view the **Findings** page, filtered to exclusively display all findings for this source.
- **Connection** – The Azure or AWS Cloud Connection where the risk was located.
- **Resource** – The specific resource associated with your cloud connection; for example, a security group or database. Click the link to see details within the **Resources** page.
- **Region** – The geographic region where this resource is located.
- **Resource Type** – The type of resource; for example, a security group or database.
- **Control** – The specific security control where the resource failed.
- **Severity** – There are three levels of severity:
  - **High** – Address these issues immediately.
  - **Medium** – While not urgent, address these issues as soon as possible.
  - **Low** – Address these issues as time allows.
- **Result** – All items on the **Security Risks** page display as **Failed**.
- **Reason** – A brief description of why the resource failed. Note that a Reason is not always provided.
- **Status** – There are three potential status values:
  - **New** – You have not taken action on this item.
  - **Suppressed** – You suppressed this item. See below.
- **First Observed** – Time when this risk was first detected.
- **Last Observed** – Time when this risk was most recently detected.

- **Updated** – Time when an action was last taken on this risk, either by detection or by a user's action – like suppressing or remediating it.
- **More Details** – Toggle the arrow to see additional information for this risk.

Note: Some resources, like Secrets and Keys within KeyVault, do not use Azure role-based access control (Azure RBAC) and must provide access to the Barracuda Cloud Security Guardian scanner separately so they can be scanned. If you do not provide this access, these resources cannot be scanned and they will not appear in the **Security Risks** or **Security Findings** pages. For more information, refer to the Azure documentation for Azure RBAC.

Taking Action

Click a resource to view its details and take action.

For each resource, you have two options:

- **Suppress** – Click **Suppress** to change the Status for the Resource to **Suppressed**. To simplify the results on the **Security Risks** page, set the **Show Suppressed** slider to **OFF** to show only risks that you have not suppressed.
- **Console Remediation** – Select the **Console Remediation** tab and click the link to remediate the resource within either the AWS Security Hub or Azure Security Center. The next time the system is scanned, the status for this risk will be **Resolved**.
  Clicking the link brings you to one of these locations:
  - **Azure Security Center:** https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction
  - **Security Alerts in Azure Security Center:** https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview
  - **AWS Security Hub:**https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html
  - **Findings in AWS Security Hub:**https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings.html

After you resolve a risk, it is no longer available on the Security Risks page, but is still available on the Security Findings page.

Figures

1. SecurityRisksLarge.png
2. risksBadgeSmall.png