Security Findings

https://campus.barracuda.com/doc/93196220/

Navigate to the **Security Findings** page to view all of your resources with associated security findings. This page includes resources that have either passed or failed controls in your security policies.

By contrast, the **Security Risks** page shows only those resources that have failed conditions in your policies.

Security Findings Sources

Information on this page is sourced from the Barracuda Compliance Scanner. Azure Security Center alerts and AWS Security Hub findings are also periodically retrieved. As described below, use the **Source** filter on this page to select one or more information sources. When viewing the Finding Details, click a link to go to the source where the risk was found.

For more information, refer to the following resources:

- **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

Reviewing Findings

By default, information on this page is sorted by date, so the most recently-observed data is at the top.

You can take the following actions on the table to find and display data:

- Click a column to sort by it.
- Click **Columns** to show or hide columns on this page
- Click **Export JSON** to export the data, based on your current filters.

Findings for resources that no longer exist in your public cloud are hidden 24 hours after the resources have been removed.

Filtering Findings

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.

Click a resource to see its details.

- **Source** – Select one or more sources for the information on this page. Options include Barracuda Compliance Scanner, Azure Security Center, and AWS Security Hub.
- **See all risks from this source** – Click the link to view the **Risks** page, filtered to exclusively display all risks for this source.
- **Cloud 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** – Items on the **Security Findings** page might be either **Passed** or **Failed**.
- **Reason** – A brief description of why the resource passed or 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.
  - **Resolved** – You remediated this item. See below.
  - **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 Findings** or **Security Risks** 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 failed resource, you have the following options:

- **Suppress** – Click **Suppress** to change the Status for the Resource to **Suppressed**.
- **Unsuppress** – Click **Unsuppress** if you previously Suppressed the resource and have changed your mind. The status of the resource is no longer **Suppressed** and it is not **New**, so it becomes blank, symbolized by a hyphen character.
- **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.htm

|