Reports

https://campus.barracuda.com/doc/78809498/

Generate a report to visualize data from your cloud connections.

To create a report:

1. Within Barracuda Cloud Security Guardian, in the left menu, select **Reports**.
2. On the **Reports** page, select the **Report Name** you want to run. See **Report Types** below.
3. Depending on the Report Name you choose, additional information might be required. Select the information requested.
   Some fields you might need to select include:
   - **Cloud Connection** – Select which of your connections you want to view.
   - **Scan Type** – Select the standard to use for the report.
4. Click **Run Report**.
   The system generates a PDF file and saves it to your chosen download location.
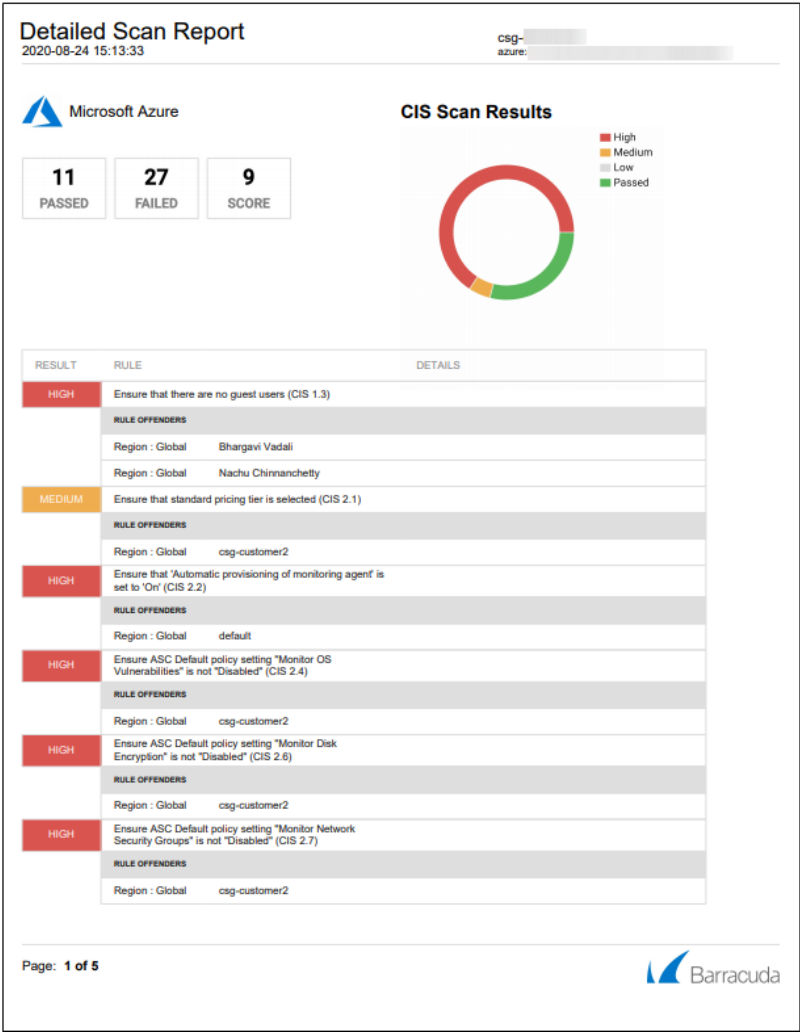
Report Types

Currently, the Detailed Scan Report is available. Additional Report Types will be released in the future.

Detailed Scan Report

Run a **Detailed Scan Report** for details about a single security standard (the Scan Type you select; e.g., NIST) for a single one of your cloud connections.

The report provides an overview section of your score for that security standard, based on how many of the controls your connection passed and failed. A graph shows the proportions of controls for which you have High, Medium, and Low risk, along with those controls that your connection passed. Below the overview, you can see how your cloud connection fares against each individual control within the selected standard.

You might choose to view a scan report from before a fix then a scan report from after the fix to compare them.

Barracuda Cloud Security Guardian

Detailed Scan Report
2020-08-24 15:13:33

csg-
azure:

Microsoft Azure

11	27	9
PASSED	FAILED	SCORE

CIS Scan Results

- High
- Medium
- Low
- Passed

RESULT	RULE	DETAILS
HIGH	Ensure that there are no guest users (CIS 1.3)	
	RULE OFFENDERS	
	Region : Global Bhargavi Vadali	
	Region : Global Nachu Chinnanchetty	
MEDIUM	Ensure that standard pricing tier is selected (CIS 2.1)	
	RULE OFFENDERS	
	Region : Global csg-customer2	
HIGH	Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (CIS 2.2)	
	RULE OFFENDERS	
	Region : Global default	
HIGH	Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled" (CIS 2.4)	
	RULE OFFENDERS	
	Region : Global csg-customer2	
HIGH	Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled" (CIS 2.6)	
	RULE OFFENDERS	
	Region : Global csg-customer2	
HIGH	Ensure ASC Default policy setting "Monitor Network Security Groups" is not "Disabled" (CIS 2.7)	
	RULE OFFENDERS	
	Region : Global csg-customer2	

Page: **1 of 5**

Barracuda

Figures

1. DSRreport.png