Health Overview Dashboard (Armor Anywhere)

This topic only applies to **Armor Anywhere** users.

To fully use this screen, you must add the following permission to your account:

- Read Dashboard Statistics

Overview

You can use the **Health Overview** screen to see the overall health status of virtual machines that contain the installed Armor Anywhere agent.

If you are a new user, then you may need to install the Armor Anywhere agent in order to receive data to populate this screen.

To learn how to install the agent, see Installation.

The top of the **Health Overview** screen contains four types of information, displayed in various widgets.

Widget	Description

Overall Health Score

This widget displays an average of the **Protection**, **Detection**, and **Response** scores.

> Scores in the security dashboards are calculated and updated every night at 2:00 AM UTC.

Protection

This score is based on the stability of the Armor agent and any corresponding subagents. For more information, see:

- Protection Dashboard (Armor Complete)
- Protection Dashboard (Armor Anywhere)

Detection

This score is based on the incoming activity (log activity) of the Armor agent and any corresponding subagents. For more information, see:

- Detection Dashboard (Armor Complete)
- Detection Dashboard (Armor Anywhere)

Response

This score is based on the response time for a support ticket between you and Armor. For more information, see:

- Response Dashboard (Armor Complete)
- Response Dashboard (Armor Anywhere)

Score range	Health status
10 - 8	Good
7 - 4	Fair
3 - 1	Poor

Critical Incidents	This widget displays the number of open or pending support tickets that are considered highly important, security-focused incidents, known as **Critical Incidents**. Internally, when Armor Support reviews a support ticket, a support personnel can label the ticket as a **Security Incident**. These tickets will be given a severity rating (**low**, **medium**, **high**, **critical**), and then displayed in the **Security Incidents** screen. A **Security Incident** with a **Critical** status is also known as a **Critical Incident**. In the **Security Incidents** screen, you will only see an incident if you are listed as a recipient on the support ticket or if you opened the support ticket. Armor Support, you, or someone on your account can open a support ticket that can eventually evolve into an incident. To learn more about the **Security Incident** screen, see: • Security Incidents (Armor Complete) • Security Incidents (Armor Anywhere) Under **Security Alerts Needing Attention**, you can click a specific incident, and then you will be redirected to the **Security Incident** screen with the table already filtered.
Logs Parsed (Past 24h)	This widget displays the number of logs that Armor has received and analyzed in the past 24 hours.
Vulnerabilities	This widget only applies to **Armor Anywhere** users. This widget displays the number of detected vulnerabilities, based on the information from the weekly vulnerabilities report. A vulnerability scan takes place every Sunday at 10:00 PM, local server time. After a scan is complete, the corresponding report is added to the **Vulnerability Scanning** screen of the Armor Management Portal (AMP). Additinoally, this widget is updated based on the scan. To learn about the **Vulnerability Scanning** screen, see Vulnerability Scanning (Armor Anywhere).

Review API calls

- Get Security Analytics Overview