MSFT Defender Reporting - Content Pack

Description

About Content Packs: FileWave is immensely powerful, but can be daunting when it comes to stitching the various components together. Content packs are meant to give you a leg-up in creating distributable content and are also a great way to learn by example! Each content pack is meant to be a "whole solution", putting together all of the pieces of FileWave to accomplish a goal.

About This Content Pack: This FileWave Content Pack focuses on reporting on Microsoft Defender Compliance, and gives you some really great custom field data and a dashboard built on the very same to show Defender is behaving in your environment. The purpose of this pack is provide the information you need to proactively manage your environment and is comprised of all of the contents listed below:

What You Get in this Content Pack

This content pack provides:

Custom Fields:

"Custom Fields" are a terrific way to extend the "inventory attributes" of your devices. In this content pack we have included:

- Defender App Version: Reads the version of the Defender App installed on the device (macOS/Windows)
- Defender Defs Version: Reads the version of the Defender Definitions installed on the device (macOS/Windows)
- Defender Defs Date: Reads the date of the Defender Defs installed on the device (macOS/Windows)
- Defender Engine Version: Reads the version of the Defender Engine installed on the device (macOS/Windows)
- Defender Health: At a high level indicates whether Defender is "healthy" on this device (macOS/Windows)
- Defender Threats Detected: Reads the threats log on the device (macOS/Windows)
- Defender Detailed Status: Gives verbose status on the Defender client (macOS/Windows)

> Note that the following report and dashboard are based upon the above custom fields. Those custom fields will only populate when the clients report in, so initially your report and dashboard will be empty, but will soon populate.

Reports (aka Inventory Queries):

Reports are a great way of measuring the effectiveness of distributing content, and can be used for all sorts of compliance purposes as well. Trust, but verify is what reports are all about. In this pack we have included the following reports:

- MSFT Defender Information: A report including data from the custom fields listed above for every Mac and Windows device. (You may want to further edit this report to only look at "Last Connected" for a certain time range to make sure you are only reporting compliance on "active" devices.)

Dashboards:

Dashboards build upon reports and are an incredibly powerful tool for showing aggregated data in charts and graphs. This pack provides the following dashboard:

- Defender Dashboard: A collection of compliance charts that give you summary and detail information on Defender health, threat status, and overall compliance to your security standards.

Ingredients

- FileWave Central Admin & Credentials
- Base64 API Token
- Content Pack:

(Only one of the following is needed, based on your admin device's OS platform)

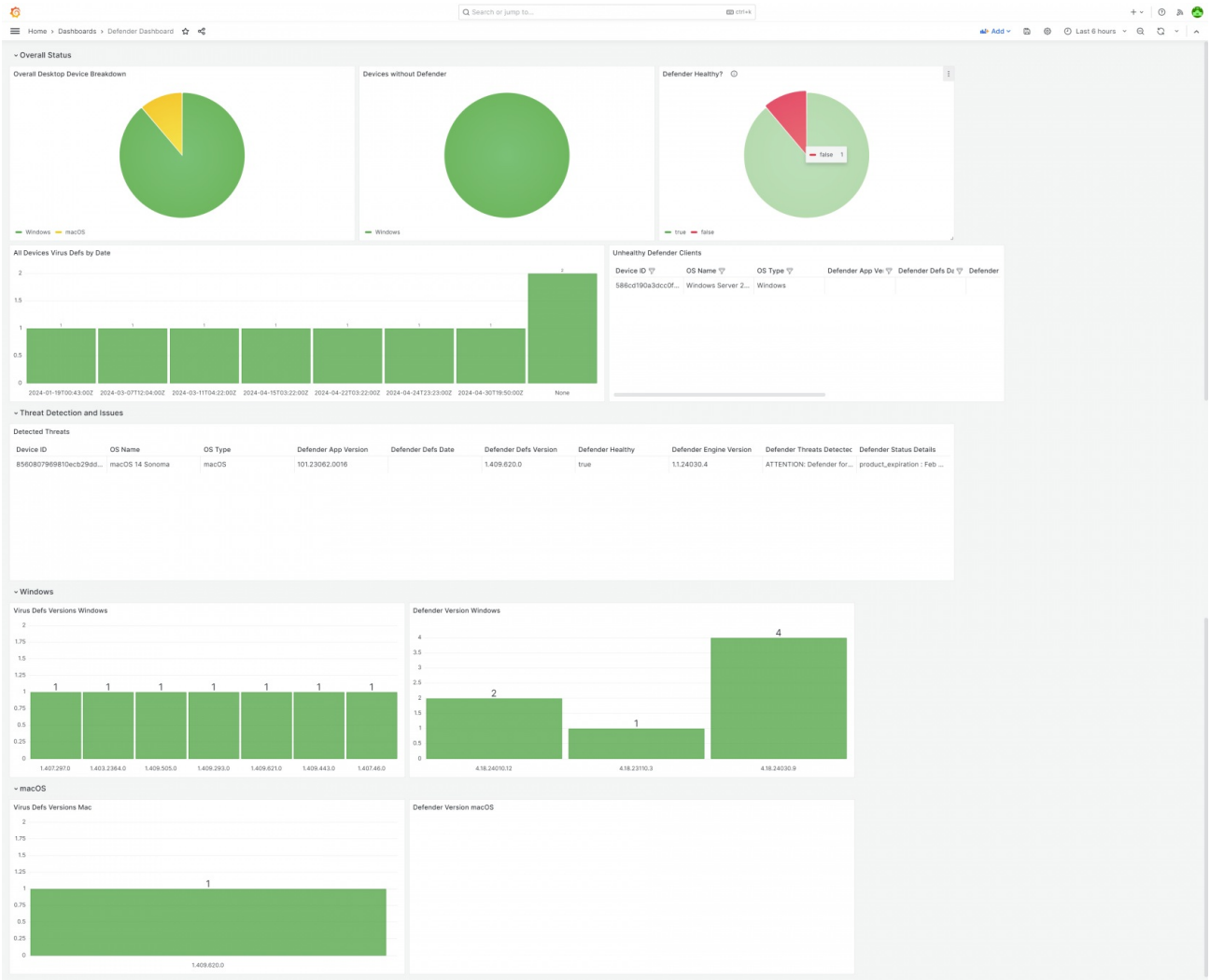
Windows Content Pack	Windows Content Pack Download
macOS Content Pack (ARM based)	> On macOS, we need to use curl to download so that Gatekeeper doesn't quarantine the import application. You can copy and paste the following into Terminal.app...the example provided downloads import_pack.zip to the desktop `curl -o ~/Desktop/import_pack.zip https://kb.filewave.com/attachments/342`

macOS Content Pack (Intel based)	On macOS, we need to use curl to download so that Gatekeeper doesn't quarantine the import application. You can copy and paste the following into Terminal.app...the example provided downloads import_pack.zip to the desktop `curl -o ~/Desktop/import_pack.zip https://kb.filewave.com/attachments/343`

Directions

1. Download the appropriate content pack above (based on your admin device's platform) and unzip it
2. Run the user_interface tool in the user_interface folder, using appropriate credentials for your environment (check out our overview article on importing content packs here)
3. Once completed, verify the new content in your system (and import the dashboard)

Sample Screenshots



Notes

Note that you can freely edit any of the content in this content pack. We do recommend reviewing each of the types of content as provided first though so that you can get a feel for how things "fit together" before modification.

Related Content

- How to Import a Content Pack

- Getting an API Token
- Importing a Grafana Dashboard
- Content Packs
- More Info on how to use:
  - Custom Fields
  - Client Group Structure
  - Inventory Reports
  - Custom Dashboards

Revision #10
Created 1 May 2024 13:33:36 by Tony Keller
Updated 3 October 2024 13:43:38 by Josh Levitsky