Crowdstrike: RFM & EOS

Crowdstrike includes a number of tools designed to provide visibility into your managed assets. This article focuses on devices in End of Support and Reduced Functionality Mode, including what these statuses mean and how you can track these assets in your environment.

What is End of Support?

Devices in End of Support (or EOS) are running an Operating System that is no longer receiving support or security updates from the manufacturer. This is a concern because new OS vulnerabilities are constantly being discovered, so an Operating System that is no longer supported or updated will only become less and less secure over time. Devices in EOS should be found and updated or replaced as soon as possible. Note: the EOS status is currently available only for Windows and MacOS.

What is Reduced Functionality Mode?

Reduced Functionality Mode (or RFM) is a status that the Crowdstrike Sensor will enter when an asset's kernel is uncertified or unsupported by the sensor. There are a few reasons this can happen:

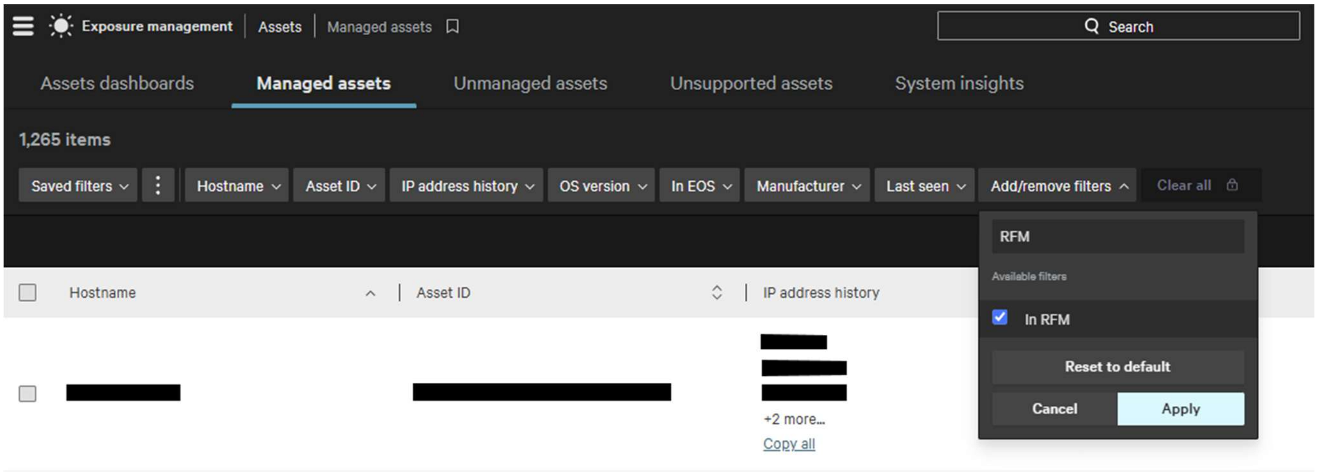
- **Windows Updates** that alter the OS kernel can cause assets to enter RFM until the update is certified by Crowdstrike. This certification typically occurs 24-48 hours after the update has been released and will resolve any related RFM statuses automatically.
- **Macs** may show as RFM if Full Disk Access is not enabled on the host. Enabling Full Disk Access, either directly on the host or via an updated MDM profile, is needed to remove the RFM status.
- The **Operating System** itself may no longer be supported by Crowdstrike. This would typically mean that the device is also in EOS. Updating to a supported OS will resolve the RFM and EOS statuses.

What happens if my devices are in RFM?

It depends on which OS your RFM assets are running. For instance, RFM on Linux prevents *any* sort of detections from occurring, so Crowdstrike is powerless to stop threats until the issue is resolved. In Windows and MacOS RFM can lead to reduced sensor visibility and in some cases result in missed detections, but it's generally not quite as concerning as RFM in Linux.

Finding EOS and RFM devices in your environment:

- In **Exposure Management > Managed Assets** you can filter on the 'In EOS' and/or 'In RFM' status to generate a list of impacted assets. If either filter is not visible, they can be added by clicking the 'Add/remove filters' button. You can use the 'Saved Filters' menu to save this view for future use:



1,265 items

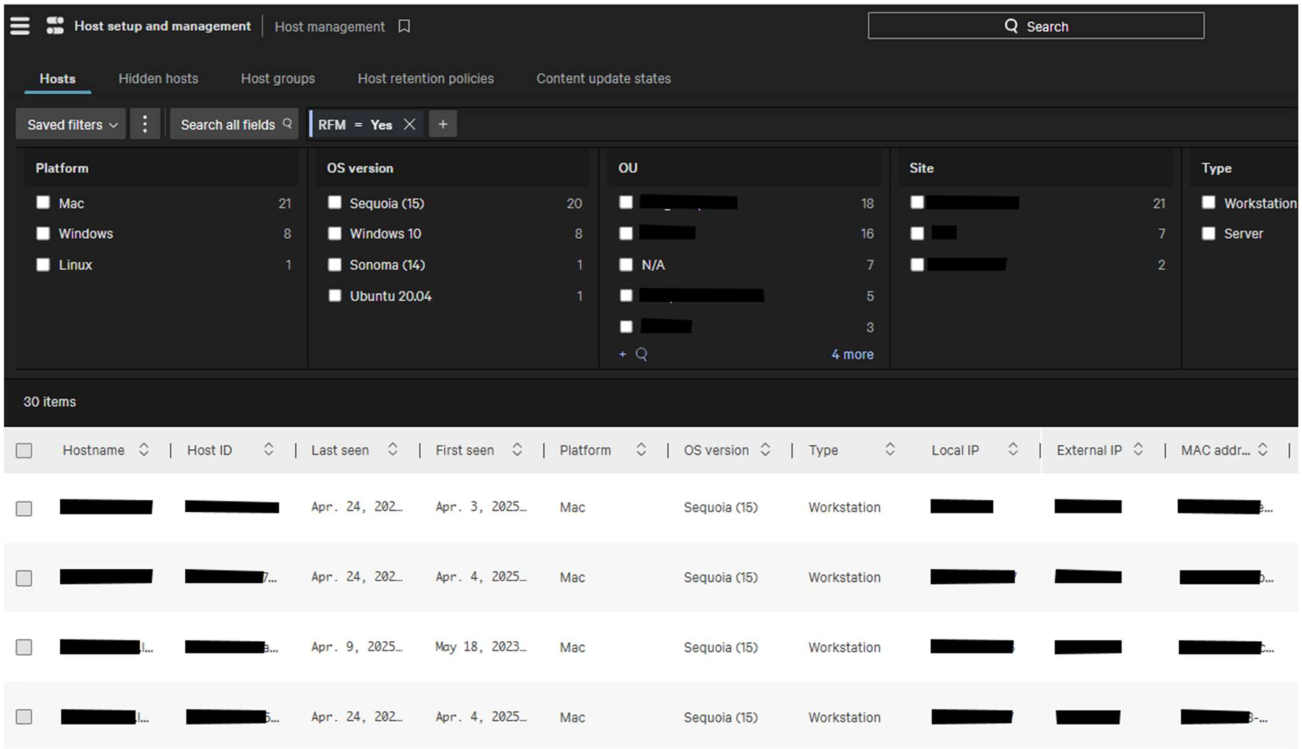
RFM

☑ In RFM

□ [redacted] [redacted] [redacted]

These lists can be exported to CSV or JSON to share with staff members without Crowdstrike access.

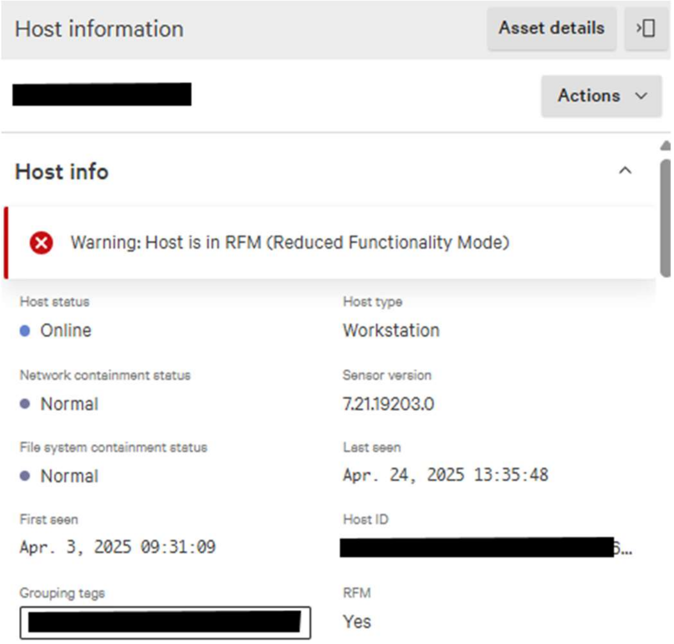
- RFM assets are also searchable and visible in **Host Management**.



Platform		OS version		OU		Site		Type
□ Mac	21	□ Sequoia (15)	20	□ [redacted]	18	□ [redacted]	21	□ Workstation
□ Windows	8	□ Windows 10	8	□ [redacted]	16	□ [redacted]	7	□ Server
□ Linux	1	□ Sonoma (14)	1	□ N/A	7	□ [redacted]	2	
		□ Ubuntu 20.04	1	□ [redacted]	5			
				□ [redacted]	3			
				+ 4 more				

30 items

□	Hostname	Host ID	Last seen	First seen	Platform	OS version	Type	Local IP	External IP	MAC addr...
□	[redacted]	[redacted]	Apr. 24, 202...	Apr. 3, 2025...	Mac	Sequoia (15)	Workstation	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	Apr. 24, 202...	Apr. 4, 2025...	Mac	Sequoia (15)	Workstation	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	Apr. 9, 2025...	May 18, 2023...	Mac	Sequoia (15)	Workstation	[redacted]	[redacted]	[redacted]
□	[redacted]	[redacted]	Apr. 24, 202...	Apr. 4, 2025...	Mac	Sequoia (15)	Workstation	[redacted]	[redacted]	[redacted]



[redacted]

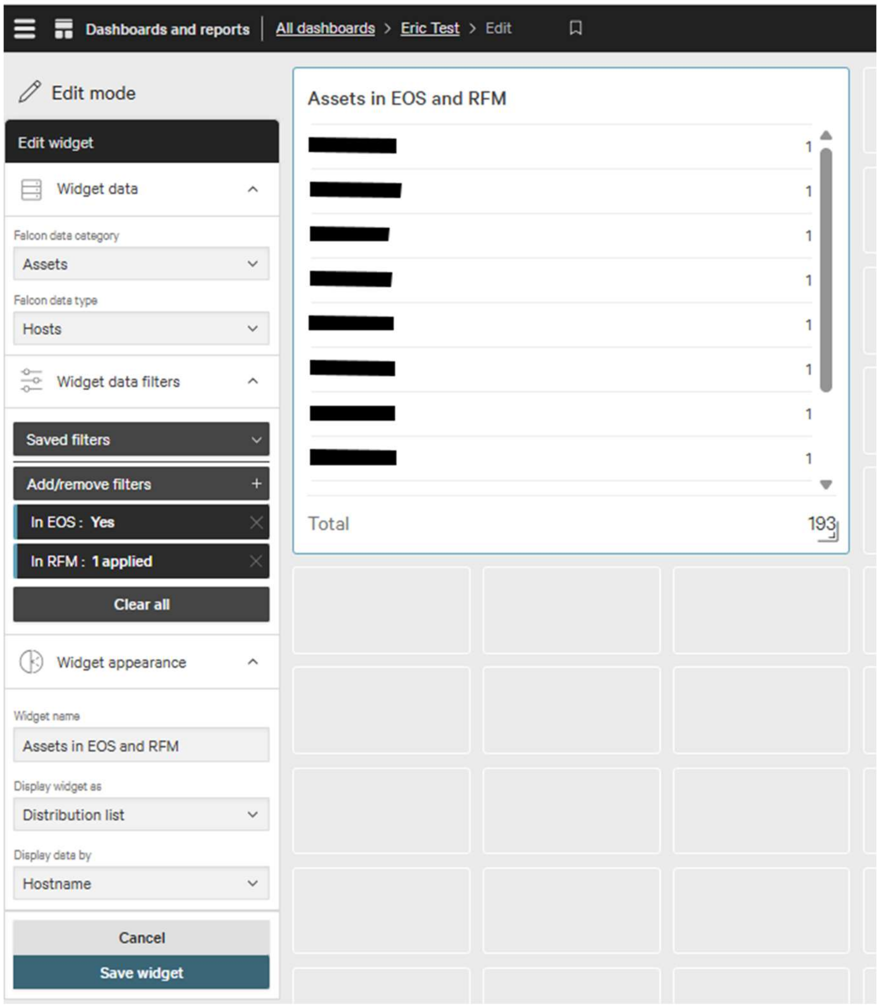
Host info

Warning: Host is in RFM (Reduced Functionality Mode)

Host status ● Online	Host type Workstation
Network containment status ● Normal	Sensor version 7.21.19203.0
File system containment status ● Normal	Last seen Apr. 24, 2025 13:35:48
First seen Apr. 3, 2025 09:31:09	Host ID [redacted]
Grouping tags [redacted]	RFM Yes

- **Custom Dashboards** allow you to pull together information from different Crowdstrike modules into a single destination. This is a great way of keeping track of everything you may care about in Crowdstrike without needing to spend a lot of time clicking around to different areas of the console. You can even send out a custom dashboard as a scheduled report, which allows you to receive the information via email at your preferred cadence.

There are many preset widgets available, and you can build custom widgets to fit your needs. In this example we've built a widget that pulls Hosts data from the Assets module, filters our view to look at assets in EOS and RFM, then sets the appearance to show a list of hostnames that meet those criteria.



Falcon data category: Assets

Falcon data type: Hosts

In EOS : Yes

In RFM : 1 applied

Widget name: Assets in EOS and RFM

Display widget as: Distribution list

Display data by: Hostname

Assets in EOS and RFM

[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
[redacted]	1
Total	193

If you are interested in tracking RFM and EOS in your environment or you have questions about resolving these issues, please contact MCNC Security Operations at secops@mcnc.org.