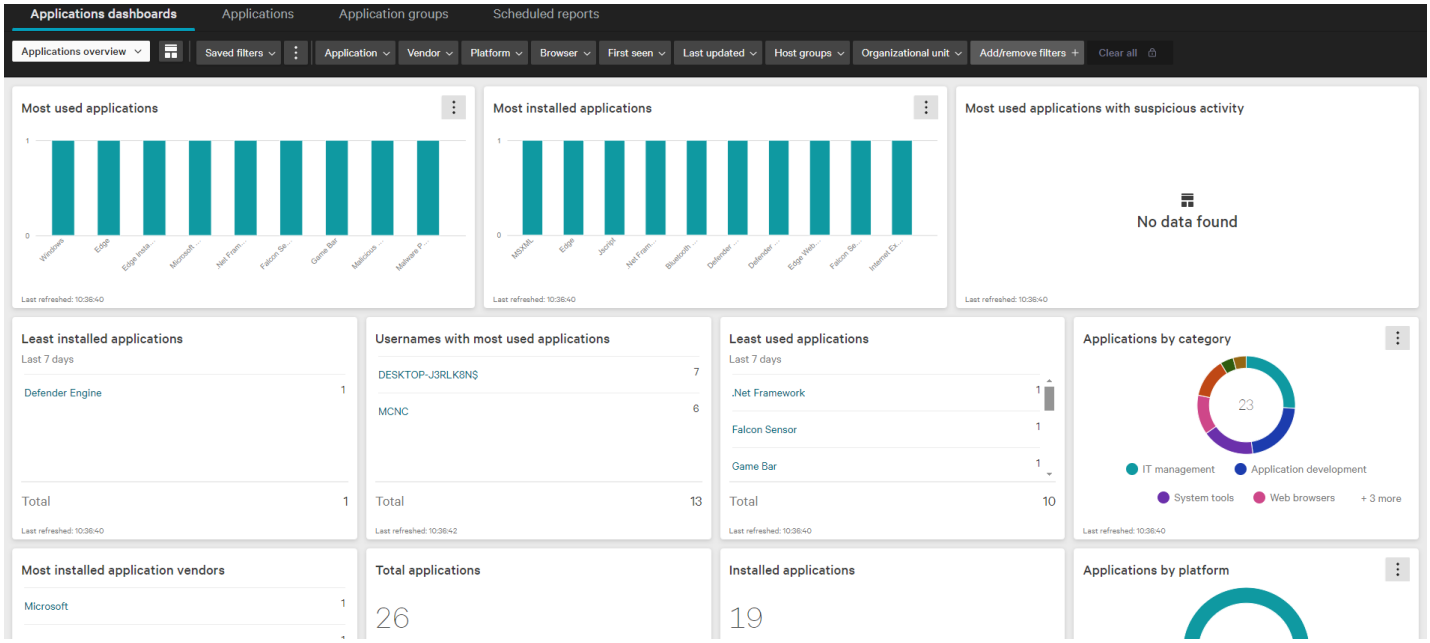
Exposure Management - Applications

Crowdstrike provides many tools that allow increased visibility into your managed assets. Today we're going to take a look at the Application visibility within the Exposure Management module.

Dashboards

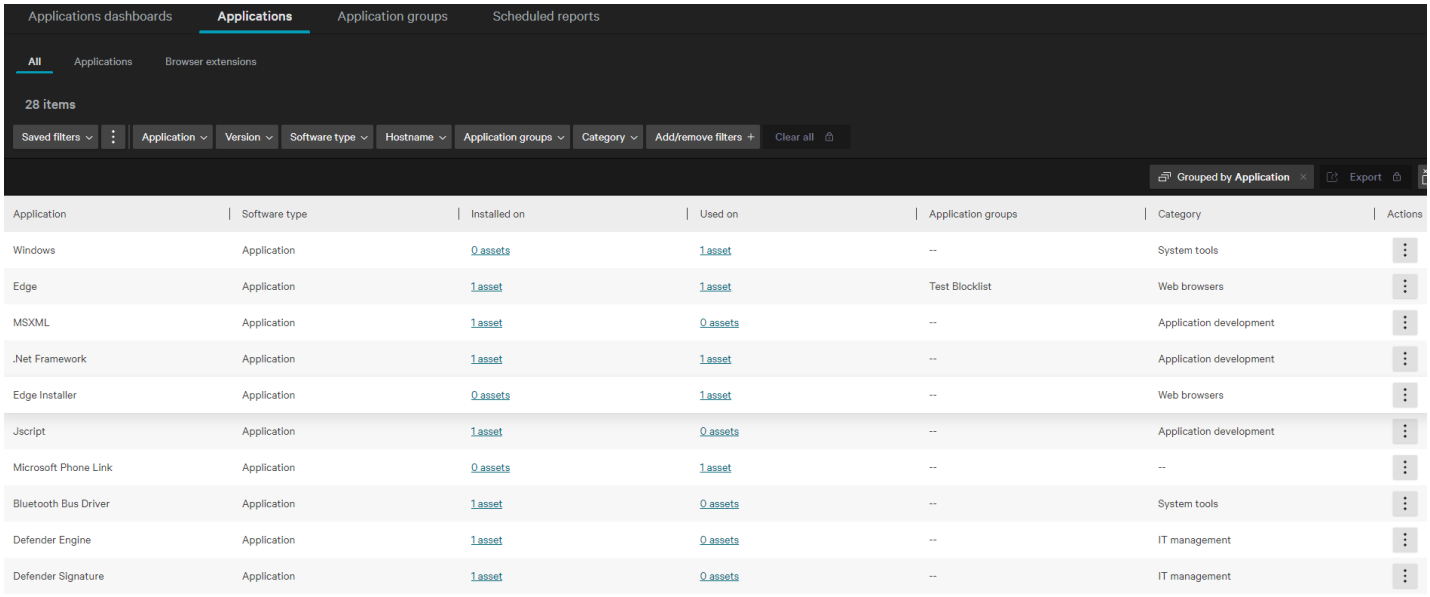
Like most areas of the Crowdstrike console, the Application view starts with a dashboard view. By going to Exposure Management>Applications>Dashboards, you can get an idea of the visibility it provides.



There's too much here to include in a screenshot, but this is a great starting point for looking at what applications are installed. We can see which apps are most used, installed apps by category, uncommon apps, etc. These dashboards can also be filtered via the dropdown menu at the top, so if you'd like a view into apps for a specific OU or asset type that's easily doable. Many of the widgets are interactive, so clicking through is an quick way to look at interesting things in more detail.

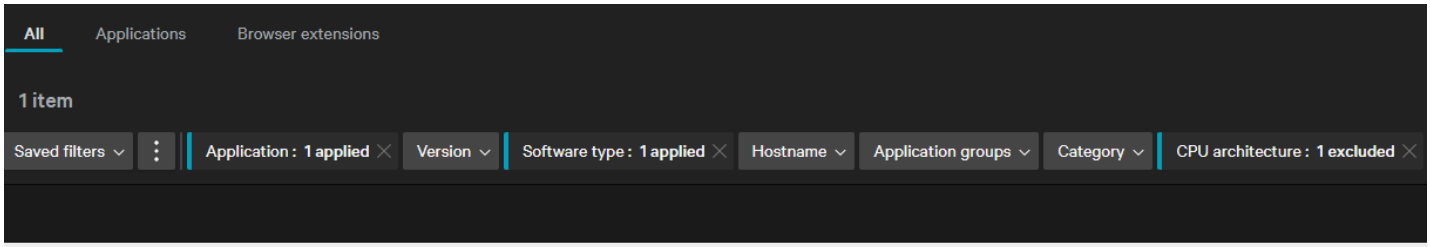
Applications

Now we'll get into the data behind the dashboards. Here we're looking at all applications that are installed and have been used in our (not very active) test CID.



Application	Software type	Installed on	Used on	Application groups	Category	Actions
Windows	Application	0 assets	1 asset	--	System tools	
Edge	Application	1 asset	1 asset	Test Blocklist	Web browsers	
MSXML	Application	1 asset	0 assets	--	Application development	
.Net Framework	Application	1 asset	1 asset	--	Application development	
Edge Installer	Application	0 assets	1 asset	--	Web browsers	
Jscript	Application	1 asset	0 assets	--	Application development	
Microsoft Phone Link	Application	0 assets	1 asset	--	--	
Bluetooth Bus Driver	Application	1 asset	0 assets	--	System tools	
Defender Engine	Application	1 asset	0 assets	--	IT management	
Defender Signature	Application	1 asset	0 assets	--	IT management	

We can click on any of the results in the 'installed on' or 'used on' columns to get a breakdown of which assets have installed or used a specific application.



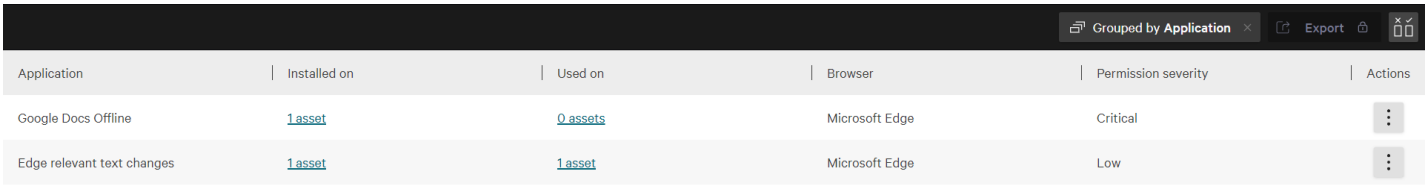
Hostname	Asset ID	Installed applications	Used applications	Application
MCNC-ELEE-LAB-3	d0ed65999f764161a07d5373c4f317...	1 application 0 browser extensions	1 application 0 browser extensions	Falcon Sensor

By default the grouping is set to 'Grouped by Application', which aggregates data at the application level. However, there are other options including the ability to group by Application Version. This can be really helpful if you are looking for older software that may be out of support or vulnerable to a new zero-day.

Edge	1.3.195.25	Application	1 asset	0 assets
Edge	124.0.2478.67	Application	0 assets	1 asset
Edge	129.0.2792.89	Application	1 asset	1 asset

Browser Extensions

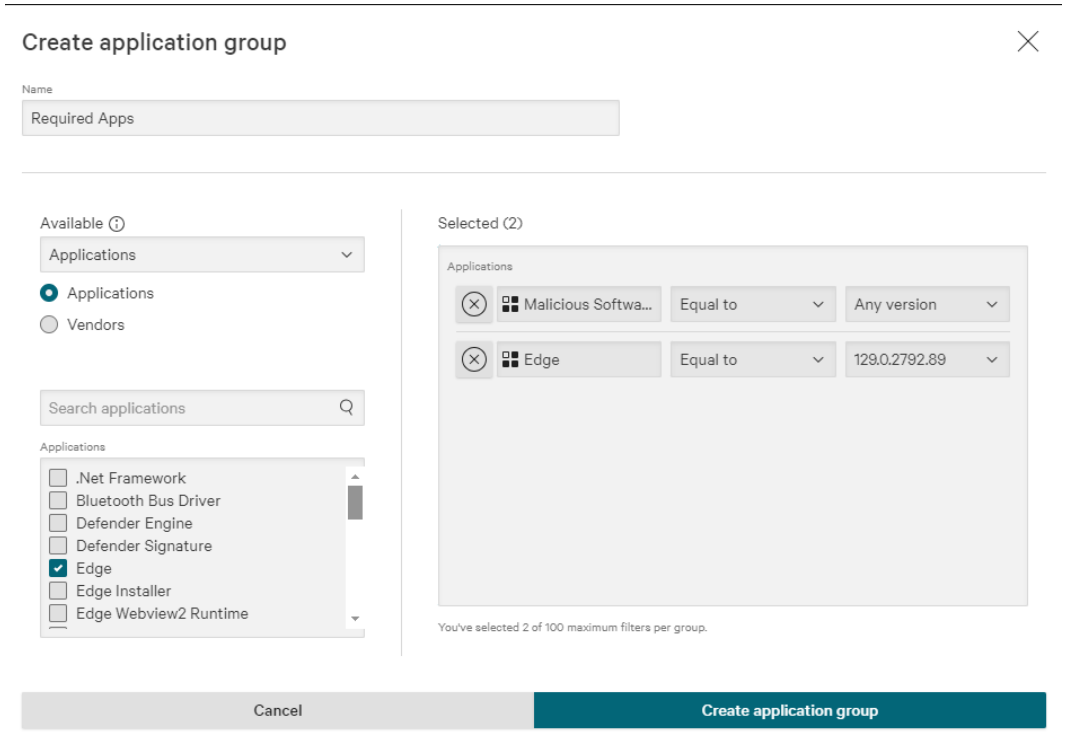
In addition to applications, Crowdstrike has recently updated the Exposure Management visibility to highlight installed browser extensions. We can see not only which extensions are installed where; Crowdstrike also assesses extensions based on the level of permissions the extensions have. This can be useful to track unwanted extensions in your environment that may be risky to your users.



Application Groups

Another relatively new feature is the ability to create and manage Application Groups. Application Groups are used to track certain applications in your environment. This could be applications that are supposed to be installed on all managed assets (think things like MDM tools, patch management, etc) or it could be applications that shouldn't be installed anywhere (games, unwanted tools, etc). Once created, you can leverage these groups to get notification any time an asset falls outside your defined policy.

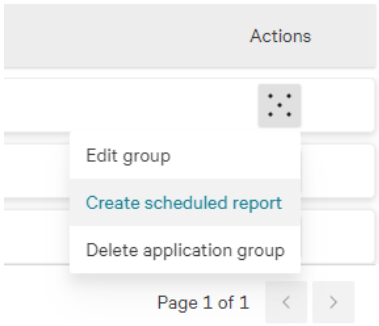
Here's a quick example. We'll create an application group for 'Required Apps'.



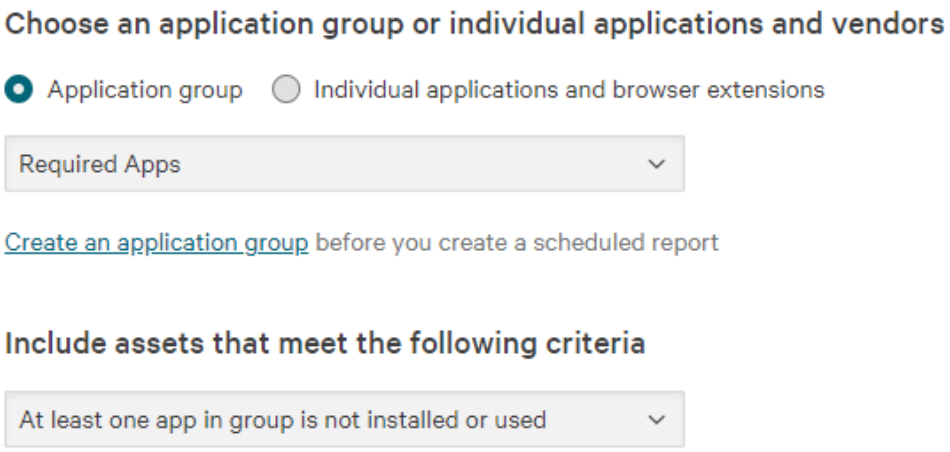
As you can see, you can add specific versions or just look for the presence of the app itself. In some cases you can also check for versions ‘Less Than’ or ‘Greater Than’ a specific version, but this is dependent on the formatting of the reported version and is not always an option.

Scheduled Reports

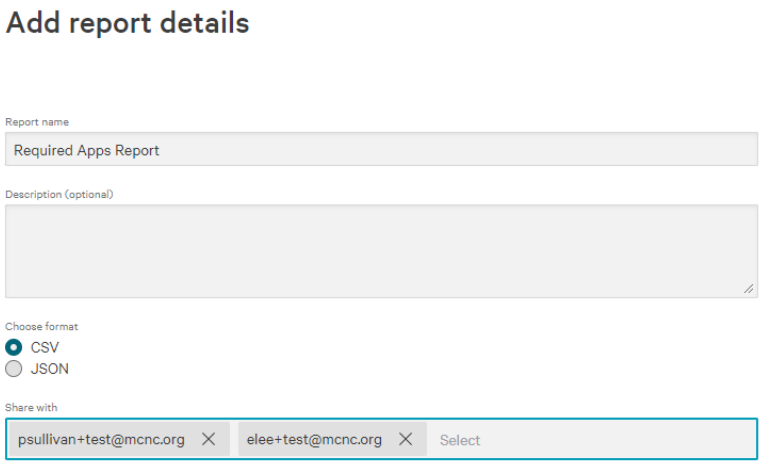
Once we’ve created the group we can set up a scheduled report that will email us whenever a managed asset *doesn’t* have a required app installed.



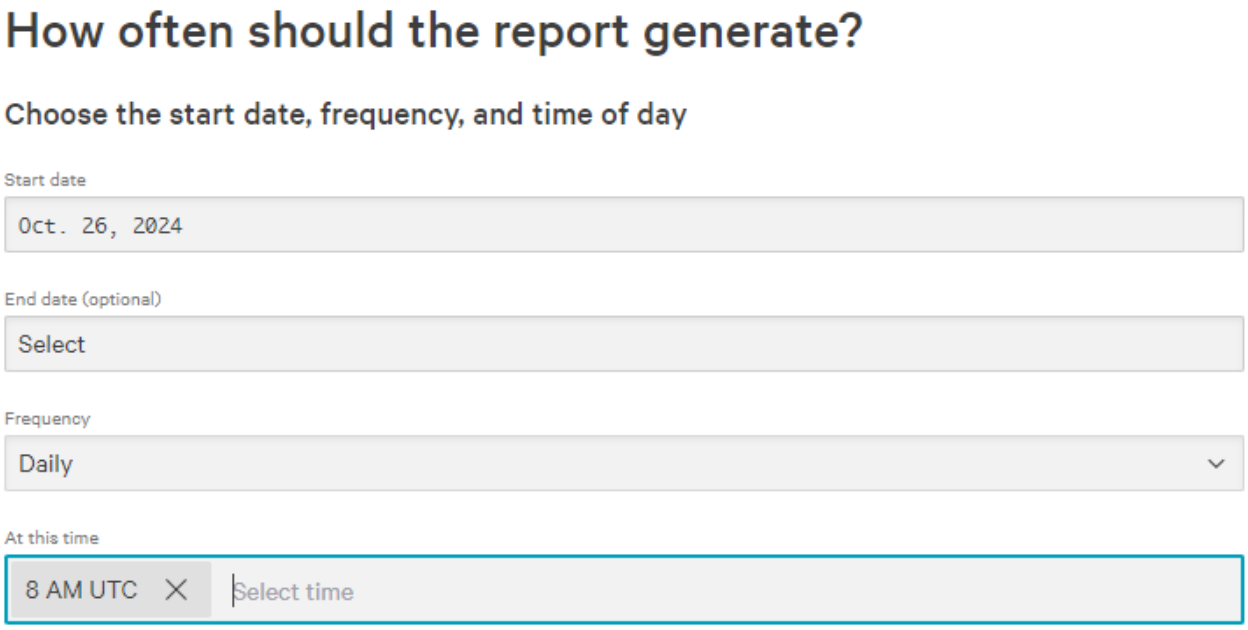
From the action menu next to the report, go to ‘Create scheduled report’. The group should already be selected for you. In this example we’re looking at ‘Required Apps’, so we’ll want to know whenever one of our assets doesn’t have one or more of those required apps.



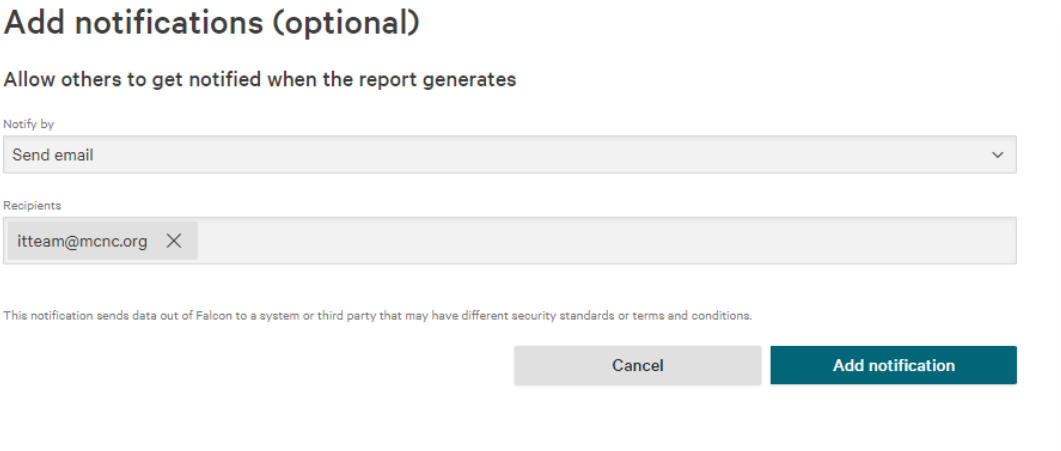
You can also filter for specific device types or groups, but I'll leave it unfiltered so we're monitoring all our assets. Now we just need to finish the report creation. We'll name it, choose the format and who we're sharing with.



On the next page we'll select the schedule. We'll run this report every morning.



Finally, we'll choose whether we want to send out notifications when the report is generated (you'll only get an email if the report has content). You can email the notification to whomever you want, so feel free to use a distribution list here, but anyone who gets the email will still need a Crowdstrike account to access the report so keep that in mind.



Once you've created a scheduled report you can access it within 'Dashboards and Reports>Scheduled reporting'. From here you can edit parameters, run the report on-demand, update scheduling, disable, delete, or view historical reports. There are also plenty of other types of scheduled reports you can create using these tools, which we may cover in a future document.