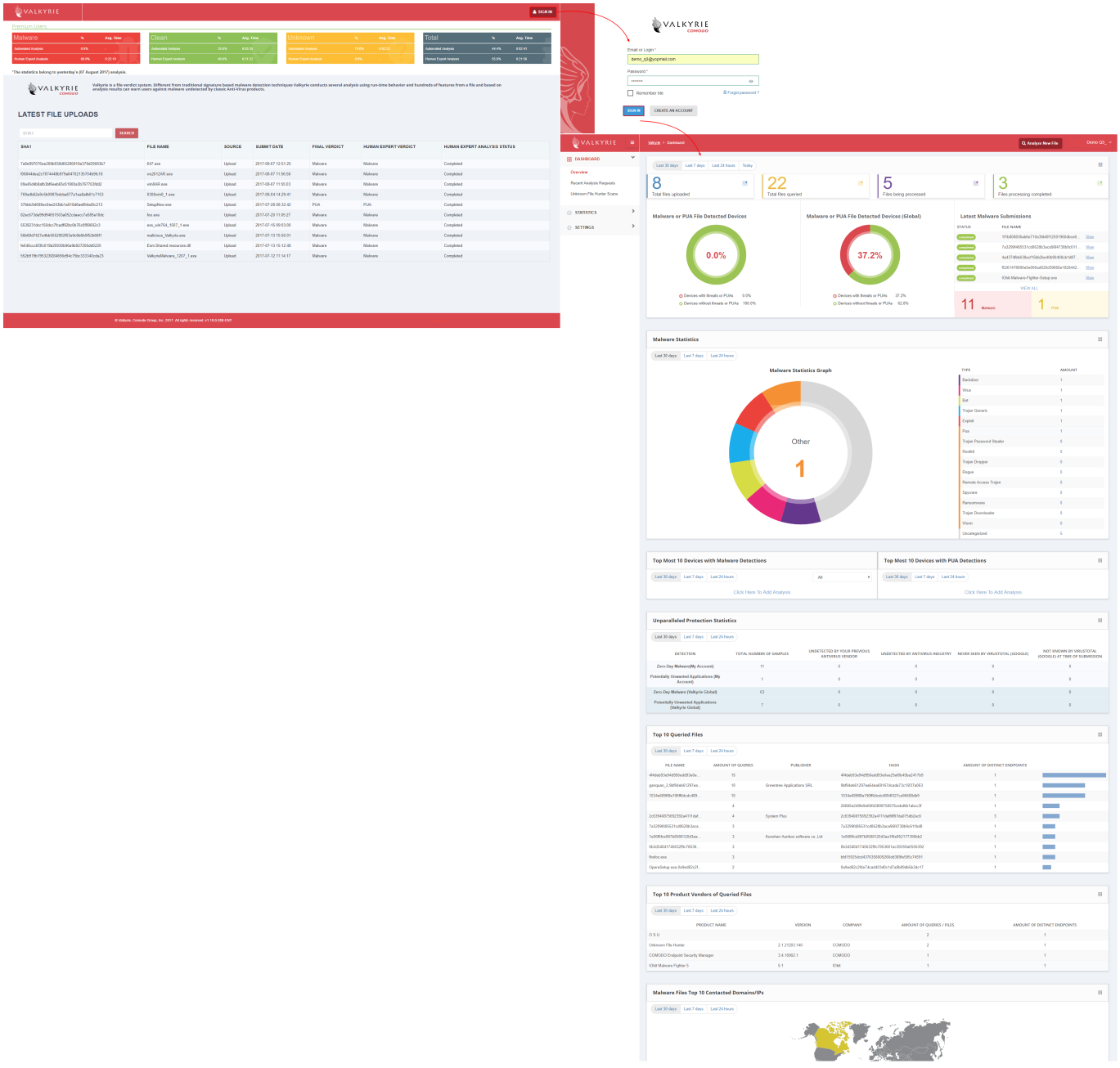
How to check Valkyrie dashboard Overview

The functionality for the Valkyrie Dashboard has been enhanced with an overview, recent analysis requests and unknown file hunter scans sections on Overview as a friendly way of analyzing the file.In this section, we are going to concentrate on Dashboard Overview.

Step [1]: Login into Valkyrie,
Go to --> https://valkyrie.comodo.com click Sign In Button which is available on the top most corner of the page, by clicking it will navigate to signup page on that provide credentials of your C1 account and click "Sign In" Button.It will display the Valkyrie dashboard Overview which provides the overall statistics for the devices that have been linked to a user account

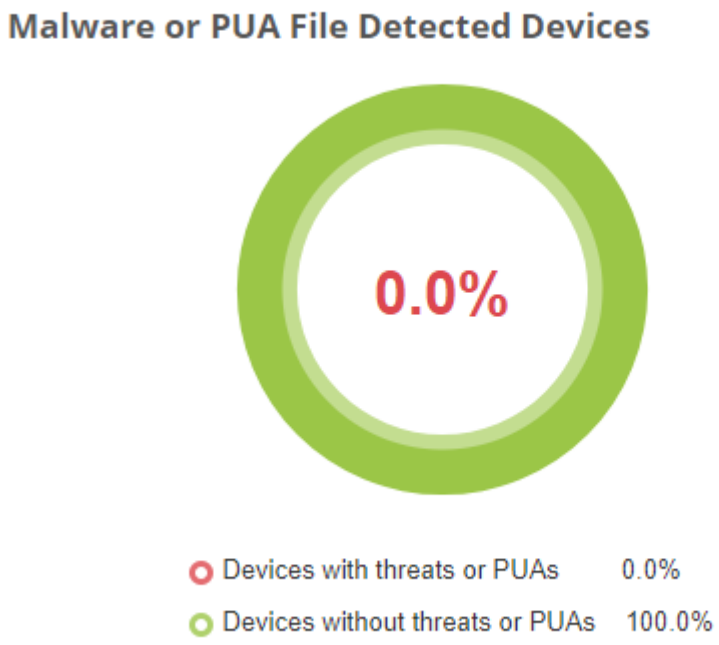


DashBoard Overview:

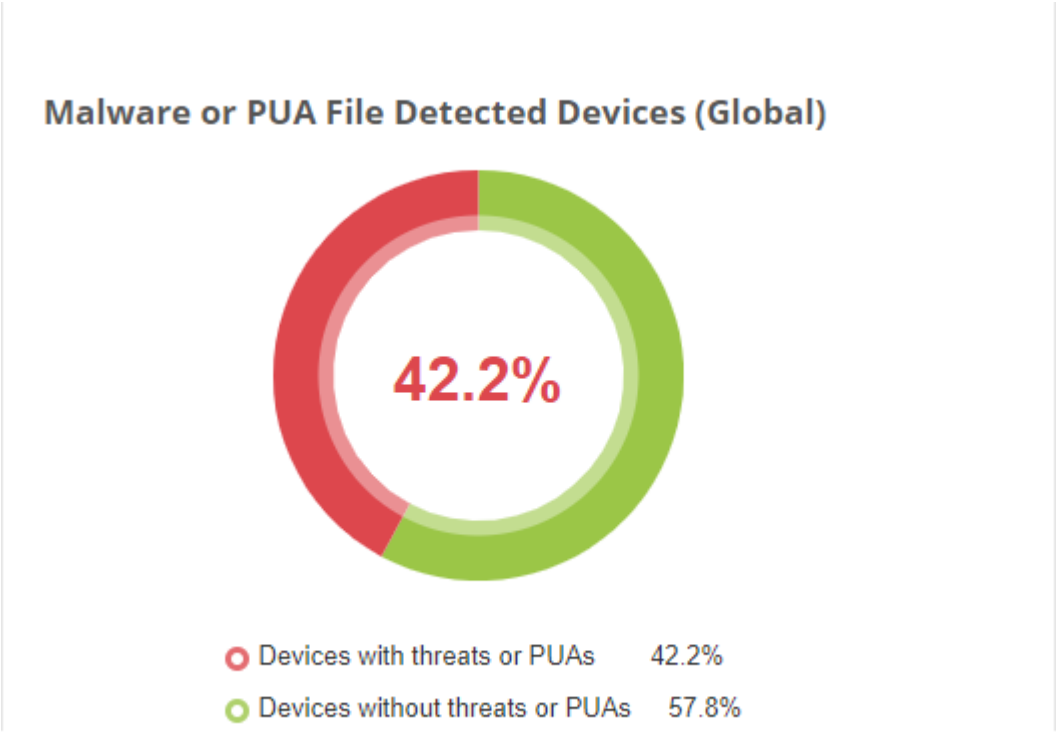
The dashboard provides the overall statistics of the devices that are linked to a user account.It has many sections for detecting risk that is enrolled to a particular account.The overall statistics of the Total Files

Upload, Total Files Queried, Files being Processed and Files Being Completed Statistics have been provided on the top.By this feature, users can able to track the file details.Newly they have provided the feature for analyzing the file on the top with "Analyze new file" as an user-friendly.

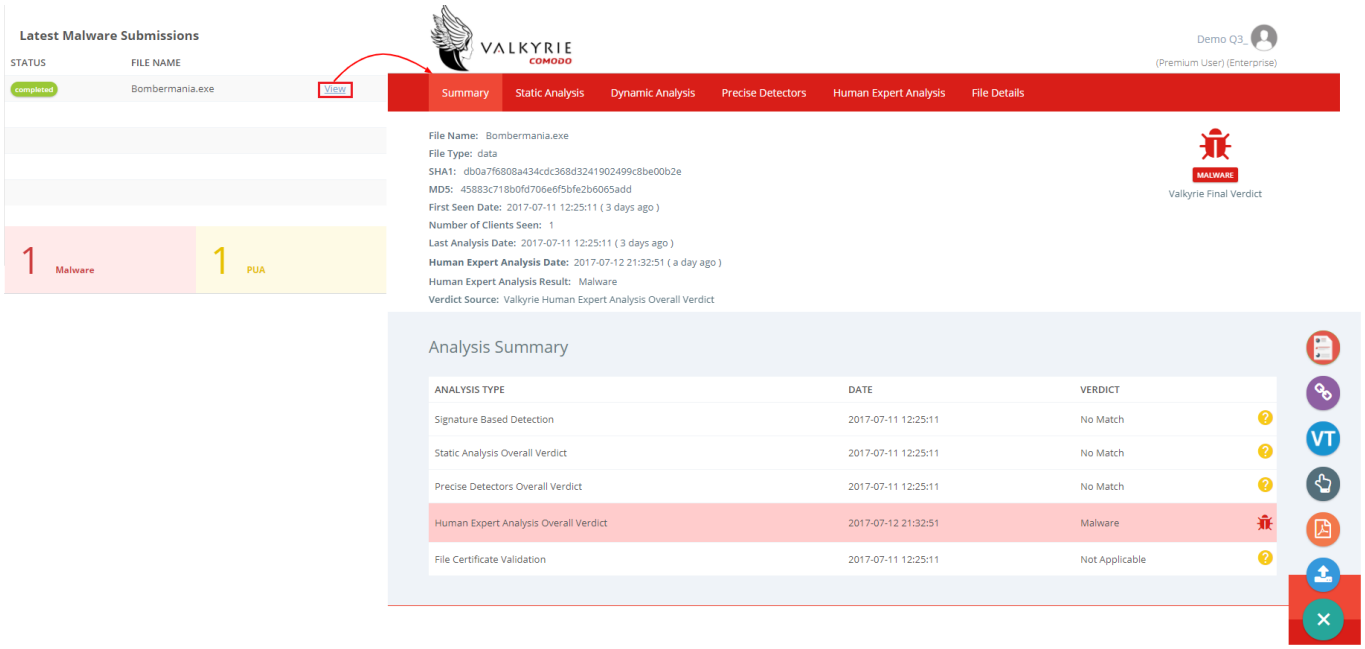
Malware or PUA File Detected Devices: This field depicts the diagrammatic representation of the devices with or without threats of PUAs.By this feature, a user can able to view the device details of the affected malware file.



Malware or PUA File Detected Devices (Global): It illustrates the diagrammatic representation of the devices with or without threats or PUAs as like Malware or PUA file detected devices but in a global manner.



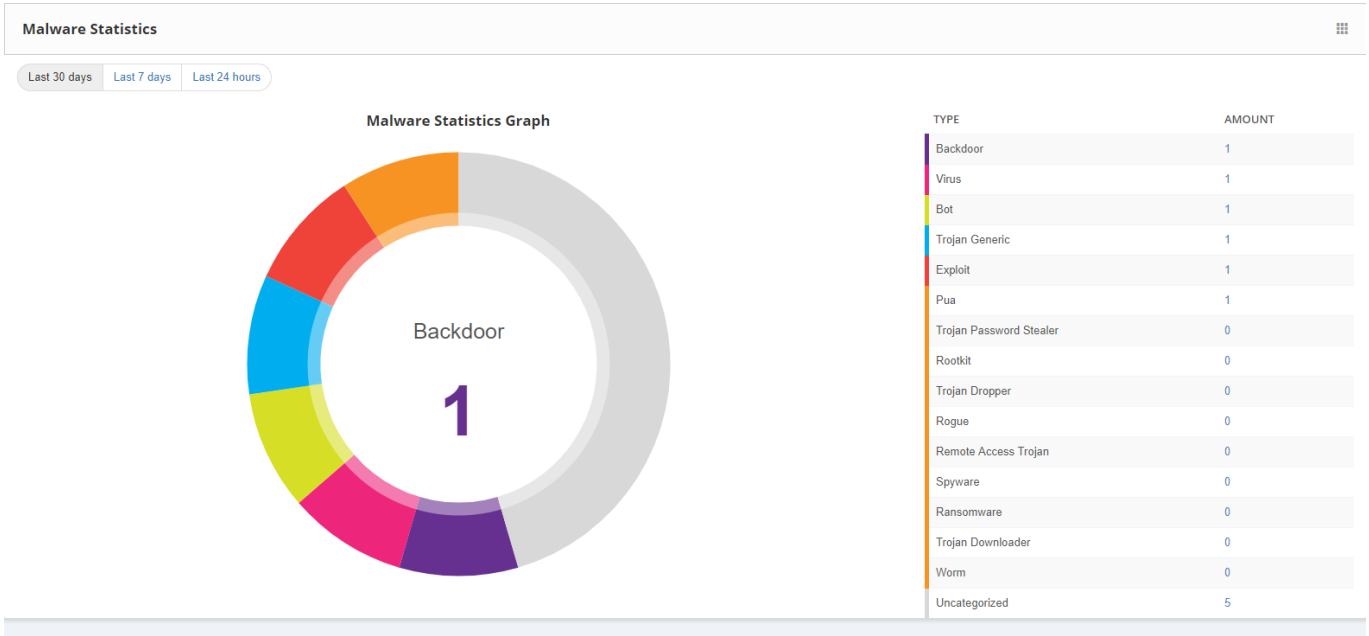
Latest Malware Submissions: It displays the records of the latest malware submissions along with the status.By clicking the view button, it navigates to the next page where a detailed description of the selected malware file resides.Based on the file report it will be placed on PUA and malware file list present on the bottom.This widget lists the most recently detected files along with the result without searching the particular file information.



Malware Statistics: It displays the report of the malware files as a statistic graph.By this new widget, users can able to view the distribution of malware file according to the malware families.

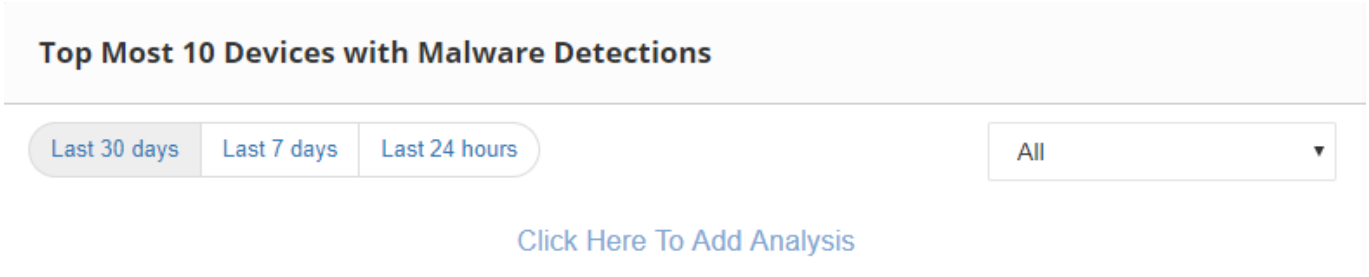
Note:

- We can add the file to an analysis by clicking the Click here to Add Analysis.
- Sorting the file details can be done by selecting the last 30 days, last 7 days and last 24 hours.
- We can simply move the fields of the dashboard by using widgets.

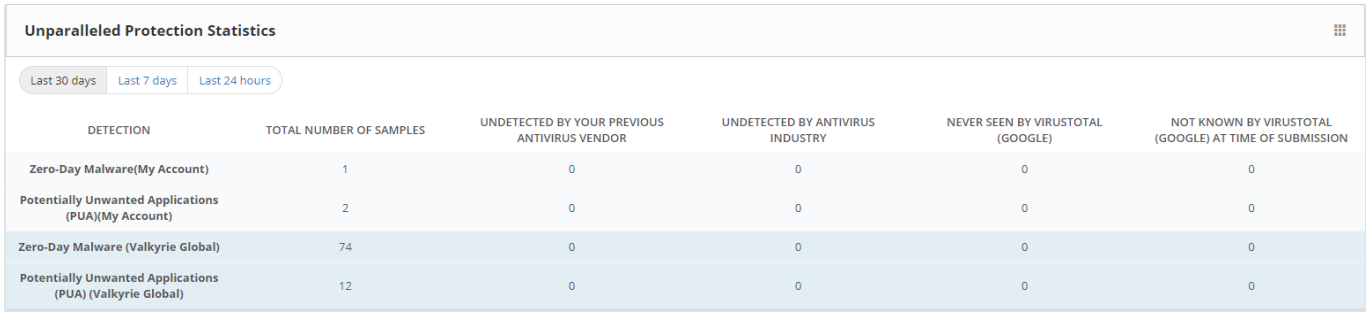


Top Most 10 Devices with Malware Detections: It lists the devices where the malware files have been analyzed.By this feature, users can able to protect the devices which are more vulnerable for the malware

files.



Unparalleled Protection Statistics: This displays the detection files based upon Zero-Day Malware(My Account), Potentially Unwanted Applications (PUA)(My Account), Zero-Day Malware (Valkyrie Global), Potentially Unwanted Applications (PUA) (Valkyrie Global) with the Total no. of samples, Undetected by your previous antivirus vendor, Undetected by Antivirus Industry, Never seen by Virus Total(Google) and not known by virus total (Google) at the time of submission.This feature used for viewing malware and PUA file which are not detected by any company before and this helps the user to take some precautionary measures

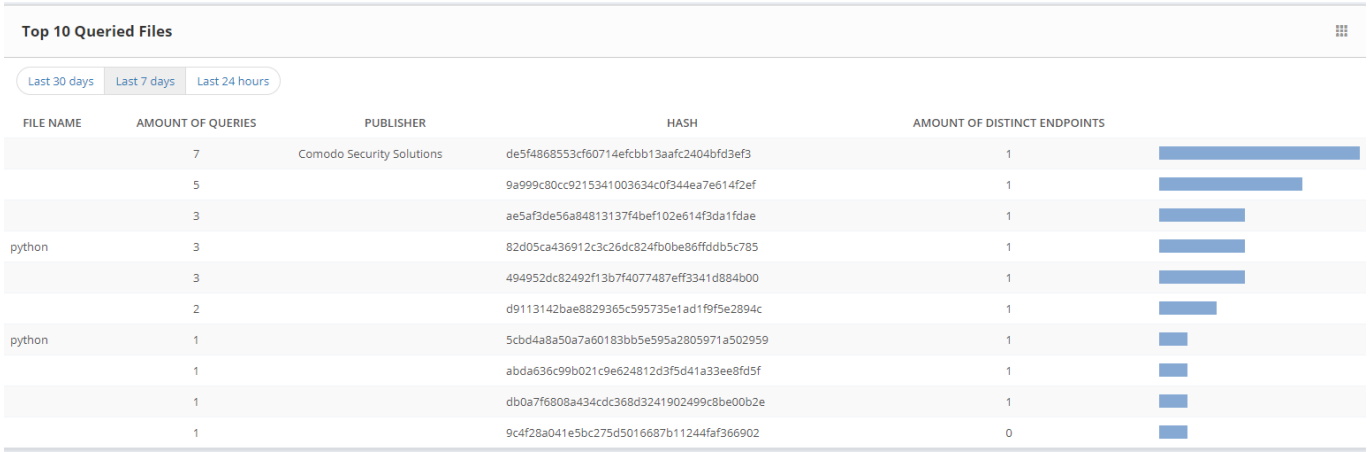


Unparalleled Protection Statistics

Last 30 days | Last 7 days | Last 24 hours

DETECTION	TOTAL NUMBER OF SAMPLES	UNDETECTED BY YOUR PREVIOUS ANTIVIRUS VENDOR	UNDETECTED BY ANTIVIRUS INDUSTRY	NEVER SEEN BY VIRUSTOTAL (GOOGLE)	NOT KNOWN BY VIRUSTOTAL (GOOGLE) AT TIME OF SUBMISSION
Zero-Day Malware(My Account)	1	0	0	0	0
Potentially Unwanted Applications (PUA)(My Account)	2	0	0	0	0
Zero-Day Malware (Valkyrie Global)	74	0	0	0	0
Potentially Unwanted Applications (PUA) (Valkyrie Global)	12	0	0	0	0

Top 10 Queried Files: It displays the last analyzed files in user devices.By this feature, it allows the files that are seen on the endpoint which was analyzed.

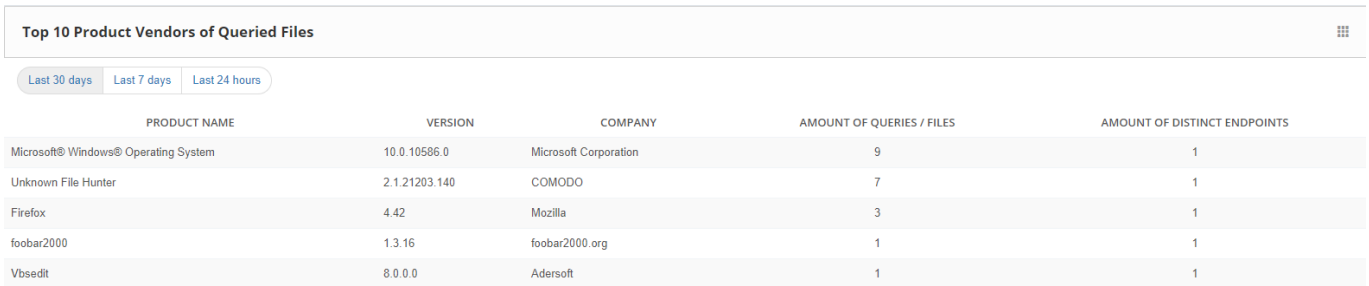


Top 10 Queried Files

Last 30 days | Last 7 days | Last 24 hours

FILE NAME	AMOUNT OF QUERIES	PUBLISHER	HASH	AMOUNT OF DISTINCT ENDPOINTS
	7	Comodo Security Solutions	de5f4868553cf60714efcbb13aafc2404bfd3ef3	1
	5		9a999c80cc9215341003634c0f344ea7e614f2ef	1
	3		ae5af3de56a84813137f4bef102e614f3da1fdae	1
python	3		82d05ca436912c3c26dc824fb0be86ffddb5c785	1
	3		494952dc82492f13b7f4077487eff3341d884b00	1
	2		d9113142bae8829365c595735e1ad1f9f5e2894c	1
python	1		5cbd4a8a50a7a60183bb5e595a2805971a502959	1
	1		abda636c99b021c9e624812d3f5d41a33ee8fd5f	1
	1		db0a7f6808a434cdc368d3241902499c8be00b2e	1
	1		9c4f28a041e5bc275d5016687b11244faf366902	0

Top 10 Product Vendors of Queried Files: It displays the last analyzed products in user devices.By this feature, it allows the most checked products on the endpoint.



Top 10 Product Vendors of Queried Files

Last 30 days | Last 7 days | Last 24 hours

PRODUCT NAME	VERSION	COMPANY	AMOUNT OF QUERIES / FILES	AMOUNT OF DISTINCT ENDPOINTS
Microsoft® Windows® Operating System	10.0.10586.0	Microsoft Corporation	9	1
Unknown File Hunter	2.1.21203.140	COMODO	7	1
Firefox	4.42	Mozilla	3	1
foobar2000	1.3.16	foobar2000.org	1	1
Vbsedit	8.0.0.0	Adersoft	1	1

Malware Files Top 10 Contacted Domains/IPs:
It lists the IP where the most malware files have been analyzed.By this feature, the users can able to set

precautionary steps for the malware files on the domain.