## How to view and analyse statistics of containment

We have a brand new feature for Containment From now on, you will be able to view statistics of containment components for each process. By this way, you can analyze how containment protects you with statistics on Registry, COM, IMA etc. both in containment and real-time.

Note: This new feature under containment task is available only for Comodo client security version-10.2.0.6537 and above

To install Comodo Client Security(CCS) in endpoint, please refer this wiki topic: https://wiki.itarian.com/frontend/web/topic/how-to-install-comodo-client-security-on-windows-linux-and-mac-devices

To Update Comodo Client Security(CCS) in endpoint, please refer this wiki topic: https://wiki.comodo.com/frontend/web/topic/how-to-manually-run-updates-on-endpoints

**Step 1:** Open Comodo Client security application from the endpoint in which it is installed. Select Tasks-> Containment Task

COMODO Client - Security 10			- ×
吕 TASKS ్రస్తి SETTINGS			
COMODO Client - Security 10			- ×
🗙 HOME ငြို့ SETTINGS			
Secure   The virus signatu	re database is NOT up-t	o-date	
GENERAL TASKS FIREWALL TASKS	CONTAINMENT TASKS	ADVANCED TASKS	Q
Scan Scan your computer for virus	F		
Update           Run the updater to check for database updates.	F program and virus		

**Step 2:** Select the new feature Containment Statistics Analyser then a new window will be opened for installing the feature. In the new window click "Agree and install".

COMODO Client - Security 10 - X						
K HOME C SETTINGS						
Secure   The virus signature database is NOT u	up-to-date					
GENERAL TASKS FIREWALL TASKS CONTAINMENT TASK	ADVANCED TASKS					
Run Virtual Run applications in the container and create shortcuts for them on the desktop.	Open Shared Space           Open the storage space shared between virtual and real applications.					
Reset the Container Clean container data by erasing all its content.	Watch Activity Open COMODO KillSwitch to monitor advanced process and system activity.					
View Active Processes View the details of the processes active on this computer.	Containment Statistics Analyzer           View analysis of Containment events and protection statistics of the component.					
r⊄× SILENT MODE	?					

## COMODO Client - Security 10

Install Required Packages The feature requires installation of ac	dditional packages.				
Package Name	License Agreement	Size			
Containment Stats Analyzer		0 MB			
By pressing "Agree and Install", you agree with user license agreements for all the packages listed above.					
		AGREE AND INSTALL			

.

 $\times$ 

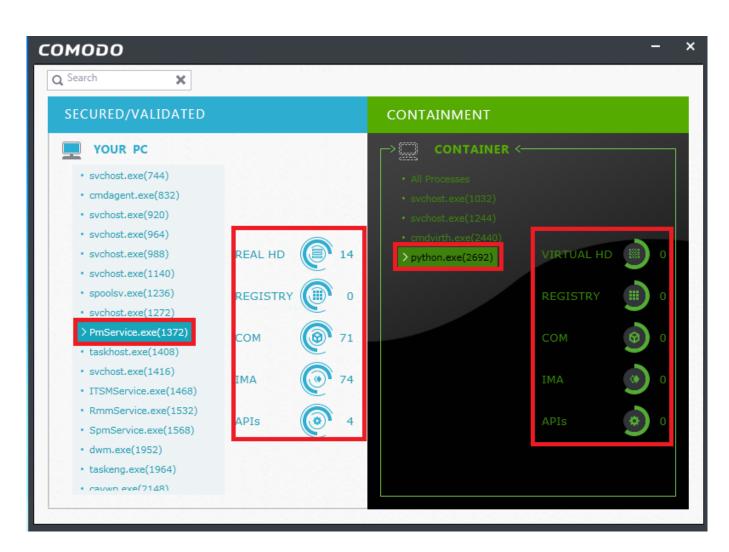
Step 3: The containment analysis windows consists of two major section Secured/validated and Containment.

			соморо	Client - Securi					-
обомс					- ×				
Search X									
SECURED/VALIDATED			CONTAINMENT			ining			
YOUR PC			_> CONTAINER ←			ENT TASKS	ADV/	INCED TASKS	
> All Processes • SandboxStat.exe(1 • smss.exe(300)			> All Processes • svchost.exe(1032) • svchost.exe(1244)			te	80	Open Shared Space Open the storage space shared between and real applications.	n virt
wininit.exe(436)     csrss.exe(448)     REC	al HD	6317 31608		VIRTUAL HD		tent.	$\bigoplus$	Watch Activity Open COMODO KillSwitch to monitor ac process and system activity.	ivano
winlogon.exe(492)     services.exe(536) COI     lsass.exe(552)     lsm.exe(560) IMA		40760 202781		СОМ	<ul><li></li><li></li><li></li><li></li><!--</td--><td>▶ n this</td><td></td><td>Containment Statistics Analyzer View analysis of Containment events and protection statistics of the component.</td><td>I</td></ul>	▶ n this		Containment Statistics Analyzer View analysis of Containment events and protection statistics of the component.	I
svchost.exe(664)     svchost.exe(744)     cmdagent.exe(832)     WmiPrvSE.exe(908)	is 🧿	329			•				
svchost.exe(920)									

i)The process statistics details can be obtained together for all processes running in the system.

СОМОДО				- ×
Q Search				
SECURED/VALIDATED		CONTAINMENT		
YOUR PC		CONTAINER <-		
> All Processes • SandboxStat.exe(1		<ul> <li>All Processes</li> <li>svchost.exe(1032)</li> </ul>		
• smss.exe(300)				
svchost.exe(328)     csrss.exe(384)     REAL HD	6353		VIRTUAL HD	
wininit.exe(436)     csrss.exe(448)     winlogon.exe(492)	31618		REGISTRY	<b>())</b> 65
services.exe(536)     Isass.exe(552)	40958		СОМ	<b>9</b> 10
Ism.exe(560)     IMA     svchost.exe(664)	210603		IMA	<b>9</b> 54
svchost.exe(744)     cmdagent.exe(832)	330		APIs	₅ ⊘
WmiPrvSE.exe(908)     svchost.exe(920)				

ii) If the statistics details are needed for any single process means it can also obtained by selecting that particular process from the list.



**Secured/validated:** This section displays the list of executables which are considered as trusted process/executables. These executables have full access permission to get executed in the PC. The statistics available for this section are:

Real HD: Total memory space occupied by the process in the physical hard disk is shown.

Registry: Total number of modification made in the registry by the process are shown.

COM: Shows total number of services accessed which are provided by other processes.

IMA: Number of the directly accessed process are shown.

APIs: Number of sensitive Application programming interfaces(APIs) accessed by the process is shown.

**Containment:** This section displays the list of executables and process which are allowed to run in the separate virtual space (i.e.) container. These executables have limited access permission for execution The statistics available for this section are:

Virtual HD: Total memory space occupied by the process in the shared space or virtual provided for containment

**Registry:** Total number of modification made in the registry by the contained process is shown **COM:** Shows total number of services accessed which are provided by other processes

IMA: Number of the directly accessed process are shown.

**APIs:** Number of sensitive Application programming interfaces(APIs) accessed by the contained process are shown