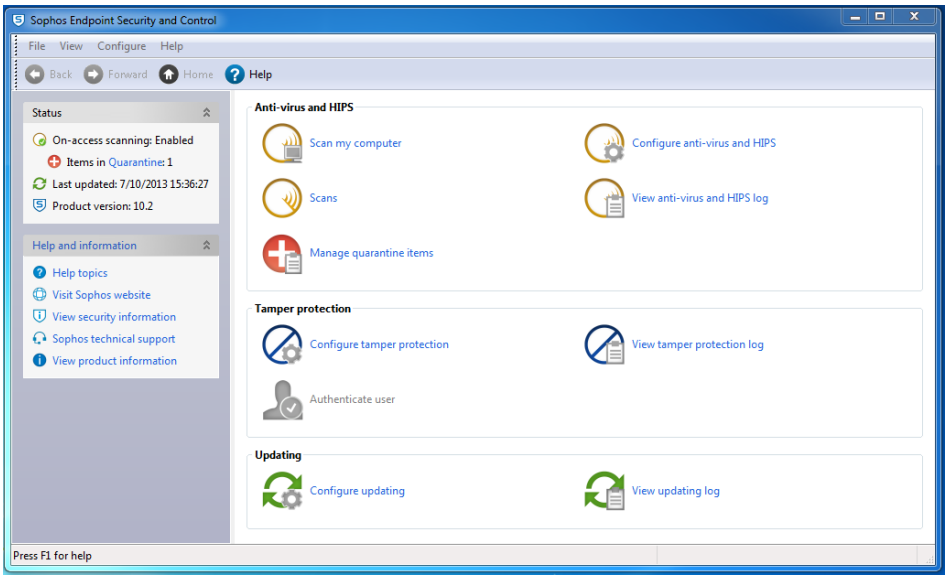
Sophos Endpoint Antivirus with Windows Firewall (Updated and Default Settings)
Malware Security

User Interface:



System Memory:

- **5 Running Process**
- **189 Megabytes of ram**
- **Little slow on the system**

Image Name	User Name	CPU	Memory (...	Description
svchost.exe	LOCAL ...	00	620 K	Host Process for Windows Services
svchost.exe	LOCAL ...	00	3,152 K	Host Process for Windows Services
taskhost.exe	Malwar...	00	2,308 K	Host Process for Windows Tasks
UI0Detect.exe	SYSTEM	00	1,932 K	Interactive services detection
lsass.exe	SYSTEM	00	2,488 K	Local Security Authority Process
lsm.exe	SYSTEM	02	1,228 K	Local Session Manager Service
msdtc.exe	NETWO...	00	2,960 K	Microsoft Distributed Transaction Coordinator Service
sppsvc.exe	NETWO...	00	1,096 K	Microsoft Software Protection Platform Service
SearchIndexe...	SYSTEM	00	6,920 K	Microsoft Windows Search Indexer
System	SYSTEM	00	60 K	NT Kernel & System
System Idle P...	SYSTEM	76	24 K	Percentage of time the processor is idle
SavService.e...	LOCAL ...	00	178,428 K	Performs virus scanning and disinfection functions
services.exe	SYSTEM	00	4,224 K	Services and Controller app
SAVAdminSer...	SYSTEM	00	1,148 K	Sophos Administrator Service
ALsvc.exe *32	SYSTEM	00	1,356 K	Sophos AutoUpdate Service.
ALMon.exe *32	Malwar...	00	1,000 K	Sophos Endpoint Security and Control
swi_service.e...	SYSTEM	00	4,012 K	Sophos Web Intelligence
spoolsv.exe	SYSTEM	00	5,936 K	Spooler SubSystem App
taskeng.exe	Malwar...	00	1,408 K	Task Scheduler Engine
TPAutoConne...	Malwar...	00	2,112 K	ThinPrint AutoConnect component
TPAutoConnS...	SYSTEM	00	2,056 K	ThinPrint AutoConnect printer creation service
vmtoolsd.exe	SYSTEM	00	4,840 K	VMware Tools Core Service
vmtoolsd.exe	Malwar...	00	7,284 K	VMware Tools Core Service
audiodg.exe	LOCAL ...	00	9,860 K	Windows Audio Device Graph Isolation
explorer.exe	Malwar...	02	18,520 K	Windows Explorer
winlogon.exe	SYSTEM	00	1,836 K	Windows Logon Application
smss.exe	SYSTEM	00	292 K	Windows Session Manager
wininit.exe	SYSTEM	00	1,112 K	Windows Start-Up Application
taskmgr.exe	Malwar...	03	2,952 K	Windows Task Manager
msiexec.exe	SYSTEM	00	4,072 K	Windows® installer
WmiPrvSE.exe	SYSTEM	00	1,712 K	WMI Provider Host

30 Web Links (Zero to 1 Day Old Links):

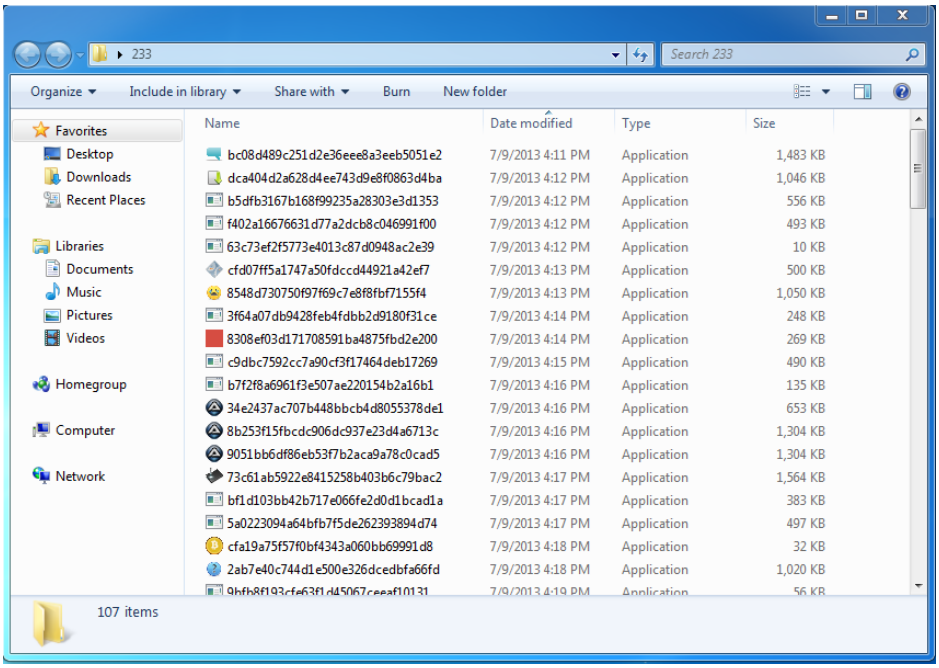
- **22/30 Links Blocked**

Missed Links:

```
1.  picasa.com.tuson.ca/bot.txt???-----------------------3/32 Virus Total Blocked
2.  notjustbooks.co.za/ZQb.exe---------------------------3/33 Virus Total Blocked
3.  noshua.it/-------------------------------------------5/39 Virus Total  Missed
4.  moalemha.ibsblog.ir/post/2---------------------------6/39 Virus Total Blocked
5.  mediaseb.pl/-----------------------------------------7/38 Virus Total Blocked
6.  jxnews.com.cn/att/0/11/69/52/11695275_
    465535.xls?COLLCC=142388094&COLLCC=4162456675--------4/34 Virus Total Blocked
7.  hoststar.co.in/g86r.exe------------------------------3/33 Virus Total Blocked
8.  homegame.org/news/gateway/---------------------------4/33 Virus Total Blocked
9.  hiprop.de--------------------------------------------5/33 Virus Total Blocked
10. helpmaster.nl/wp-content/h/n3mtc>/;??n%5Ens----------3/33 Virus Total Blocked
11. greatlakesinitiative.org/.file/win.txt??-------------6/37 Virus Total Blocked
12. fisioterapiacarioni.it/------------------------------3/33 Virus Total  Missed
13. enecasemehr.ibsblog.ir/post/7/-----------------------5/38 Virus Total Blocked
14. empowervrouwen.nl/-----------------------------------7/36 Virus Total  Missed
15. eco-build.gr/iqbze.exe-------------------------------3/34 Virus Total Blocked
16. daciaklub.pl/user/zlot1/index_16.htm-----------------4/39 Virus Total  Missed
17. corpomusicalegermagnano.it/--------------------------7/33 Virus Total  Missed
18. coniv.it/--------------------------------------------6/36 Virus Total  Missed
19. bossche.be-------------------------------------------3/33 Virus Total Blocked
20. baza.gazetaautorow.pl/tempamb.exe--------------------6/38 Virus Total Blocked
21. aslanisejahrood.ibsblog.ir/post/35/------------------5/39 Virus Total  Missed
22. anamnesis.info/ie-index.htm--------------------------5/34 Virus Total  Missed
23. 218.4.59.194/uploadfiles/2013-1/182141157235.zip----3/33 Virus Total Blocked
24. 198.23.161.189/
    SERNAC/DOCUMENTOS/Informe-17-02-2013.exe-------------6/35 Virus Total Blocked
25. blogger.com.abhisolution.in/force2.php---------------5/38 Virus Total Blocked
26. up.brydah.org/do.php?downex=26684--------------------8/39 Virus Total Blocked
27. sofontes.com.br/down/E/EnglischeSchJoiTDemBol.zip---4/39 Virus Total Blocked
28. raomai.vn/caidat.rar---------------------------------8/39 Virus Total Blocked
29. mfox4.altervista.org/lg.txt--------------------------4/39 Virus Total Blocked
30. lordskitchen.org/Formulario.exe----------------------9/39 Virus Total Blocked
```

Malware Pack Containing 233 Files (1 Day Old Files):

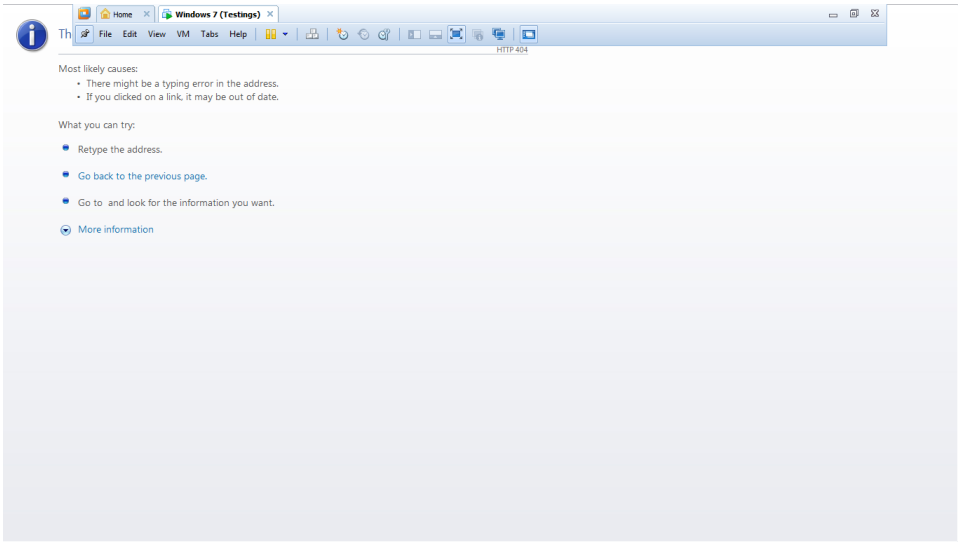
126/233 Files detected = 54.07%



Caught Later By Behavioral Blocking, Firewall, Etc.:

- **I only ran the first file and it locked my vmware with ransomware, I don't know why it's not an FBI ransomware telling me to pay in order to unlock!**

- **This is the file g-data caught and quarantined it before it locked my vmware**



Hitmanpro and Malwarebytes results after behavioral blocking test:

- **Couldn't scan because of ransomware locking my vmware!**

5 Star Rating:

- **1 Star: User-friendly: 1/1 Star**
- **1 Star: Low Ram Usage, 60mb or less: 0/1 Star**
- **1 Star: 24/30 Web Links, 80%: 0/1 Star**
- **1 Star: Detection 85%+: 0/1 Star**
- **1 Star: Behavioral Blocking, 50%+: 0/1 Star**

1/5 Stars

Summary:

Advantages:

- **Easy looking user interface, but looks old fashion!**

Disadvantages:

- Heavy on ram
- Not good detection rate!
- Slow custom scan and removal
- Not so good on web blocking
- Behavioral blocking didn’t save me from ransomware, I took the star away because it’s a big issue for people who do not know what to do!

According to my testing’s, Sophos did not pass all the test, especially from a major ransomware. I would not recommend this antivirus to users!