

# Executive Summary On Avast Free Antivirus



**CYBER SECURITY &  
PRIVACY FOUNDATION**

---

**Software:** Avast Free Antivirus for Windows.

**Lab Setup:**

Oracle Virtualbox v4.3.6 r91406

**Operating System:**

Machine 1: Windows 7 32-Bit.

**Processor:**

Intel(R) Core(TM)i5-4200U CPU @1.60GHz 2.30GHz

**RAM:**

512MB

**Test Criteria:**

We have set up the test in four levels.

**Known Malware-** Malware that is widely spread and is detect by a majority of antiviruses.

**Known Malware (Variant)** - Malware that is widely spread but has been crypted using a custom crypter (tried to make undetectable)

**Unknown Malware-** Malware samples that were developed exclusively for this test hence unknown to any antivirus vendor. The antivirus will only be able to stop such attacks using heuristics.

**Pre Infected Machines-**In this test the computers were infected with known malware before the anti-virus is installed. The reason for this test is that most of Indian computers are already infect with some sort of malware before an antivirus is installed and the this test hopes to test if the antivirus is able to remove all previous infections after it is installed.

### Installation:

General Installation with all the Terms and Agreement to be agreed.

### Configuration:

General pre-built Configuration that comes by default in Avast.

### Test Results (Known Malware):

Detected the Known Malware sample as malicious and removed it successfully.

- Real-time
- Offline

### Test 1: Detection of Known Virus

Successfully detected the Virus Sample and successfully removed it.

- Real-time
- Offline

### Test 2: Detection of Known Keylogger

Successfully detected the Keylogger and was able to remove it.

- Real-time
- Offline

### Test 3: Detection of Known RAT (Remote Administration Tool)

Did not detect the RAT and the RAT was able to run successfully and added itself to startup processes.

- Real-time
- Offline

### Test Results (Known Malware -Variants):

Did not detect the malware sample.

- Real-time
- Offline

### Test 1: Detection of Known Virus-Variant

Did not detect the virus sample.

- Real-time
- Offline

### Test 2: Detection of Known Keylogger-Variant

Did not detect the Keylogger.

- Real-time
- Offline

### Test 3: Detection of Known RAT (Remote Administration Tool) –Variant

Did not detect the RAT Tool.

- Real-time
- Offline

### Test Results (Unknown Malware-New Samples)

Did not detect the malware sample.

- Real-time
- Offline

### Test 1: Detection of Unknown Keylogger

Did not detect the malware sample.

- Real-time
- Offline

### Test 2: Detection of Unknown Downloader

Did not detect the malware sample.

- Real-time
- Offline

### Pre-Infected Machines:

The presence of malware in the computer prevented Avast from Installing.  
Out of 10, 6 got into the startup and all 6 were removed.

### Conclusion:

From the Testing that we were able to perform on the Avast, it was found that Avast Free Antivirus was able to detect all the known malware and virus samples, but when it came to the part of variants of the known malware and viruses, it was not able to detect the samples. It was also found that Avast was not able to detect one of the widely used RAT and its variant. It was not able to detect any of the unknown malware samples, and was able to successfully clean the pre infected system of known malwares.

During the testing it was also found that the Boot Time Scan was really good.

The overall rating that we give Avast Free Antivirus is

**“7/10”**