



Ten reasons for TECHNICIANS ...

... why you should consider the Avira AntiVir Engine for your solution.

Ten reasons for TECHNICIANS ...



Unfortunately for us, every marketing department praises its products using superlatives and it is not always easy to make a decision for a non-technician. On the other hand, Avira uses many technologies we do not want to show the world in detail in order to maintain our competitive edge. Below you will find technical details that may give a more technical understanding of how Avira is able to reach the top position compared to the giants.



1. Superior detection rates

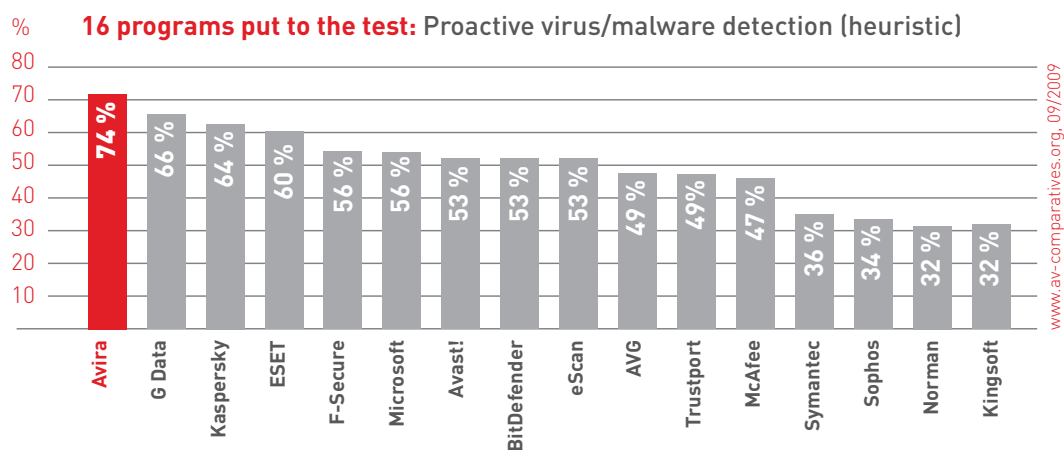
One reason for the high detection rates achieved by Avira is how we handle polymorphic and metamorphic malware. Polymorphic viruses constantly change their “face” to be undetectable by classic signature based methods.

Avira has built a very special virtualization module together with a generic decryption engine for these kind of threats, it allows us to emulate the malware by faking the processor instructions and OS behavior without being detected as an emulator. As soon as the code is decrypted in memory we can detect every single variant of the polymorphic malware without having to add a new signature for it.

Metamorphic viruses are even harder to detect because they change the “face” even in the emulator. To detect metamorphic viruses we use a combination of several technologies like static analyse, partly emulation, AHeAD heuristic and X-Raying to ensure 100% detection without having to adjust the virus signatures. The benefit of this is that we can focus more on other new malware that might not be as wide spread.

2. *Advanced Heuristic Analysis and Detection (AHeAD)*

The great detection rates are supplemented by unique heuristics. While almost every vendor today offers an integrated heuristic solution the difference is in the technical implementation. Without going into details we can say, that the combination of the factors on which the detection is based and the logic used to compute these factors allows us to rebuild a humans decision which is behind the secrets of the success of AHeAD.

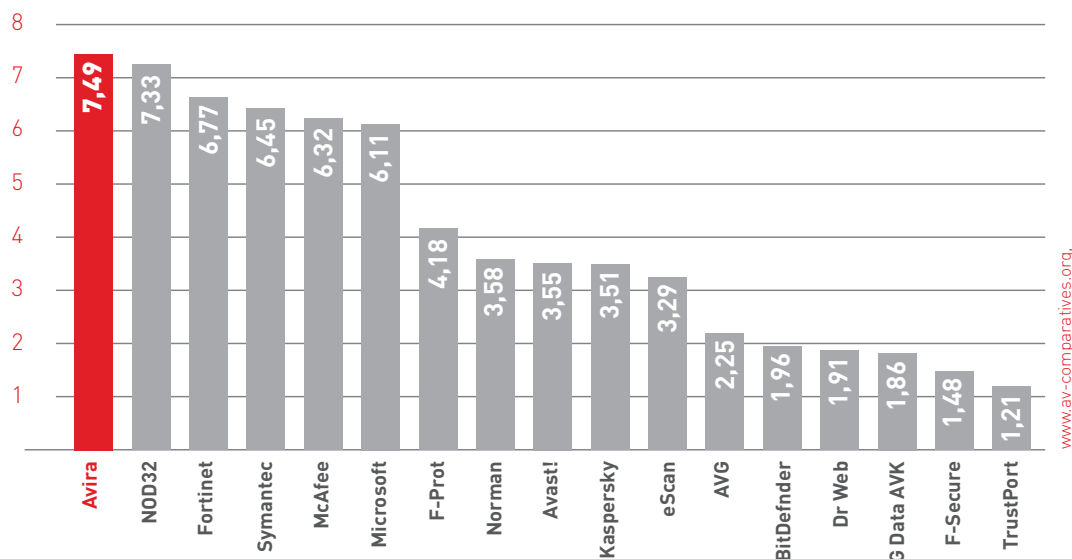


3. Very low system impact

Typically there is a contradiction in having the biggest number of virus signatures versus achieving the best performance and consuming the lowest memory resources. While one way is to trust compiler optimizations only Avira uses the development principal “fast by design” and invests a lot of low level know-how in this field.

The compiler optimizations bring the last pinch of speed after the development. The other critical component of system impact, the memory usage is addressed very seriously. By using a lot of generic detections and signatures that are less than half in size of most competing products the memory consumption is amazingly low compared to the number of detected malware files.

MB/sec **17 programs put to the test: Scanning Speed**



www.av-comparatives.org

4. Ease of use and implementation

The Avira Engine and the OEM Integration SDK “SAVAPI” have been developed with partners in mind from the very beginning. Today we offer partners a reliable and easy to implement solution, that saves development time.

5. Cross platform concept

Using a single source engine for all platforms helps us to focus more on reliability and speed than on platform support. Combined with the Cross- Platform-SAVAPI, our SDK for OEMs, a partner can integrate our technology into different platforms whether they are 32 bit or 64 bit, little or big endian, INTEL, AMD, SPARC or ARM using the same interface and providing the same functionality.

6. Stability and robustness

The Avira AntiVir Engine is known not only to be one of the smallest and fastest of its kind but also one of the most reliable and stable. Several additional features like the Program Integrity Check help to prevent malware from manipulating the behavior of the AV Engine. The integrity check is a transparent way of ensuring the anti-virus system is functioning correctly at all times.

7. Strong content and archive handling

The Avira Engine is capable of detecting malware even if it has been packed multiple times using a broad range of runtime packers as well as different archive-, office-, email program- and other formats. Support is provided e.g. for ZIP, ARJ, RAR, LZH/LHA, CAB, Unix Mbox, Netscape/Thunderbird Mbox, Eudora, PST, Binhex, UUE/XXE, MIME and several other formats, almost 90% of the used runtime packer like UPX, ASPACK, FSG, MEW, UPACK, PECompact, Petite and many others as well as the most frequently used formats from office applications like DOC, XLS and PPT and HTML and other browser oriented files.

8. Multithreaded design

Solutions that need to scale into larger environments like central mailbox and web-content-scanning can make usage of the extremely high scalability of the Avira Engine when implemented through the SAVAPI SDK. Combined with the high overall speed the advantage on multiple core systems is extremely impressive.

9. Coverage of all major threats

The Avira Engine doesn't just cover classical viruses, but also Trojans, backdoors, ad- and spyware, phishing, worms, keyloggers, dialers, droppers, downloaders and applications that can be classified as a security or privacy risk in certain environments. This reduces the need for additional security tools to be installed.

10. Detectable objects

As well as the standard checking of file based objects, the Avira solution can scan and repair virtual files, perform an “in-memory” scan and can provide the file inside a stream.



Avira GmbH
Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0

www.avira.com