Avira

Avira Protection Cloud

White Paper

Contents:

1.0 Introduction

Many users are already familiar with the concept of cloud computing, which is why the Avira Protection Cloud builds on this to offer you a new level of Internet security. Read on to learn all about the next generation in Internet security – the Avira Protection Cloud.
We start with a brief introduction to the Avira Protection Cloud before going on to consider the fundamental elements. Following that, you will find a description of all the benefits this new technology offers you, as well as answers to frequently asked questions.

1.1 Why do I need the Protection Cloud?

The development of the Avira Protection Cloud began with a question: How can users protect themselves from malware when hackers and malware authors are producing new threats at an alarming pace?
Thousands upon thousands of new malware threats are developed every day and then unleashed: Trojans lurk in hiding within email attachments; rootkits sabotage programs which are actually there to remove rootkits; adware displays annoying and potentially unsafe pop-ups; and keyloggers spy on users' passwords.
In the past, PC security was still relatively straightforward: Developers of virus protection software programmed countermeasures and had sufficient time to react to new viruses. However, hackers and malware authors worked constantly on getting ever better – resulting in a sort of competition between the hackers and the virus protection programs. Just like the arms race, this resulted in a vicious circle where each side tried to outdo the other.
Hackers initiated virus attacks and security experts designed massive virtual protective walls to counter the attacks. The hackers then attacked the programs until they found a way through the wall. The security experts responded by expanding and reinforcing the virtual walls. However, the malware authors refused to admit defeat and attacked the new virus protection measures repeatedly until they discovered further vulnerabilities. The security experts were then forced to design new protective walls, which were ultimately overcome again by the hackers. Both sides were trapped in a never-ending battle to stay one step ahead of the other.
This model of reactive defense was the foundation of successful Internet security for many years. However, this approach wasn't really sustainable. Continuously strengthening security measures slowed PC performance and consumed valuable resources required for performing actual work on the computer. Calls for more intelligent protection for users grew ever louder.
On top of this, this cyber battle entered a new phase: The actors were now experienced pros. Hacking is no longer the work of lone individuals who design malware for their own dubious entertainment – it's now done by organizations who specialize in spying on personal information. Data theft, identity theft, money laundering, and many other areas of Internet fraud and extortion are part of their profession, and they are skilled in their trade.
The new hacker generation has an immense advantage: It has access to the same virus protection programs as users. It's now easier to write malicious code if the hacker has the same virus protection program. The whole process by which hackers test their code is automated, allowing the discovery of vulnerabilities with just one really specific change to the code.
This is why higher and thicker walls no longer offer adequate protection. Gigantic firewalls which use cutting-edge malware-detection algorithms only protect users from known threats. As a result, a completely new approach to virus protection needed to be taken. The Avira Protection Cloud was developed precisely because of these factors.

1.2 About the Avira Protection Cloud

The Avira Protection Cloud is a global, cloud-based online system that classifies files in real time in a way that is truly innovative and resource-friendly. This intelligent Internet security system is active around the clock and distributed over several sites.
Or to put it another way: It is a worldwide PC network with a collective online database for file definition. These files are classified using innovative algorithms and systems, and then provided to users in real time. The result: Reliable virus protection with an extremely short response time, in combination with a fast, ultra-light platform.

1.3 How does the Avira Protection Cloud work?

The Avira Protection Cloud process is activated when an individual PC, protected by the cloud and located anywhere in the world, calls up an unknown file. The user is notified and the Avira Protection Cloud process is launched automatically.
A "fingerprint" of this file is immediately uploaded to the Avira Protection Cloud as soon as the unknown (not suspicious, but not yet classified) file is called up. Following the upload, the fingerprint is compared with millions of definitions of safe and unsafe files already stored in the Avira Protection Cloud. If the file matches one that is already known to be safe, the call is approved and the user is granted access – the process then continues as normal.
However, if the file cannot be identified, the Avira Protection Cloud prompts the user to upload the complete file for a comprehensive analysis. Once it has been scanned, if any malware is detected the Protection Cloud will immediately quarantine it and classify the file as "malicious" – a process which only takes a few seconds (if an infected file is found, the user will of course be alerted).
On the other hand, the Avira Protection Cloud will flag a new file – which is classified as being free from malware – as "safe". This information is made available to all other Protection Cloud users, saving them from having to go through the same process.

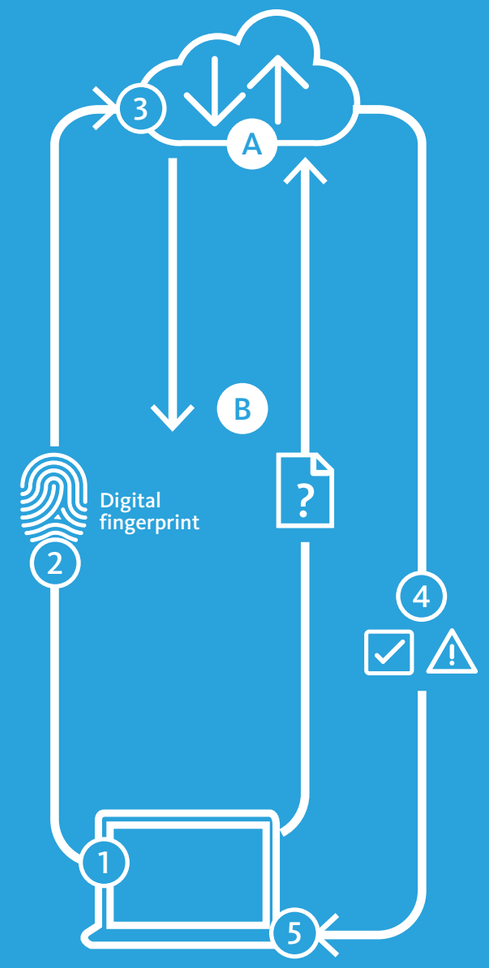
Avira Protection Cloud

1. Avira Antivirus finds a suspicious file on the PC.
2. The file's digital fingerprint is determined and sent to the Avira Protection Cloud for analysis.
3. This fingerprint is compared with files which were checked previously by the Avira Protection Cloud. This can lead to two outcomes:

A. The fingerprint belongs to a file already scanned by the Protection Cloud and is immediately classified as either "safe" or "malware".

B. The fingerprint is new to the Avira Protection Cloud, so the Protection Cloud uploads the file, analyzes it, and classifies it either as "safe" or "malware".

4. The Protection Cloud reports the status (safe or malware) of the fingerprint to Avira Antivirus on the PC.
5. If the file is classified as malware, Avira Antivirus removes the threat.



2.0 Better protected with the Avira Protection Cloud

2.1 Swarm intelligence

The first, and one of the key benefits of the Avira Protection Cloud platform is its access to the worldwide Avira network of more than 100 million users for detecting new viruses. Users call up countless files each and every day when surfing, scanning, shopping, browsing, streaming, downloading, and chatting. This results in an enormous number of files that all need to be scanned. This is also an ideal opportunity to significantly enhance Avira's malware detection capabilities.

The Avira Protection Cloud makes use of this opportunity by combining the scanning potential of millions of independent computers on a single, central platform for malware classification. In this respect, it functions as a distribution node and provides Protection Cloud users around the world with new virus detection patterns in real time.

In other words: One computer alone doesn't have to do the job of detecting and identifying malware. The Avira Protection Cloud enables any connected PC anywhere in the world to increase global Internet security by transmitting unknown files for analysis.

2.2 Real-time detection

The second benefit of the Avira Protection Cloud is that, compared to virus protection systems which are updated on a scheduled basis, it has a real-time update system.

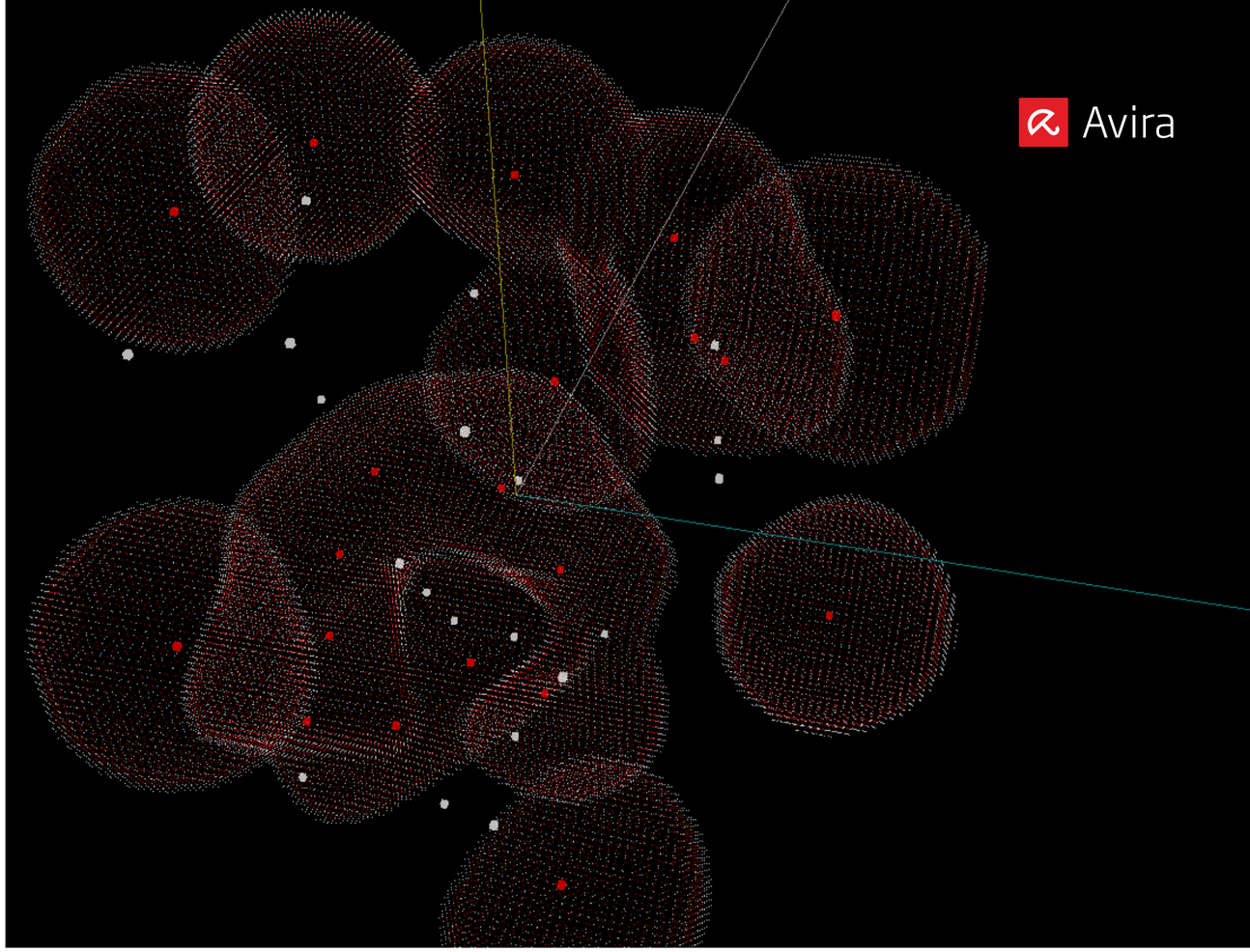
With a traditional antivirus system, the PC user always needs to run a manual virus update to be protected against new threats. Between these updates, the virus definition on the PC is not 100% up to date, meaning that the PC is vulnerable until the next update.

By contrast, the Avira Protection Cloud keeps detailed information on many millions of files constantly updated and readily accessible every second of the day 24x7. This gives every user immediate on-demand access to the latest virus definitions even when the definition was only discovered a few seconds ago.

2.3 Detection protection

As mentioned, malware authors do not simply use conventional PCs. They are clever enough to hack directly into a local antivirus program and analyze the detection processes. The hackers then use the antivirus program as a kind of laboratory, where they can develop new viruses or adapt their malware so that it remains undetected.

But as Avira performs these processes in the cloud, they remain invisible to hackers and they can't access them. This key benefit is what Avira calls "detection protection". Since the Avira Protection Cloud is not a local program, hackers can't analyze the entire antivirus platform. In addition, hackers can't analyze the various modules and algorithms, with which the detection tasks are performed, either. Software that you cannot actually see is also much more difficult to breach. A hacker who has developed a virus needs to test the code. To do this, the hacker needs to upload countless variants. But without a local product to use as a test platform, hackers can't execute this critical step.



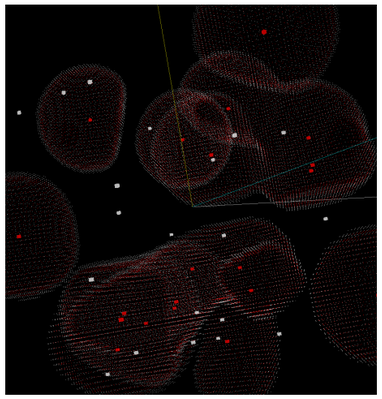
2.4 Low resource consumption

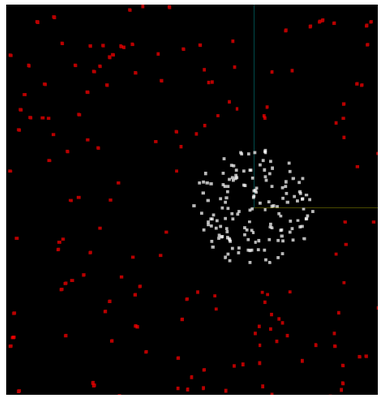
The fourth benefit of the Avira Protection Cloud is its extremely low resource consumption. The fact that Avira's award-winning detection technology runs in the cloud gives users the benefit of a product that consumes considerably fewer local resources. Furthermore, cloud-based scanning generates far less network traffic, as just a small digital fingerprint is uploaded in the first step. The Avira Protection Cloud can thus run more than 1,000 virus scan queries with just 12 kilobytes of traffic.

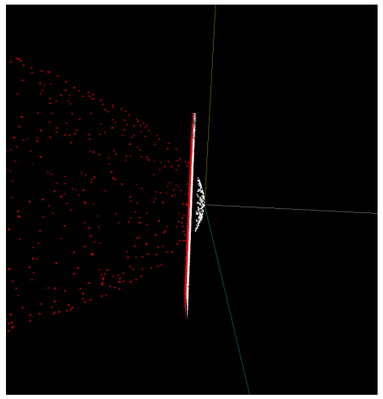
Thanks to the high-performance caches, Avira Protection Cloud achieves a much lower latency. These caches are expanded as the number of queries rises, resulting in a more streamlined virus protection technology that consumes considerably fewer PC and network resources compared to traditional local platforms. This is especially important, as no home-user PC has enough resources to run the advanced, generic detection procedures of the Avira Protection Cloud. The platform uses artificial intelligence and offers some of the world's most innovative file analysis modules.

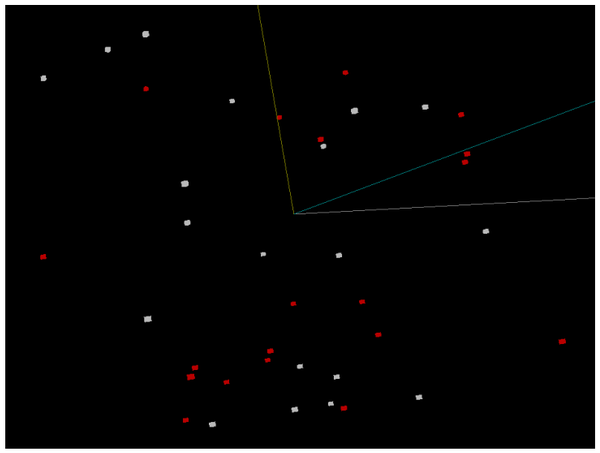
Among them, Avira employs automated malware-detection processes which use innovative algorithms. This allows newly discovered files to be interpreted and classified without the need for explicit action to be taken. Artificial intelligence is based on convex optimization which minimizes convex functions and quantities. General properties of unknown file types are classified based on certain features. These properties are then used to classify the files as "good" or "bad" – a decision which is based on thousands of input features.

To put it another way: The Avira Protection Cloud's tried and tested scanning processes are so comprehensive that they are much too sophisticated and complex to be run on a conventional PC.









The Avira Protection Cloud has a self-learning system that always incorporates the latest machine-learning findings. Optimized mathematical models are employed to detect malware. Within just a few minutes, the self-learning platform can execute tasks that would take scientists many years to perform.

3.0 Benefits of the Avira Protection Cloud

- Swarm intelligence significantly expands detection possibilities.
- The cloud memory allows users to use the Avira scan engine. This is regularly awarded first place by AV-Test in proactive and reactive tests.
- Avira's self-learning technology classifies files without the need for human intervention.
- Incredibly low resource consumption for local computers.
- The Avira Protection Cloud database contains several hundred terabytes of uploaded files. This means that these files do not need to be saved locally.
- The automated database requires no prior knowledge of any kind and is very user-friendly.
- The Avira Protection Cloud is continuously expanded and developed through users' everyday activities on their PCs.
- Dynamic file classification provides protection from particularly malicious threats.
- Advanced protection blocks fast-developing malware families.
- Seamless integration of existing Avira product lines and cross-platform support with no adverse effect on service quality.
- The Avira Protection Cloud is a closed control system, meaning no personal information is stored.

4.0 Frequently Asked Questions (FAQs)

What data do PCs and the Avira Protection Cloud exchange?
Only a small identification area of the file is initially uploaded: The "fingerprint". If this fingerprint is unknown, the Avira Protection Cloud prompts the user to upload the entire file for a comprehensive analysis. Only information about executable files is uploaded to the cloud (files with .exe or .dll extensions) – not file formats like PDF, text (.txt. and .rtf), image (.jpeg, etc.), Word and other private files.

Will third-parties be able to access the data I upload?
No. The data that is uploaded is only used for malware analysis and is not stored in our cloud data center. It is not possible to forward this data to third parties. As this process is fully automated, individual files are analyzed without any human interaction.
In addition, to guarantee complete anonymity the user's identity is automatically removed when fingerprints or files are uploaded.

Is the uploaded data encrypted?
Yes. End-to-end TLS (Transport Layer Security) cryptographic protocols are used to encrypt communication between the user's system and the Avira Protection Cloud.

For which file types are fingerprints created? Is it "only" done for .EXE and .DLL files or for other types such as .OCX and .JS too?
Fingerprints are created for all Portable Executables (PE files). PE file extensions include: .exe, .dll, .sys, .drv, .scr, .cpl, .ocx, .ax, and .efi.

When connected using the SDK, how does the engine decide when to use cloud components for the analysis?
In general, the above-mentioned PE files are used. The Local Decider determines whether a hash analysis or even an upload is required.
This involves an internal analysis of many factors including the file size, header information as well as other meta information, and the creation of a risk rating.

How does the Local Decider make its decision?
The sensitivity dictates whether a file hash needs to be created and analyzed.
This sensitivity can be configured between 0 (virtually all PE files) to 7 (only those with a high risk rating) in the SAVAPI configuration using the parameter APCCheckRiskRatingLevel (for the hash analysis) or APCUploadRiskRatingLevel (for the upload, if required).

What happens if a Word document contains an EXE file?
The EXE file is extracted and analyzed by the Avira Protection Cloud. The Word document itself is not uploaded and thus is not analyzed by the Avira Protection Cloud.

5.0 About Avira

Avira, a family-owned company which enjoys above-average growth, was founded in 1986 by the IT security pioneer Tjark Auerbach in Tettnang. It is one of the most important regional employers in the Lake Constance area.
For three decades, Avira has provided its customers with security solutions, developed by Avira itself, for protection against Internet threats, malware attacks, harmful programs, and data theft. More than 100 million users, particularly micro and small businesses as well as home users, rely on Avira's software and value its reliability, performance, and usability.

Avira ranks second among the world's leading antivirus software manufacturers. The company, headed by Travis Witteveen, operates its own virus laboratories and continuously demonstrates its enthusiasm for innovation and its capabilities by developing next-generation security technologies. These include real-time protection through cloud-based malware detection and the "Online Essentials" Web Console.
Avira works closely with the Federal Office for Information Security (BSI) and is a founding member of the "IT-Security made in Germany" initiative.
Avira's experience and top-rated products and services help people move freely and safely in our digital world.
Security in the real world is another important concern for Avira. Established by the company's founder, the Auerbach Foundation supports charitable and social projects, and has already sponsored more than 300 projects in the areas of education and schooling, children, youth and family, assistance for senior citizens and people with disabilities, as well as arts and culture.

Avira

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany
Phone: +49 (0) 7542-500 0

Errors excepted. Subject to technical changes. Issued: October 2016

PROTECTING PEOPLE
IN THE CONNECTED WORLD

www.avira.com