AVIRA

Whitepaper
Avira Protection Cloud (APC)

1. Introduction

While the concept of cloud computing is familiar to many, the Avira Protection Cloud represents a different approach to internet security. Therefore, Avira has developed this document to help familiarize you with the next generation of internet security – the Avira Protection Cloud (APC).

We will start with a brief introduction of the Avira Protection Cloud and then move on to its fundamental segments. Afterwards, we will highlight the advantages of this new platform and finally we will end by answering some frequently asked questions.

1.1 Why the Avira Protection Cloud?

The Avira Protection Cloud began with a question; how can users protect themselves from malware when hackers and malware authors are evolving at a frightening rate?

Each day, hundreds of thousands of new bits of malware are developed and released into the wild. Trojans lay waiting in email attachments. Rootkits sabotage the tools designed to defeat them. Adware leads to annoying and potentially unsafe popups and keyloggers record passwords.

In the past, PC security was a straightforward affair. Antivirus software developed reactive measures that provided enough time to react to new viruses. However, hackers and malware authors improved their skills as well, and soon a competition between hackers and antivirus programs emerged. Like an arms race, it was a vicious cycle, each side trying to outperform the other.

Hackers attacked with viruses and security experts built massive virtual walls to keep them out. In response, hackers simply kept attacking the program until they found a way through the wall. When they did, security experts responded by making the virtual wall thicker and taller. In response, malware authors simply probed these new antivirus defenses again until they found another weak spot. Then security experts were forced to build yet another wall, which of course the hackers would eventually defeat. Day in and day out, hackers and security experts were locked in a struggle to stay one step ahead of each other.

For many years, this model of reactive defense was the cornerstone of successful internet security. However, this approach was not sustainable. Ever-increasing security measures simply weighed a PC down, consuming valuable resources that were better spent on computing

tasks. Users needed smarter protection.

More recently, a new challenge has emerged-outright cyber warfare waged by experienced professionals. Today, hacking is no longer the work of lone individuals writing malware for their own mischievous entertainment. There are organizations that specialize in consumer and private espionage, data theft, identity theft, money laundering and all manners of internet fraud and blackmail-and they are good at what they do.

The major difference is that this new generation of hackers now has access to the same antivirus programs as the users. Once they posses the actual antivirus product for themselves, writing a new malicious code becomes easier. They simply use an automated process to test their codes until they find a particular permutation that gets through the wall.

Therefore, thicker walls are no longer the answer. Simply placing PCs behind massive Firewalls and filling them full of cutting-edge malware detection only defends users against known threats. A new way of thinking about antivirus was needed and it is precisely in this environment that the Avira Protection Cloud was born.

1.2 What is the Avira Protection Cloud?

The Avira Protection Cloud is a global, online cloud-based system that provides lightweight and state of the art file-classification in real-time. It is a round-the-clock, intelligent internet security system distributed across multiple data centers.

In more simple terms, the APC is a global network of PCs all feeding into an online file definition database. These files are classified using state of the art algorithms and systems and then made available to users in real time. The result is a fast, lightweight, highly responsive and very reliable antivirus platform.

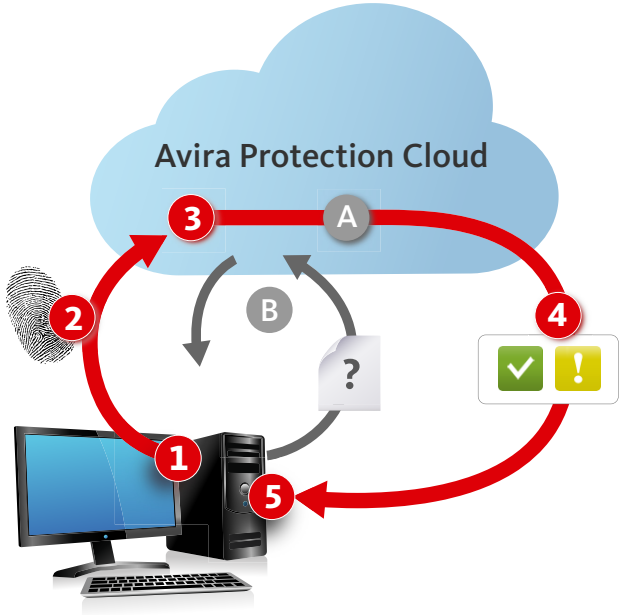
1.3 How Does the Avira Protection Cloud Work?

The Avira Protection Cloud process begins when a single APC-protected PC, located anywhere in the world, accesses an unrecognized file. When this occurs, the user receives an alert and the Avira Protection Cloud process automatically swings into action.

In mere split seconds after the unknown (not suspicious, simply unrecognized) file is accessed, a “fingerprint” of this unidentified file is instantly uploaded to the Avira Protection Cloud. Once received, the file’s fingerprint is compared to the millions and millions of safe and unsafe file definitions already stored in the Avira Protection Cloud. If the file corresponds to a previously recognized file that is known to be safe, the process is approved, the user accesses the file and life goes on as normal.

However, if the file cannot be identified, the APC will request the user to upload the complete file for a full analysis. After scanning, if this full file is found to include malware, the APC will instantly quarantine it and define it as “malicious”. The APC completes this process in a matter of seconds (of course, if the file is infected, the user will also receive an alert).

On the other hand, if the new file is determined to be malware free, the APC will label this file as “safe” and make that information available to all requesting APC users- preventing them from having to complete the same process.



How it works

1. The Avira application discovers a suspicious file on a PC.
2. The file's digital fingerprint is extracted and sent to the Avira Protection Cloud for review.
3. The fingerprint is compared with those of files that have previously been analyzed by the Protection Cloud. This process can have two outcomes:

   A. The fingerprint belongs to a file that has previously been analyzed in the Protection Cloud. It's immediately labeled as clean or malware.

   B. The fingerprint is new to the Protection Cloud. The complete file is uploaded to the Protection Cloud, thoroughly examined and judged as clean or malware.

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

For a full description of the Avira Protection Cloud, please visit the Avira website (http://www.avira.com/en/avira-protection-cloud)

2. Key Advantages of the APC

2.1 Community Intelligence

A main advantage of the APC platform is that it leverages Avira's global network of over 100,000,000 users towards detecting new viruses. Each day, untold numbers of files are accessed as users surf, scan, shop, browse, stream, download and chat. This represents an astounding number of files to examine, but at the same time, it represents a golden opportunity to greatly expand Avira's malware detection footprint.

To capitalize on this, the APC connects the scanning potential of millions of independent machines into a single, central malware definition platform. The APC then acts as a distribution hub, dispersing new virus definitions to APC users across the globe in real-time.

To put it plainly, instead of one computer working independently to locate and identify new malware, the APC empowers every APC-equipped PC across the globe with the ability to contribute to global internet security by submitting unrecognized files for analysis.

2.2 Real-Time Updates

The second advantage of the APC is that, in contrast to a scheduled-update antivirus system, the APC employs a real-time update system.

In a traditional antivirus system, a PC user had to manually update their antivirus in order to be protected from newly defined threats. Between these updates, a PC's virus definition is actually not 100% current. This leaves the PC vulnerable until the next update arrives.

However, within the APC, detailed information about tens of millions of files is updated and communicated continuously, every second, 24 hours a day, seven days a week. This means that every APC user benefits from immediate, on-demand access to the most current virus definitions – literally seconds after they are discovered.

2.3 Detection Protection

As mentioned, aside from simply accessing personal PCs, malware authors are clever enough to hack directly into a local antivirus program and view its detection processes from the inside. Hackers then use the antivirus program itself as a sort of laboratory to develop new viruses or adapt their malware to remain undetected.

Yet, since the APC stores these processes on the Cloud, these processes are invisible and inaccessible to hackers. Avira calls this third APC advantage "Detection Protection". Since the APC is not a local product, hackers are not able to view the entire antivirus platform and therefore are not able to investigate the various modules and engines performing tasks within. It is far more difficult to hack software that you cannot see. Second, once a virus is developed, a hacker must test their virus codes by uploading them and their different permutations en masse. Without a local product to use as a testing platform, hackers cannot complete this critical step.

2.4 Lightweight Profile

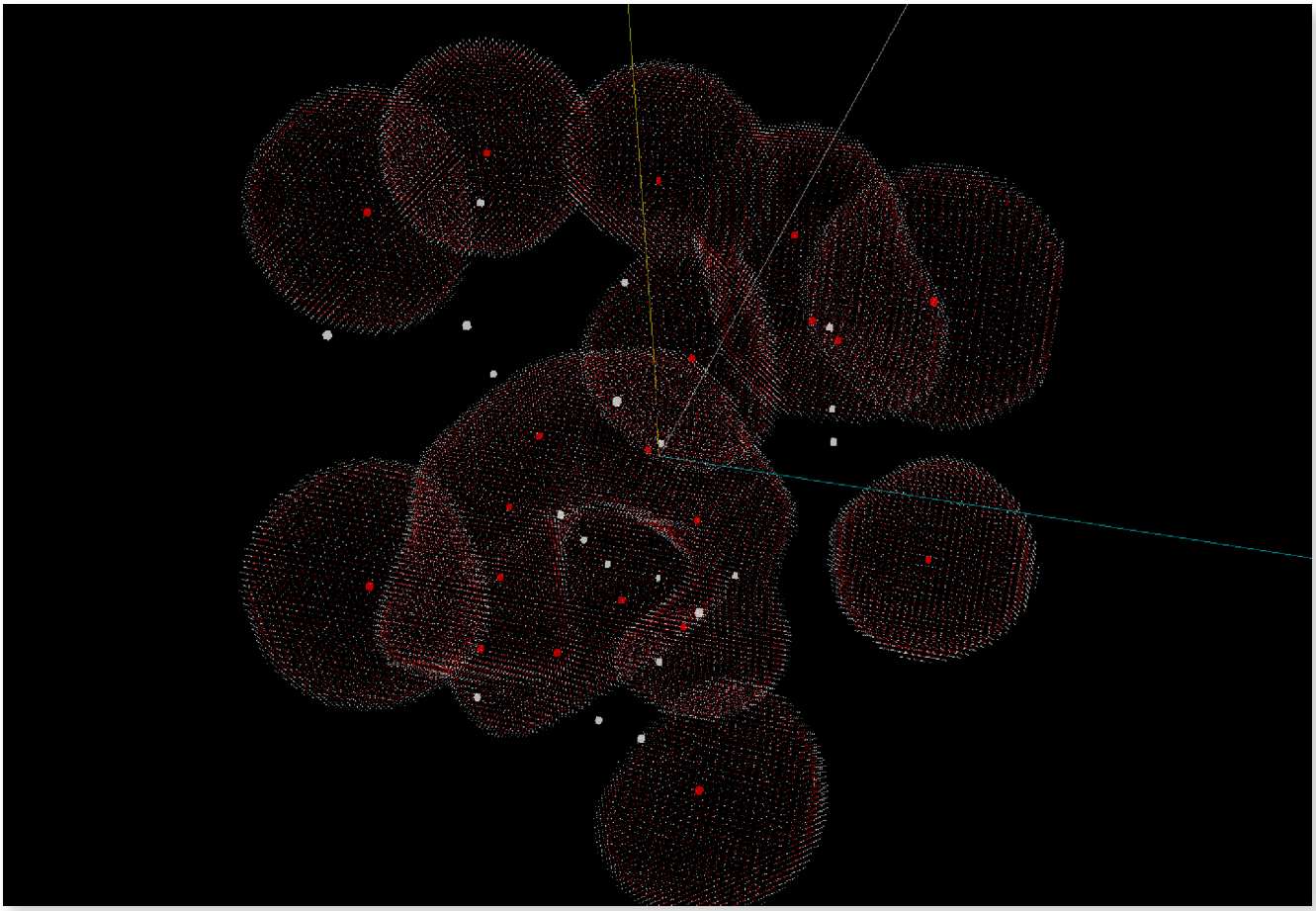
The fourth advantage of the APC is its incredibly lightweight profile. By offering Avira's award-winning detection engine on the cloud, users are benefitting from a product that accomplishes much more using far less local resources. Furthermore, APC-based scanning requires significantly less network traffic since initially, only the small file fingerprint is uploaded. This way, the APC can process 1000 virus definition requests using only 12 Kilobytes.

At the same time, Avira Protection Engineers have reduced latency by designing the APC with high-performance caches that scale according to the number of requests. The result is a leaner, slimmer antivirus platform that consumes significantly less PC and network resources when compared to traditional onboard antivirus platforms. This is especially important since there is simply no way a consumer PC could have the resources to run the Advanced Generic Detection processes included in the APC as the Artificial Intelligence platform features some of the world's most advanced file analysis module.

For example, Avira has automated malware analysis processes using advanced algorithms that interpret newly discovered files and classify them without any human intervention. This Artificial Intelligence uses convex optimization, a technique designed to minimize convex functions and convex sets to reduce instructions and use specifics to create generalities regarding un-

known file types. These generalities are then used to classify files into "good" or "bad" using thousands of characteristics as inputs.

Quite simply, the APC's proven scanning technologies operate on such a massive scale, that they are far too large and complex to run on a consumer PC



The APC is powered by an automated learning system that uses the latest advancements in machine learning to create highly optimized mathematical models for malware detection. In minutes, this self-teaching platform is able to complete tasks that would take researchers years.

3. Benefits at a glance

- Community Intelligence greatly expands the scope of detection
- Cloud storage allows users to take advantage of the Avira scanning engine, which is consistently ranked #1 in proactive and reactive AV testing
- Augmented Avira self-learning technology classifies files without relying on human intervention
- Low resource consumption for local machines
- Avira Protection Cloud database holds several hundred gigabytes and terabytes of uploaded files, but does not require these files to be stored locally
- Automated database requires no previous knowledge and minimal user effort
- Avira Protection Cloud grows and expands as users go through their day-to-day computing activities
- Dynamic file classification for advanced persistent threats
- Enhanced protection against rapidly evolving malware families
- Seamless integration with existing Avira product line and cross-platform support without eroding service
- The APC is a closed loop system that does not store any personal information. The APC relies on file "fingerprints" and is entirely anonymous

4. FAQ

What kind of data does my PC exchange with the APC?

Initially, only a small identifying portion of a file, called a "fingerprint" is uploaded. However, if that fingerprint is unrecognized, the APC will request the user to upload the entire file for a full analysis. Furthermore, only information about executable files is uploaded to the Protection Cloud (executable files end with .exe or .dll). Files such as PDFs, text files (.txt and .rtf), pictures (.jpeg, etc.), Word documents and other private files are not uploaded to the Cloud.

Can anyone get access to my uploaded data?

No. Uploaded data is only used for malware analysis and is saved in our cloud data center. Sharing this

data with third parties is prohibited. The process is entirely automated and no human checks the files individually. Most importantly, when uploading fingerprints or files, the user's identity is automatically deleted to ensure complete anonymity.

Is the uploaded data encrypted?

Yes. Every communication step between the user's system and the Protection Cloud is always encrypted using Transport Layer Security, or TLS.

5. About Avira

Avira wants its customers to 'live free' from spyware, phishing, viruses and other internet-based threats.

The company was founded 25 years ago on Tjark Auerbach's promise to "make software that does good things for my friends and family." More than 100 million consumers and small businesses now depend upon Avira's security expertise and award-winning antivirus software, making the company the number-two market share leader globally. Avira provides IT-security protection to computers, smartphones, servers and networks, delivered as both software and cloud-based services.

In addition to protecting the online world, Avira's CEO promotes well-being in the offline world through the Auerbach Foundation, which supports charitable and social projects. The philosophy of the foundation is to help people to help themselves.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang | Germany
Telephone: +49 7542-500 0
Facsimile: +49 7542-500 3000
www.avira.com