Reviewer's Guide

AVG Identity Protection 8.5

Contents

Who is AVG?

Founded in 1991, AVG Technologies has corporate offices in Europe, the US and the UK. AVG is focused on providing home and business computer users with the most comprehensive and proactive protection against computer security threats. AVG's award-winning products are distributed globally through resellers, select retail outlets, and over the Internet as well as via third parties through Software Developer's Kits. AVG has more than 80 million active users around the world.

AVG employs some of the world's leading experts in software development, threat detection and prevention, and risk analysis. This uniquely positions AVG to spearhead innovation in the industry. The company continues to invest in R&D and teams with leading universities to maintain its technological edge.

AVG has experienced significant growth in the last few years. The company is currently the world's fourth largest vendor of anti-virus software measured by installed user base. AVG will continue to expand and address the needs of the global market through improved technology and broader language and platform support.

What is AVG 8.5 Identity Protection?

In January 2009, AVG Technologies acquired Sana Security, a leading developer of identity theft prevention and protection software. Their advanced behavioral technology detects and removes malware based on what it does, not how it looks. When an attack occurs, the technology can quarantine and remove the software. This prevents users' unique personal information like logins, passwords and account information from being captured and transmitted to unauthorized third parties. No signature updates are required, because the software is continuously learning new application behaviors on which to base its detection. The technology complements AVG's existing portfolio by proactively delivering continuous threat detection and automatic removal of malicious software. Identity Protection (IDP) is integrated into AVG 8.5 Internet Security for consumers as well as being available as a standalone solution.

AVG's technology is unique in its ability to protect you against the latest threats. AVG IDP defends against identity thieves who could potentially access your personal and confidential information. Its behavioral analysis detects and deactivates any suspicious activity on your PC before it can cause damage. IDP kicks in to block new and unknown threats. In addition, it all happens in the background, in real time, and with minimal impact on system performance.

With AVG Identity Protection on your PC, you can feel safe banking and paying bills, shopping, and undertaking other online activities.

Benefits include:

- Best of breed behavior-based protection against new and unknown threats
- Instant layer of constant and proactive protection without the need for signatures or scanning
- Small footprint for fast, low-impact performance
- Compatibility with all popular consumer security products

A Layered Security Approach

AVG Identity Protection does not require other AVG products to be installed and running. However, when run with other AVG products, the combination delivers a highly effective layered security approach.

- LinkScanner® Technology for web threats and exploits
- AVG Signature Technology for known threats (viruses, rootkits, spyware)
- AVG IDP Behavioral Technology for unknown threats

The Changing Internet Security Landscape

The security threats faced by Internet users today are significantly different from those faced by computer users ten years ago. However, most conventional security products have changed little in their approach over the past decade.

As valuable as they are, conventional malware detectors that only attempt to clean up infections after the fact are no longer sufficient. Keeping users out of contact with these hidden programs that instantly breach their computer security is today's goal.

In a 2007 white paper, Yankee Group stated that signature-based anti-malware defenses were crumbling under the sheer force of the numbers marshaled by the enemy. They expected 220,000 unique variants in 2007. Recommendations they made to security vendors then included:

- Condition customers about the need for anti-malware technologies
- Integrate no-touch behavior into mainstream products (mentioned Sana Security as providing)
- Develop or license next-generation blocking behavior and herd intelligence blocking

Source: Yankee Group, Anti-Virus is Dead: Long Live Anti-Malware. June 15, 2007

Identity Theft is a Worldwide Problem

Identity theft is now the number one crime online and offline, costing US computer users more than $48 billion and claiming 9.9 million victims in 2008 alone, an increase of 22 percent over the previous year, according to Javelin Strategy and Research. Other statistics include:

- There is an estimated $3-4 billion market for ID theft services in the US alone (Source: Intersections and TrustedID Reports)
- The US Federal Trade Commission has listed ID Theft as the #1 consumer complaint for seven consecutive years
- Identity fraud is now the fasting growing UK crime (Source: CIFAS, the UK Fraud Prevention Service)
- Identity theft is costing the UK economy over $3.4 billion annually. (Source: CIFAS, 2006)
- One in four UK consumers has been a victim of identity fraud (Source: Equifax)
- Online banking fraud increased by 55% in the first half of 2006. (Source: APACS, The UK Association for Payment Clearing Services)

Behavior-based Protection

Behavior-based protection is provided by combining various features of running processes to generate a prediction of whether the process is malicious or not. Key to this is the fact that it is more difficult for a process to hide its behavior to evade a behavior-based system (such as AVG Identity Protection) than it is for a process to tweak its code to evade detection by a signature-based system.

Signature mechanisms are weak because they rely on the malicious code's structure not changing. However, using polymorphic techniques (for example), malware can avoid detection. Malware behavior, though, is more difficult to mask. Especially when measured at the operating system level.

In some respects, you can think of behavior-based protection as looking at the fact that "the whole is greater than the sum of its parts."

It is difficult to choose features that simultaneously capture the behavior of programs and are useful to discriminate normal and malicious programs. In addition, malware often consists of multiple processes that may not each have enough features to quality as malware. Yet, taken as a whole, the processes perform the malicious tasks. Suspicious behaviors could include creating a new process, then hiding in an unknown directory, adding unknown DLLs, capturing keystrokes when not necessary, or surviving multiple reboots.

AVG Identity Protection performs the task of looking "at the whole" to identify potential threats in real time. Before these threats can execute and steal someone's identity. Before a signature file

can be created. It looks at the combination and interaction of processes when it examines potential malware. It then classifies the potential malware as a normal program or a malicious program with a high degree of accuracy. Signature files never enter into the equation.

A behavior-based approach is different from behavior heuristics. Behavior heuristics look for common patterns in malicious code.

A behavior-based approach is also different from a sandbox-based system. Sandbox-based systems generally run and monitor the process in real time to see what the software does.

AVG Identity Protection Features & Benefits

AVG Identity Protection adds a layer of protection that improves your overall security against threats that your anti-virus software cannot see.

AVG Identity Protection:

- Delivers behavior-based protection against new and unknown threats
- Quarantines and terminates suspicious program activity
- Prevents identity theft by ensuring personal, private information stays that way
- Uses community-based research to continuously improve protection
- Incorporates AVG System Tools for advanced operating system monitoring and management

AVG Identity Protection uses a multi-behavioral approach to actively detect and remove malicious programs. By proactively monitoring PC behavior, AVG Identity Protection works by examining how the code acts, intelligently analyzing a combination of known bad behaviors to determine if a program is malicious. The product is able to prevent unknown threats that other products cannot protect against or see from successfully stealing users' personal identity and other critical information. This technology closes the gap between when a threat may arrive on a system and when other products provide signatures, downloads and scans that may be too late to provide the immediate protection necessary

The result is reliable, real-time threat protection that is constantly working to detect and remove new and unknown threats.

Tough on Threats

- Identity protection whenever you go online
- Unknown threats blocked before they can do damage
- Prevents rogue applications from executing

Easy on You

- No need for scheduled updates and scans

- Quick and easy to download, install and use
- Compatible with all major security products

Flexible Protection

Standalone AVG Identity Protection complements traditional anti-virus solutions from AVG Technologies and other popular security solution vendors. It adds an essential additional layer of protection against new and unknown threats. It provides an instant layer of constant and proactive protection from unknown viruses, rootkits, Trojans, and keyloggers. These are designed to evade traditional security methods and steal a user's identity and/or personal information.

AVG Identity Protection's major differentiator rests on the fact that examining each behavior individually (as other behavioral security products do) is insufficient in determining if a program is malicious. Malware is not a single behavior or process. The only effective way to classify malware is to analyze the combination of behaviors. This is where AVG Identity Protection excels.

Other Anti-Virus Products Paired With Standalone AVG Identity Protection

AVG Standalone IDP can be combined with other anti-virus products to provide protection against new and unknown threats to personal, private information.

Evaluating AVG Identity Protection

Recommended System Requirements

Operating System	Windows XP Pro or Home	Windows Vista 32-bit	Windows Vista 64-bit
Service Pack	SP1, 2	N/A	N/A
Applications	Internet Explorer 5.5 or later	Internet Explorer 5.5 or later	Internet Explorer 5.5 or later
Processor	Pentium III	Vista Capable	Vista Premium Ready
Clock Speed	600 MHz	800 MHz	1 GHz
Memory	256 MB of RAM	512 MB of RAM	1 GB of RAM
Disk Space	50 MB	50 MB	50 MB

AVG Identity Protection is initially available only in English. Please check the website at www.avg.com for the latest information on language support.

Installation

Installation is straightforward. There is no need to reboot the system. For someone who just wants protection, accepting the defaults will suffice. It is at this screen that you will enter the license key if you have purchased the product. You can also check for updates.

By installing AVG Identity Protection, and accepting the default configuration, data from Quarantine and Allow actions is automatically sent to AVG Labs. AVG Labs uses this information to refine AVG Identity Protection and to provide aggregated reports.

Users who do not want to allow data to be sent to AVG Labs can change this preference on the Settings page of the Control Center. To do this, deselect the Automatically submit to AVG Labs checkbox.
An icon appears in the system tray after installation. Upon installation, Identity Protection automatically protects PCs against known and unknown threats designed to target personal information. There are no signature files to download and install. The protection is constant.

Identity Protection's advanced behavioral technology detects and removes software based on what it does. Not on how it looks. When attacks occur, Identity Protection detects and removes all traces of the malware. This effectively prevents the threats from capturing and transmitting personal information like logins, passwords and account information.

To view the AVG Identity Protection interface, right-click on the system tray icon and select Control Center. From here you can:

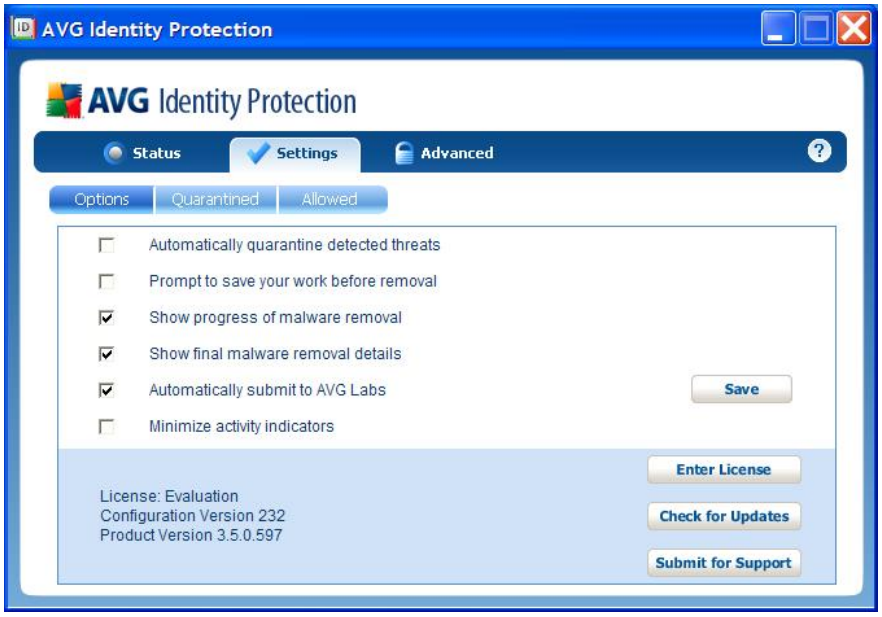
- Change settings for the notifications you receive
- Restore items from the Quarantine list
- Permanently remove items from the Quarantine list
- View active, monitored processes

There is no need to modify AVG Identity Protection's default settings. The default installation will:

- Show the progress of malware removal
- Show final malware removal details
- Submit any malware encountered to AVG Labs automatically

Other options you can initialize are:

- Automatically quarantine detected threats
- Be prompted to save your work before removal
- Minimize activity indicators

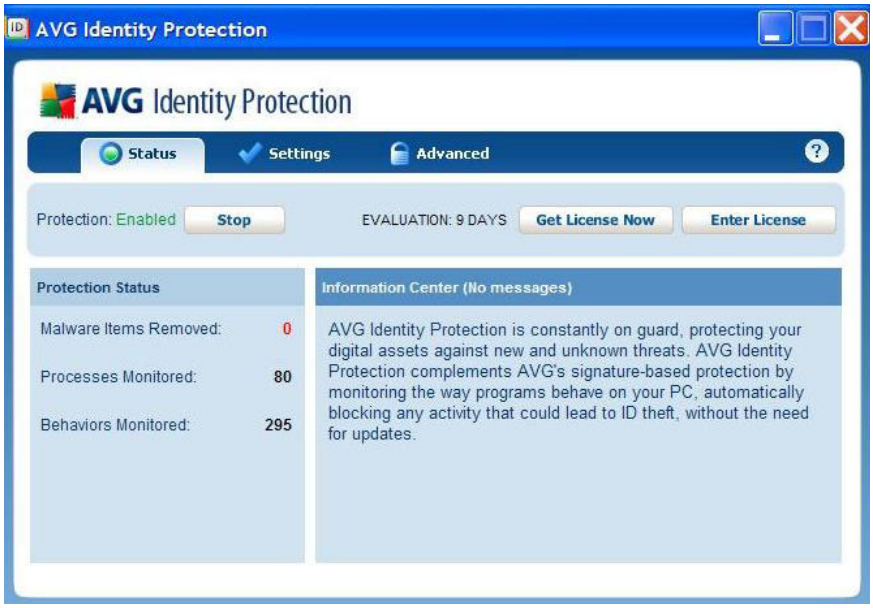


Advanced users can go "under the hood" to see what processes are running and view a record of recent activity. To do this, click on the blinking icon in the system tray. Under the Advanced setting tab, you can choose to Stop, Quarantine, or Allow a process.

Guided Tour

Now that AVG Identity Protection is installed, you can see what it does using a simulated malware sample as an example. AVG Identity Protection is unobtrusive until it finds something. There is no need to scan, no need to update pattern files. The product silently runs in the background.

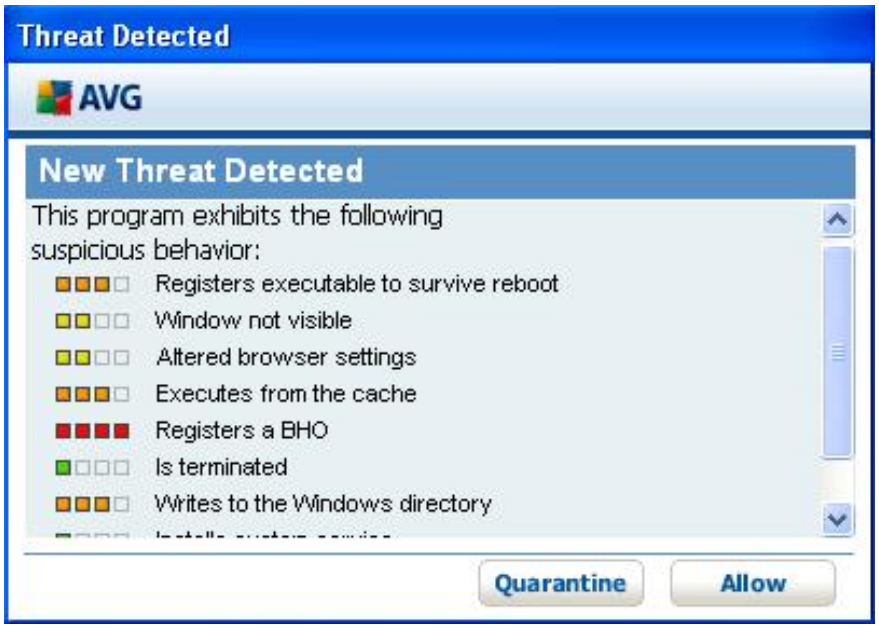
After installation, you can click on the blinking IDP icon in the system tray and this image will appear.



Threat Detected

AVG Identity Protection has identified our Test Trojan as a threat, displaying the following window which summarizes the suspicious behavior exhibited by this particular piece of malware. Click on Quarantine to prevent the program from executing; if the user knows and trusts the program, they would click on Allow. The program would activate and run in the normal way.

Clicking on **more details** provides additional information about this particular executable.



Placing the Malware in Quarantine

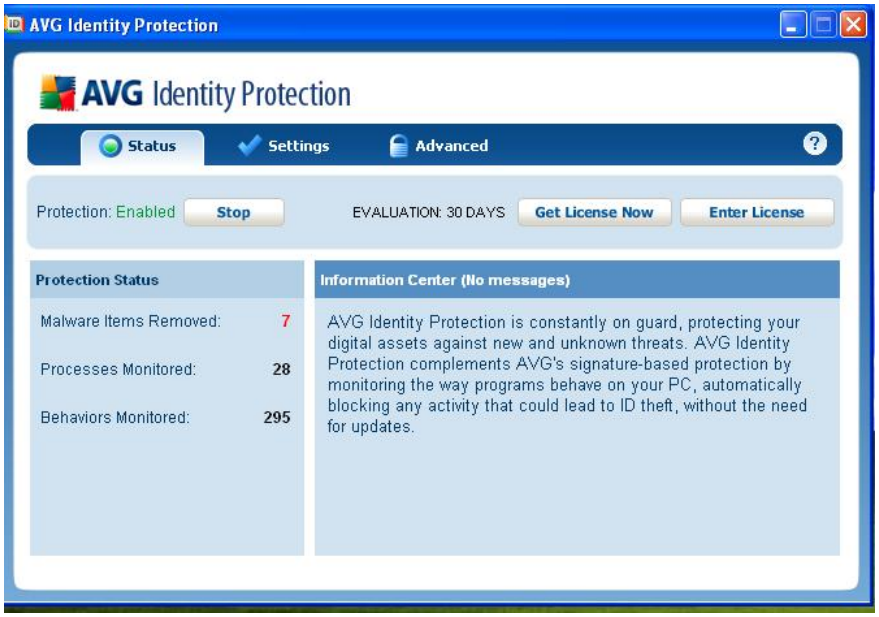
If you click to quarantine the malware, it will be placed in a quarantined file area on the PC and you will see the pop-up below. This window will also appear if, during set-up, you elected to have any detected malware removed automatically.

Obtaining Information on the Quarantined File

Most users will simply continue using their computer in the normal way at this point. More advanced users can obtain further information about malware held in the quarantine area. If you click on Quarantined under Settings, you will see additional information about the malware that you quarantined. It has not been deleted permanently. You can do this manually by clicking on the file and then clicking on Delete Permanently.

Monitoring Protection Status

Most users will never need to view the below. However, after placing the malware in quarantine, users can click on the status tab to view the total number of malware items removed. The user can just come to the status page to see if things are “okay” and to see if ensure protection is still on. The icon in the system tray will indicate if a problem is found.



Advanced Processes

Opening this window will let you see what events have taken place on your PC. The first screen below shows what the user would see prior to clicking on any potential malware. This first screen shows all monitored processes and their threat level. The second screen shows all activity and whether that activity is bad or good. In this second screen, AVG Identity Protection has identified the test malware. Clicking on that event will display some details about the malware. The casual user will never need to click on the Advanced folder or go into Activity.

The above screen show both what a user who “just wants to be protected” and a user who wants to “go under the hood" will see when malware is detected.

About the Above and Some Testing Caveats

The above should provide a feel for AVG Identity Protection’s capabilities. A simple product to run. Powerful in its capabilities. Equal protection is provided with both the standalone version and the version that is included with the consumer version of AVG 8.5 Internet Security.

Should you choose to test the software against “real malware”, it’s strongly recommended that you conduct the test on a separate test network.

Some other caveats for testing:

1. The malware has to be running and active. In other words, the malware needs to be executed. The test machine needs to be connected to the Internet, and/or whatever supporting infrastructure that it needs, for example whether some additional DLLs or a command and control center have to be actually there.

2. For behavioral detection to work, the malware needs to begin to carry out its mission. If it can't, for whatever reason, it will likely not exhibit its malicious behavior. Your best chance of achieving that is with fresh or recent malware.
3. VMWare doesn't always work for testing. The bad guys figured out that researchers use VMWare. Much malware today detects that it is running on VMWare and won't do anything.
4. It would be best if the malware is introduced into the system as close as possible to the way it will work in the wild. For example, if the malware is started from a command line, from a behavioral perspective it indicates that it's not stealthy and didn't start without user interaction.
5. Review the dynamic testing guidelines at www.amtso.org. See below. These provide additional guidelines on testing this kind of product and explain some of the potential pitfalls.

AVG Home User Product Family

Benefit	AVG Anti-Virus	AVG Anti-Virus + Firewall	AVG Identity Protection	AVG Internet Security
Protects against known viruses, worms, and Trojans	Yes	Yes	-	Yes
Protects against spyware and adware	Yes	Yes	-	Yes
Protects in real time against poisoned web pages	Yes	Yes	-	Yes
Screens your downloads for malicious content	Yes	Yes	-	Yes
Prevents accidental infections through IM chats	Yes	Yes	-	Yes
Stops hackers from accessing your PC	-	Yes	-	Yes
Helps prevent identity theft	-	-	Yes	Yes
Prevents new and unknown badware	-	-	Yes	Yes
Protection against hidden malicious code	-	-	Yes	Yes
Spam prevention	-	-	-	Yes
Free support and service 24x7	Yes	Yes	Yes	Yes

This guide has focused on the standalone version of AVG Identity Protection. More details on both home and business AVG products are on the AVG website at www.avg.com.

AVG Identity Protection Licensing

AVG licenses are purchased for a set period. AVG Identity Protection is licensed per PC. The standard license term is one year.

During the valid license period, AVG Identity Protection customers receive:

- All engine updates
- All program updates released during the license period
- Technical support (24/7) via e-mail and over the web

Support Policy

All program and malware database updates are free to the user during the license period. Note that for AVG Identity Protection, there are no malware updates.

Technical support information is available 24x7 through the following resources, which are accessible via the Support tab on the AVG website:

- FAQ pages
- Virus encyclopedia and Top Threats
- Virus removal utilities download area
- E-mail support (registered customers only)—submit web form or click Information**>Technical Support by E-mail** within the Control Center

Anti-Malware Testing Standards Organization (AMTSO)

AVG is an active member of The Anti-Malware Testing Standards Organization (AMTSO). AMTSO was founded in May 2008 as an international non-profit association that focuses on addressing the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies. AMTSO membership is open to academics, reviewers, publications, testers and vendors, subject to guidelines determined by AMTSO. We encourage reviewers to download and review testing guidelines and other materials that are available on its website. www.amtso.org

Contact Information

Craig Kensek
Global Product Reviews Director
craig.kensek@avg.com