

GFI White Paper

*Basic security -
Why purchasing antivirus,
anti-spyware and a firewall
is a must*

Paid security solutions offer significantly higher levels of protection, along with far greater value for the money through the inclusion of a broader range of key features tailored for the home user, while supporting parents and offering tools to help protect children from online harm.

Contents

Introduction.....	3
Free and paid solutions.....	3
The free software solution – you get what you pay for.....	4
Added value and protection – the paid advantage.....	5
Summary.....	6
About GFI VIPRE® Antivirus Home.....	6
About GFI®.....	7

Introduction

Home computers are at the front line of today's malware and Internet security battles, with a growing number of criminals and opportunistic hackers looking to exploit vulnerabilities in software and websites, as well as trick unsuspecting users into revealing sensitive information and handing over usernames, passwords and banking information¹.

It is a harsh reality of the Internet-centric world that we now live in – we live so much of our lives online, and carry out so many of our day-to-day interactions via our computers – that our computers are a key part of how we communicate, how we shop, how we enjoy entertainment and how we work. Therefore, it is essential that we keep our computers safe, secure and working.

Sadly, IT security is not a problem that goes away, but rather one that evolves alongside other aspects of modern computing such as operating systems, Web browsers and other key applications. As these applications change and advance, so do the security threats posed by the likes of malware, discovered vulnerabilities and data loss. Criminals looking to harvest useful information will go to great lengths, using both hardware and software² to capture useful information from consumers.

The developers of security solutions strive to create new and more advanced ways of combating the threats posed to computers, but are frequently met by increasingly sophisticated challenges posed by new strains of malware and new hacking tools. This is in addition to the challenges posed by known and unknown security vulnerabilities discovered in operating systems and key applications such as email clients, Web browsers, games and office productivity software.

Given the magnitude of the challenge, there is a vast array of security options on the market to help users protect their PCs from both Internet-based threats and malware that is introduced locally via storage devices (USB sticks, CDs, DVDs and other peripherals). Capabilities and prices vary considerably, but one group of products has broken the mold – the increasing number of free security solutions offering a basic level of security that is now part of the established security landscape.

The freeware model for certain key security products, such as antivirus, anti-spyware and firewall applications has helped many novice and cash-strapped users implement basic security on their computers.³ However, free security software is increasingly being considered as an all-encompassing option to provide home computer security, despite often lacking many features needed to protect a PC from the full range of threats and methods of depositing malware onto a computer.

So, why are paid security solutions still the best option, and why are free security solutions often unsuitable for anything but the most basic level of malware protection?

Free and paid solutions

The arrival of a plethora of free security solutions – composed of standalone freeware products and so-called 'lite' versions of existing paid solutions – has made the process of choosing the right security product for a home PC all the more difficult:

- » Lite solutions: Usually products from established IT security and antivirus vendors that offer a range of paid security software, these free products often retain the look and feel of familiar paid products, but contain only a fraction of the features and capabilities. For example, such a solution may only provide basic antivirus protection and very basic email scanning, but nothing else. Definition updates will often be less frequent as a means to both differentiate the support and service offered and to help underline the benefit of buying the paid version of the same product. There will often be in-application pop-ups and other promotional windows encouraging you to upgrade to the paid equivalent, which will offer more features, including many core features needed to ensure robust data and PC protection. Support options within the lite product will often be limited to email queries and a Web support forum

¹ <http://www.timeslive.co.za/thetimes/2011/06/20/identity-thieves-lurk-online>

² http://www.theregister.co.uk/2011/02/15/hardware_keyloggers_manchester_libraries/

³ <http://www.virusbtn.com/virusbulletin/archive/2011/06/vb201106-comment>

- » Standalone free solutions: These are usually products emanating from the open source and other free software communities with no commercial ties to an existing paid product or commercial IT security vendor. Support is usually provided in the form of peer support, while software updates and definition file refreshes rely on a volunteer workforce of developers and beta testers, meaning that while the product may be sound, updates will often be less frequent and less predictable than those for products funded through sales, subscriptions and support contracts. With no income source, development is limited to volunteers' spare time, so release schedules can be erratic and known bugs are not always fixed in a timely manner.

Free security software already has a foothold in everyday computing, thanks largely to the number of integrated security products and features included in later versions of Microsoft Windows (namely Windows XP, Vista and Windows 7), along with Microsoft products offered via the Windows Update patch distribution service. Microsoft's Windows Firewall is the most typical free security product used today, as it has been bundled in the Windows operating system since the Windows XP service pack 2.

The inclusion of basic security applications, such as a firewall, in an operating system can complicate matters, with users sometimes believing there is a higher level of security with integrated security products.

These products are not intended to offer long-term robust security protection, but rather to provide consumers with early-stage 'out of the box' protection after they first install the OS or purchase a new PC.

More recently, Microsoft has also moved into the free antivirus market with the launch of Microsoft Security Essentials⁴. This free product is distributed via Microsoft's Windows Update service and replaced Windows Live OneCare, a commercial subscription-based antivirus service for home users. However, Microsoft Security Essentials is geared for basic consumer use and is a prime example of a free security product that is neither suitable nor able to deliver sufficient protection.

The free software solution – you get what you pay for

There are more choices than ever in the market⁵, but the solutions offered vary so significantly from the low end to the high end that ensuring the one chosen has the right combination of features, support and updates can quickly become a challenge for consumers. This is particularly true when faced with the daunting array of products for sale online or a shelf-full of competing products in a PC store.

It is important to remember from the outset that most free security products, in particular free antivirus solutions, free firewalls, free anti-spyware tools and free anti-spam products from known software companies, are primarily aimed at a single-user consumer audience and at providing a minimum level of security. This audience has little, if no knowledge of security, it is certainly not IT savvy and, because users see the AV icon on their desktop, they believe that their machine is protected. Although there is basic protection in place, with so much important data at stake, can a user take the risk that their computer is 'almost' protected?

When choosing the right home PC security product, whether it is free or requires some form of one-time or ongoing payment, it is essential to consider the following points:

- » Frequency of updates – One of the biggest differentiators between paid and free software is how and when the products are updated. It is crucial to look at how often the application receives updates, as well as how regularly definition database files are refreshed. For products such as antivirus and anti-spam products, frequent definition updates are needed to keep on top of the latest security threats. This is a key area where free products lag behind paid solutions. Infrequent updates save money, but also compromise the effectiveness of a solution

⁴ http://en.wikipedia.org/wiki/Microsoft_Security_Essentials

⁵ http://www.virusbtn.com/vb100/latest_comparative/index

- » Support options – How and where to get support and ask questions are critical for an IT department to deliver effective user support. By their very nature, free products have few means to fund a substantial support operation, meaning that support is usually kept at arm's length from the developer in the form of email queries, Web forums and developer blog posts. This is far from ideal, especially for users who are not particularly technical or Web savvy. The standard of the support offered may well be high when a request is received but beyond this, free software usually offers no guarantee to uptime or response time on support queries. So an urgent query may go days and weeks without being answered, and a user may have to rely on unverified guidance from peer groups on Web forums, leading to further problems and misdiagnosis of issues
- » Limited scanning and detection – Basic security solutions are by their very nature stripped back to the basic functions. They lack the peripheral features and detailed scanning options included in paid solutions that deliver value and justify ongoing investment costs.⁶ Free products lack many real-time scanning and reporting capabilities found in commercial products, particularly paid versions of the same application
- » Integration with third-party applications – Free security software is rooted firmly in the consumer space, so ensuring compatibility with third-party products such as some email clients, browsers, file downloading applications and gaming networks cannot be guaranteed. Basic support for the most common products – such as Microsoft Outlook and Windows Live Mail – can usually be found, but beyond this, there is little integration of free antivirus and security software with the most popular Internet applications
- » License terms – Many free software products specifically prohibit commercial use, including use in a business environment or on a home PC also used for work activities. Furthermore, some open-source free products fall under open-source licenses that prohibit commercial use without payment, so you have to pay to use a 'free' product, but end up with the same lack of features and technical support.

Added value and protection – the paid advantage

It is important to note that many free security software products have a very good reputation and have received many plaudits from the media. However, when compared head-to-head with paid products, the differences soon become clear. The additional features and tailored capabilities of paid security software stand out and the level of compromise that is involved in using a free product is often significant:

- » Email platform protection – Particularly for antivirus and anti-spam solutions, there are few free products that support a broad range of email clients, while some struggle to effectively scan server-side email such as IMAP, Gmail and other proprietary server-based email services. Most paid solutions support a wide range of email applications, email protocols and can even provide robust protection when using Web-based email
- » Web filtering and rogue site interception – Basic protection usually stops at limited port blocking for firewalls, basic malware scanning and detection for antivirus and periodic scans for anti-spyware solutions. Commercial security products go much further, combining higher levels of core protection with additional interception and protection capabilities, such as intercepting known bad websites before they have a chance to load on a client PC, blocking parts of pages from loading if they are from untrusted or known bad sources
- » Broad coverage – Some free products specialize in one thing, leaving the rest under-developed and under-resourced. This often depends on the specific DNA or technical focus of the application and its developer. Commercial security solutions with a broader range of dedicated developers and resources frequently out-perform their free counterparts across a range of core functions, from scanning times to detection levels.

⁶ http://www.ehow.com/facts_6886278_limitations-antivirus-software.html

- » Parental control and lock-down capabilities – Parents wanting to maintain a level of control over what their children can and can't use their PC for will find that basic, free security software offers little in the way of Web filtering, content and application blocking and activity logging. An important feature of any well-rounded home PC security suite is capabilities for parents to 'lock down' PCs and maintain control over use, so that children can use a PC without needing constant parental supervision. Regularly updated lists of good and bad sites ensure that Web filtering keeps the majority of bad and inappropriate sites away from view, while content controls can ensure children are not using chat sites and other potentially harmful Web services when unsupervised.

Summary

The basic security afforded by free and integrated security products represents an important consideration for home users, particularly in these economically strained times. However, these tools remain largely focused on delivering the absolute minimum acceptable level of protection for individual users and offer no guarantees or route to complain if they fail. Furthermore, such products only serve to deliver a modest level of protection, partly in order to separate them from paid stable mates, but also to minimize the operating costs associated with delivering database and application updates to a user community that is not paying towards the on-going development and upkeep of a product and its back-end support systems.

Paid security solutions continue to offer significantly higher levels of protection, along with far greater value for the money through the inclusion of a broader range of key features tailored for the home user, while supporting parents and offering tools to help protect children from online harm.

When choosing the right security solution, it is critical that you consider and evaluate all the options available. It is also important to understand what you will get in return for the purchase or subscription cost of a security product, and what compromises would need to be made in order to forgo the cost of software. While free software can seem like an easy way to save some money, you have to balance this against the cost – both in time and money – if your PC is rendered inoperable by malware or if your personal and financial information is hijacked by criminal organizations.

You can seldom afford to compromise on PC and information security, and thus should think twice before relying solely on a free or integrated security solution.

About GFI VIPRE Antivirus Home

VIPRE Antivirus Home is designed to provide the fundamental, necessary desktop malware protection that you need in today's threat environment without slowing down your PC. Instead of creating a product loaded with 'marketing' features, GFI Software has focused on core functionality that consumers need, including comprehensive malware protection, easy-to-use menus and options, free technical support, free malware removal assistance and one of the best and most frequently updated malware detection databases on the market.

All this is combined with underlying technology such as Active Protection™, which delivers real-time monitoring and protection against known and unknown malware threats. Active Protection works deep inside your Windows installation to watch for malware, stopping it before it activates and does damage. VIPRE Antivirus Home also offers a range of Premium features including a powerful integrated firewall.

VIPRE Antivirus Home comes with a 30-day money back guarantee. If you are not satisfied, we offer a hassle-free full refund within this period.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized enterprises (SMEs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

ENGLAND AND IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.