

# **GFI** ADVANCED TECHNOLOGY GROUP

## STOPPING MALWARE: BEYOND SIGNATURES

April 2011



Table of Contents	
Executive Summary .....	3
Introduction .....	4
It's More Than Technology .....	4
Making a Wise Choice .....	4
Must-Have Anti-Malware Partner Requirements .....	5
Ability to Meet Time-to-Market Requirements .....	5
Trusted SDK Experience and Security Expertise .....	5
Unparalleled Customer Support .....	6
Proven SDK Technology .....	6
Engineered Efficiency.....	6
Detection Rates.....	6
Performance.....	6
Avoid False Positives/Faulty Definitions .....	8
Building for Success .....	9
VIPRE Architecture .....	10
How it Works .....	11
Your Product, Built-in Protection .....	13
Perimeter Protection .....	13
Perimeter Protection Packages Offered .....	14
Perimeter Platform Support .....	14
Endpoint Protection .....	14
Endpoint SDK Packages Offered .....	14
Endpoint Platform Support .....	14
Endless Possibilities: Placing the Protection Where It Matters .....	15
Top-Notch Relationship and Service (case study - Shavlik) .....	15
THE GFI MESSAGE (it's about the partnership) .....	15
About GFI Software   Advanced Technology Group .....	16
Appendix A   Product Comparison .....	17
Awards and Certifications .....	19

## Executive Summary

Respectively, hacking and malware consistently rank #2 and #3 as the main causes for security breaches (Verizon Business, 2010)<sup>1</sup>. While most organizations have gained some level of control over the protection for their environment, hackers continue to become more sophisticated in their methods, constantly learning how to increase their capacity for causing harm to the world's information systems and stealing the precious data housed on them. For example, some attackers prefer to use large numbers of exploits used as a combined exploit kit to get the job done. For example, the largest exploit kit observed in 2H09 included 23 exploits. (Microsoft, 2009)<sup>2</sup>. As their attacks increase in depth, complexity, and invisibility, keeping up with the technology to combat these threats can be difficult at best.

Signature and rule-based detections remain an important piece of the protection puzzle<sup>3</sup>, but it's certainly not enough on its own. New, proactive technology is required for effective malware detection and remediation, streamlined performance, and efficient resource utilization.

While protection against system attacks requires technology such as antivirus, the solution can't be solely about the technology. In addition, both service and support are key components to consider when looking to define, design, build, deploy, and support an information system protection solution on time, in today's demanding environment. Selecting a partner that will be there when it matters is crucial.

This whitepaper examines the challenges in integrating malware protection into broader product offerings, provides an in-depth review of the VIPRE® SDK, and covers the benefits of partnering with the GFI Advanced Technology Group to deliver the most efficient and effective protection solutions available.

1. Verizon 2010 Data Breach Report
2. Microsoft Security Intelligent Report Vol8
3. Gartner Research Blog: Long Live AV

## Introduction

With hacking and malware responsible for over 95% of reported data compromises<sup>4</sup>, it is important for security-minded technology vendors to not lose sight of the core anti-malware capabilities required to deliver secure systems and proactive protection to their clients. Worms and other potentially unwanted software were two categories of threats that increased in prevalence during the previous four quarters. (Microsoft, 2010)<sup>5</sup>

Of these two categories, one of the most noteworthy types of attacks comes via rogue security software. This malicious software displays false or misleading messages about vulnerabilities or infections located on the victim's PC that need to be repaired. The software usually offers to do this as a service for the victim, for a price. Often referred to as scareware, the malicious software appears to provide a security benefit when in reality it uses an array of common attack methods to swindle money from its unsuspecting victim. According to a Microsoft Security Intelligence Report, this form of attack has increased by 46.5 percent in recent months, up from 5.3 million infected computers in 1H09 to 7.8 million infected computer in 2H09. This would suggest that there is a huge market for the creation and distribution of these software applications. (Microsoft, 2009)<sup>6</sup>

This is proof that anti-malware technologies and their resulting protection products are far from redundant and remain a critical component in securing the world's information systems. Providing the best possible malware detection and repair is a non-negotiable item and the selection of the right technology and partner must be considered carefully.

Are you missing anti-malware capabilities in your product? Or, have you let your existing malware detection capabilities slide? Do you risk failing to deliver the much-needed protection your clients demand and deserve?

## It's More Than Technology

When it comes to delivering value to the customer, being innovative and creative is only half of the equation. There is more to it than just bringing a product to market. To complete the picture, the solution must combine industry expertise and unmatched support such that the end user can truly reap the rewards of the solution.

## Making a Wise Choice

Select the wrong partner and, not only could you find yourself wasting time integrating a less-than-perfect anti-malware engine into your offering, you could put your clients at risk of being compromised. At the same time, you could find your product lost in the product development shuffle as the provider of the SDK attempts to fix their own anti-malware products first, leaving yours to lag behind with an outdated engine.

4. Verizon 2010 Data Breach Report

5. Microsoft Security Intelligent Report Vol9

6. Microsoft Security Intelligent Report Vol8

## Must-Have Anti-Malware Partner Requirements

The following should be considered compulsory when selecting a partner to support you in the on-time delivery and ongoing maintenance and support of your malware-protecting product offering.

### Ability to Meet Time-to-Market Requirements

Building the best solution possible is all for naught if the offering doesn't make it to market on time. It is of utmost importance to meet the clients' needs in time for it to matter for them. Worse yet, if building the solution requires more resources than what should be allocated due to poorly designed APIs or poorly documented functions, your organization would be wasting valuable resources that could otherwise be applied to additional engineering tasks geared toward generating additional revenue and/or increasing customer satisfaction.

The VIPRE SDK includes well-documented features and APIs, with clear examples of application code. With this kit, developers get everything they need to 'drop in' anti-malware protection into any new or existing product.

### Trusted SDK Experience and Security Expertise

It is important to select a security partner and SDK technology that has consistently proven its success. The technology should be developed by a team of security experts familiar with building effective, efficient, and easily embeddable OEM software. There are a variety of methods available to determine the success of the provider and its technology. Some of the most common methods include checking with industry analysts, reviewing independent product reviews, speaking to a few reference clients, and most importantly, reviewing your own specific development and support requirements directly with the SDK provider.

To ensure top-notch detection rates, the VIPRE SDK is backed by a dedicated team of research professionals specializing in the discovery and analysis of dangerous malware and malicious websites. The team creates new signature definitions and advanced heuristics for zero-day threats, rogue applications such as fake antivirus programs, and other malicious files. Additionally, GFI's user community, consisting of millions of VIPRE consumer users, anonymously sends potential threat information to GFI Labs™, thereby improving their ability to produce the best detection and remediation capabilities available.

GFI and its product offerings have been recognized by a number of well-respect institutions around the world, ranging from independent test labs to industry media publications and detection comparative groups to channel analysis firms. VIPRE holds numerous awards and certifications from recognized industry reviewers and testers.

The VIPRE SDK can be found in use within many industry-leading protection offerings. Case study references can be found throughout this paper.

### Unparalleled Customer Support

GFI has a team dedicated to helping OEM partners implement the VIPRE SDK. U.S. based support includes a dedicated developer for any escalated SDK support issues. Additionally, GFI has an on-line ticketing system through its dedicated OEM portal coupled with other on-line support tools.

### Proven SDK Technology

Below are some of the more critical technology items to consider when selecting an anti-malware engine SDK.

**Engineered Efficiency:** A number of SDKs available on the market today have been developed as an afterthought to an existing anti-malware product offering. These are typically the result of the engine being extracted from the

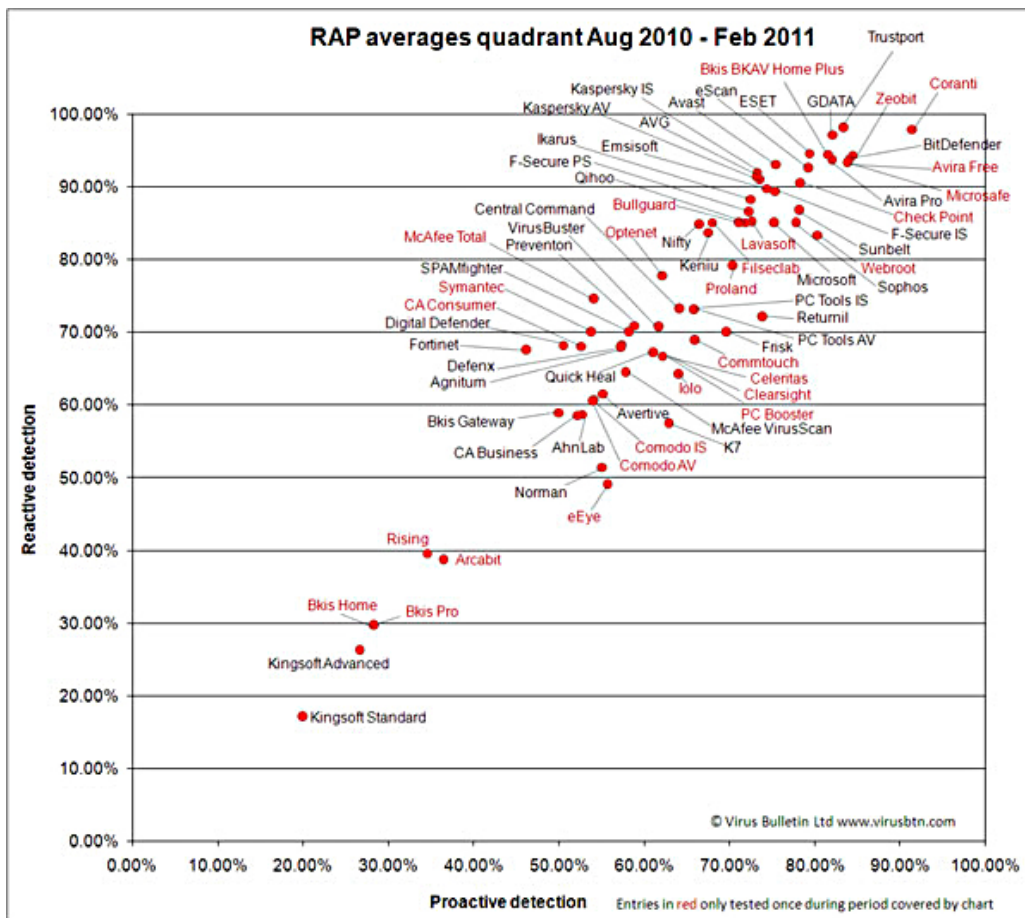
product and then wrapped in an SDK. Many vendors build a separate SDK just for OEMs use – a different version of the product, a different code base, different support cycle, and slower response times for reported bugs. To this end, a number of these vendors' SDKs suffer from being bloated and extremely inefficient, making the resulting products ineffective and the in-market support process unpleasant.

The VIPRE SDK has been designed from its inception to be an embeddable malware engine for purposes of delivering industry-leading detection capabilities to software and appliance vendors around the world. To ensure ease of use and functionality as its client expect, GFI 'eats its own dog food'. To this end, the VIPRE SDK is used within both the VIPRE Antivirus Business and VIPRE Antivirus Home versions of their endpoint protection products.

**Detection Rates:** The primary purpose of an anti-malware engine should be to provide the best detection capabilities possible. In order to accomplish this, a multitude of protection capabilities must be available within the engine, with the scanning functions available to the calling application from well-documented, easy-to-use APIs.

The VIPRE SDK benefits from multiple threat data sources for developing its threat definition updates. GFI Labs processes tens of thousands of malware samples a day, utilizing its live threat data and folding it directly into the VIPRE SDK.

The following chart shows the Virus Bulletin RAP results obtained over the last four tests, with average reactive scores plotted against average proactive scores for each product. GFI/Sunbelt is amongst the top performers in this report.



Source: Virus Bulletin<sup>7</sup>

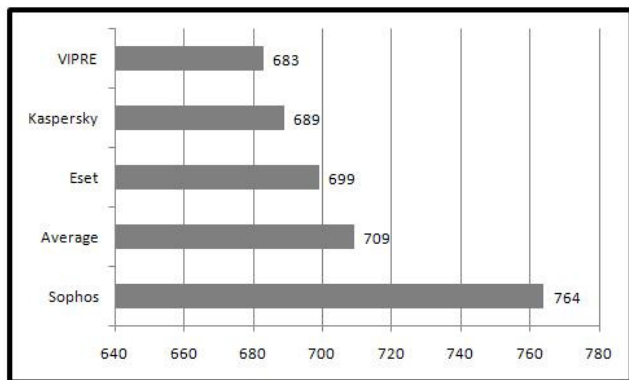
7. Virus Bulletin RAP Averages, Aug 2010 -Feb 2011

When the VIPRE endpoint protection product is deployed to an already-infected environment, rest assured that it will effectively detect, identify and clean up any payload left behind by existing malicious software that found its way onto the network and endpoint devices prior to VIPRE doing its job.

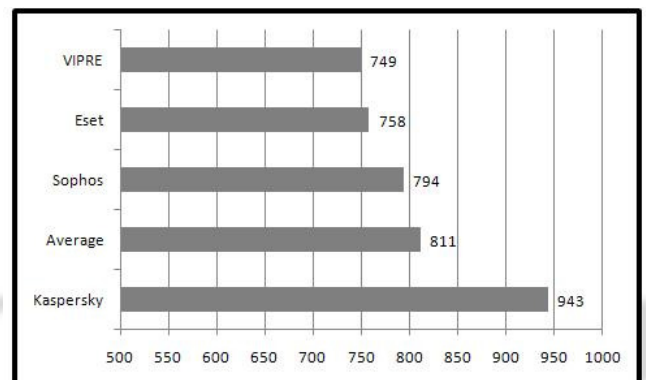
**Performance:** The anti-malware engine of choice should be small in size, easy to deploy, quick to install, lightweight, nimble, efficient, and not utilize an unreasonable amount of memory or CPU while doing its job. This high-performance engine must not come at the expense of experiencing the best protection and repair rates possible.

After it has been installed, the protection product should use memory wisely and efficiently. Be sure to look at memory usage while the application is idle and while it is performing a security scan. Refer to the figure below for example memory usage statistics for some of the most common protection products on the market.

**MEMORY USAGE DURING SYSTEM IDLE (MEGABYTES)**

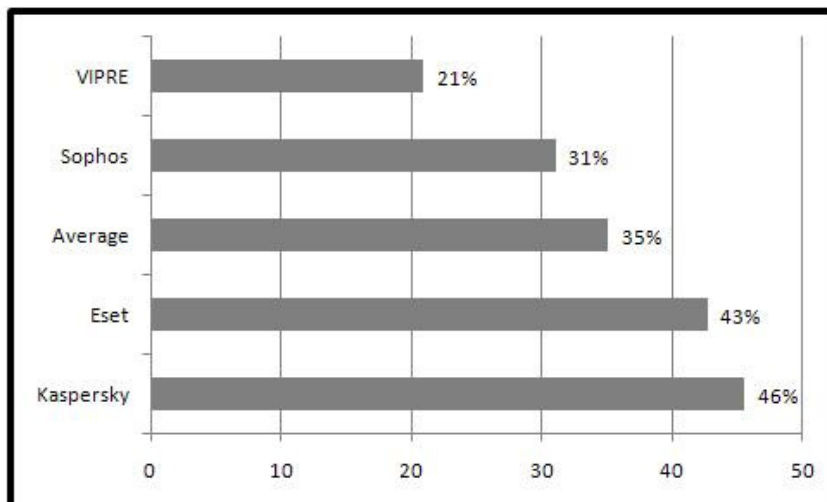


**MEMORY USAGE DURING SCAN (MEGABYTES)**



Equally important to memory utilization is the amount of CPU used by the application. Refer to the figure below for example CPU rates during a security scan for some of the most common protection products on the market.

**CPU USAGE DURING SCAN (PERCENT)**

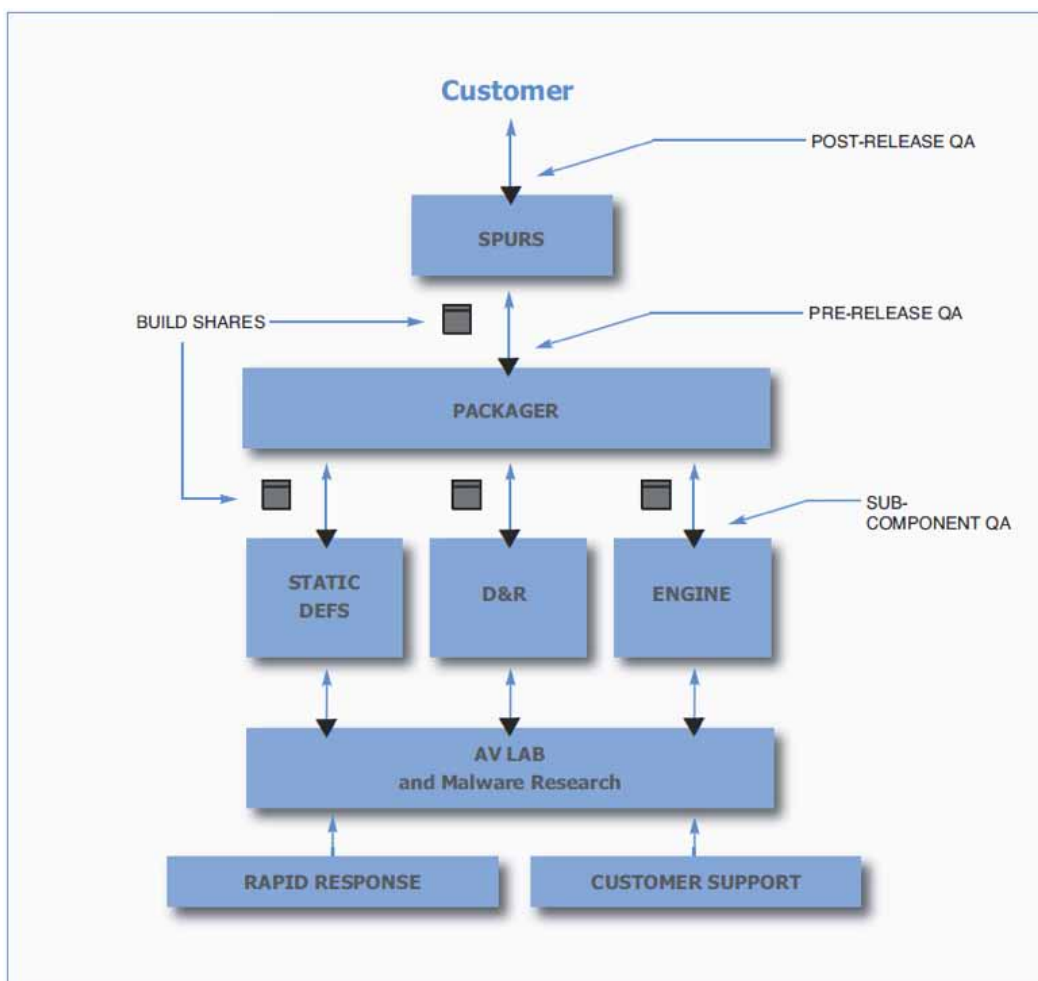


**Avoid False Positives/Faulty Definitions:** Turning up the dials to get the best possible detection rates oftentimes leads to non-threatening activities being erroneously identified as threats or malicious behavior. These faulty detections are referred to as false positives. Chasing down a false positive can be annoying at best and a huge waste of time in a more severe case.

Most organizations have either indirectly heard of, or have experienced first-hand, a virus definition or signature set that causes the system to crash, reboot, or even be rendered disabled. This is unacceptable behavior and the history of success and failure in this area should be reviewed very carefully as the SDK provider is selected.

The VIPRE SDK avoids false positives by incorporating an extensive whitelist of legitimate vendors' digital certificates where the certificate is used to digitally sign the binaries and confirm that a given file has been published by a given vendor in a trusted manner. Additionally, the SDK uses a whitelist of file hashes of common applications in the cases where a file certificate is not available.

The VIPRE SDK also avoids false positives and bad definition sets from being rolled out and being deployed in production by passing each and every threat definition through multiple comprehensive quality assurance tests, checking for false positives and verifying detection and remediation accuracy.



## Building for Success

GFI has translated years of hands-on and in-the-trenches experience researching, identifying, and remediating the most sophisticated of malware in order to develop its next-generation anti-malware protection technology. The VIPRE SDK is not a result of cobbled together functions built on top of older generation antivirus engines. The VIPRE SDK is designed using the latest design best practices and cutting edge technology, delivering the best detection, remediation, and performance. Equally important, the VIPRE SDK does not use any sourced technology components.

The VIPRE SDK creates the opportunity for software developers, solution providers, and OEM partners to design, develop, and deliver specialized yet economical high performance, best-of-breed, security-enabled applications using its lightweight, real-time anti-malware protection engine with minimal development time.

## Top Features and Benefits

**Easy integration:** With well-documented and extremely flexible APIs, it is easy to integrate the protection required into any appliance-based or application-driven offering. GFI provides all the components needed for a developer to simply 'drop in' anti-malware capabilities into an existing application or appliance with a minimum amount of customization or development work. The VIPRE Gateway SDK can also be used as a drop-in replacement for ClamAV with minimal integration effort as well.

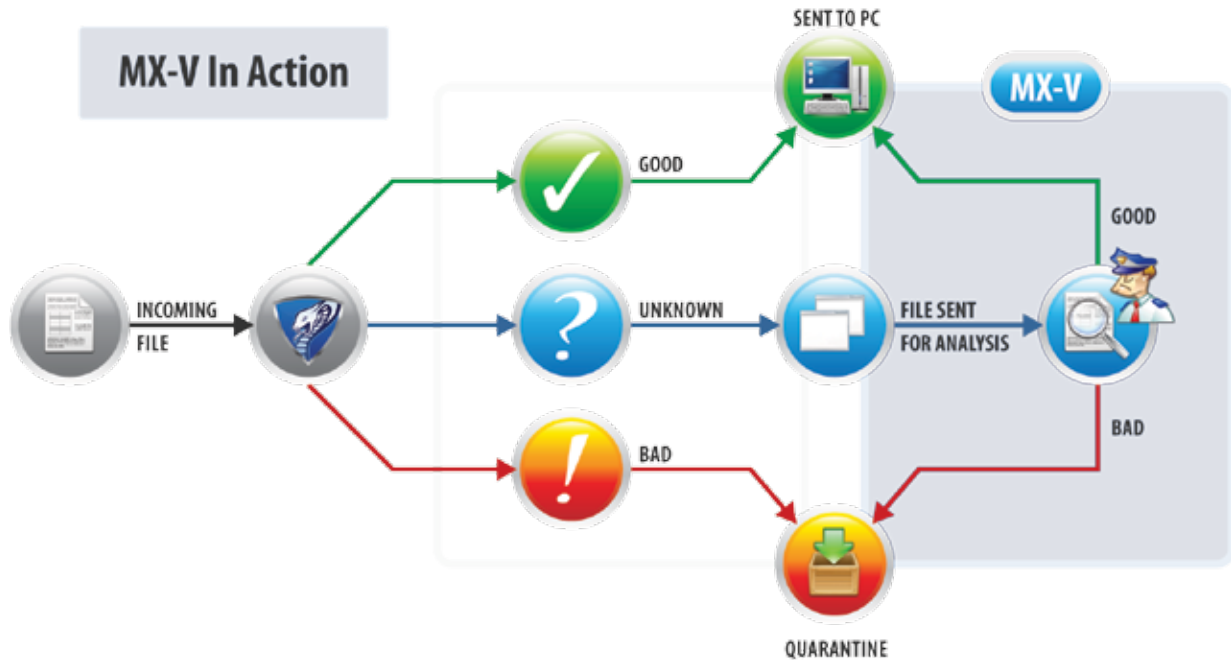
As an OESIS-OK Gold Certified product, VIPRE provides seamless integrated control and visibility to the desktop when using any OESIS-enabled device, including the market-leading NACs and SSL VPN gateways from vendors such as Cisco, F5, Juniper, Microsoft, SonicWALL, HP, and Dell.

GFI's VIPRE SDK is by far the most complete and easily-embeddable offering on the market.

**Top rated performance:** VIPRE delivers high speed and memory efficient scanning through the use of its advanced technology engine. The result is the lowest possible impact on CPU and memory. Experience top-notch security with all the functionality you need and nothing you don't – ensuring optimal performance for your end users.

**MX-Virtualization™ (MX-V):** MX-V malware analysis technology rapidly analyzes potential malware by observing its behavior in a virtual environment so that malware never actually executes on a user's machine. Because MX-V uses the fastest emulation technique available, Dynamic Translation, it is extremely fast, able to identify potential threats by observing their behavior without compromising system performance. MX-V technology helps protect users from many unidentified or new variants of malware without the need for a specific signature or rule.

**Unmatched protection:** Protection against known and unknown threats using a combination of proprietary detection methods including signature-based capabilities, behavioral-based analysis, heuristics, and dynamic translation.



The advanced rootkit scanner finds and removes malicious and often hidden processes, threats, modules, services, files, Alternate Data Streams (ADS), and registry keys. Your application can optionally block Java script, VB scripts, and ActiveX controls as well.

VIPRE includes comprehensive protection against email viruses, with direct support for Outlook, Outlook Express and Windows Mail along with support for any other email program that uses POP3 and SMTP.

Included in the VIPRE SDK are pre-defined IDS rules that are updated through VIPRE threat signatures. You also have the ability to write detailed rules based on the Snort® language to complement your own application and target security profiles. Rules can be made to block administrator-defined inbound or outbound traffic allowing you flexibility in your own implementations of the SDK.

**Real-time updates:** In addition to traditional analysis methods, GFI uses its own GFI Sandbox™ automated malware analysis technology to identify malicious files and create signatures without the need for human intervention. GFI's teams of researchers in North America and Asia monitor this process, verify the signature effectiveness and write new behavioral signatures where needed. The resulting definitions are updated frequently throughout each day using the continuous update service. This assures that your offering and its users, have the latest, fully-tested threat definitions available to them when it is needed.

## Your Product, Built-in Protection

The following are sample integrations of the VIPRE SDK.

### Perimeter Protection

Use the VIPRE SDK to deliver protection within your gateway product, such as a perimeter firewall, an email gateway, or a customer portal web application.

#### SAMPLE USE CASE

Deploy a comprehensive anti-malware scanning service as a stand-alone solution, or as part of an integrated suite of managed security services. VIPRE technology allows you to quickly integrate efficient malware protection into your existing or new gateway products. VIPRE Gateway SDK provides you unmatched real-time malware protection for software proxies or gateway appliances from an industry leader.

*"After studying the market, GFI Software was a clear choice. The integration of VIPRE as an exciting, market-leading solution will significantly boost malware and virus protection for our customers."*

George Lungley, Managing Director  
SmoothWall

### Perimeter Protection Packages Offered

- Core Integration: Provides deep, granular control with a direct interface to the scan engine and low-level integration of VIPRE with your application.
- Threat Engine Integration: Leverages the core while providing your application with real times scanning with Active Protection and rootkit protection at wire speed.

### Perimeter Platform Support

- The VIPRE SDK works with virtually any flavor of Linux

### Endpoint Protection

Use the VIPRE SDK to scan memory, files and network activity to deliver malware protection within any endpoint product imaginable, such as an endpoint protection solution, a SSL/VPN client, or a cloud-based file collaboration synchronization client.

**SAMPLE USE CASE**

A full arsenal of malware detection, intrusion prevention, remediation, and firewall technologies in a single, powerful threat engine with low impact on system resources. The VIPRE Desktop SDK allows you to quickly integrate best-of-breed antivirus, bi-directional firewall, and web filtering into your existing or new products, providing unmatched endpoint security.

*“When you embed an SDK in your product, you want clean, straight-forward integration, best-in-class functionality and performance, and a technology team that knows their business. With VIPRE SDK and the team, you get all of this and more.”*

Ben Battle, VP of Product Development  
ScriptLogic Corporation

**Endpoint SDK Packages Offered**

- Core Integration: Provides deep, granular control with a direct interface to the scan engine and low-level integration of VIPRE with your application.
- Threat Engine Integration: Leverages the core while providing your application with Active Protection, rootkit protection, and full system scanning capabilities.
- Service Integration: Leverages the Threat Engine while adding even more functionality, all wrapped up in an easy to use COM interface. Service allows you to quickly build a UI and get a product to market.

**Endpoint Platform Support**

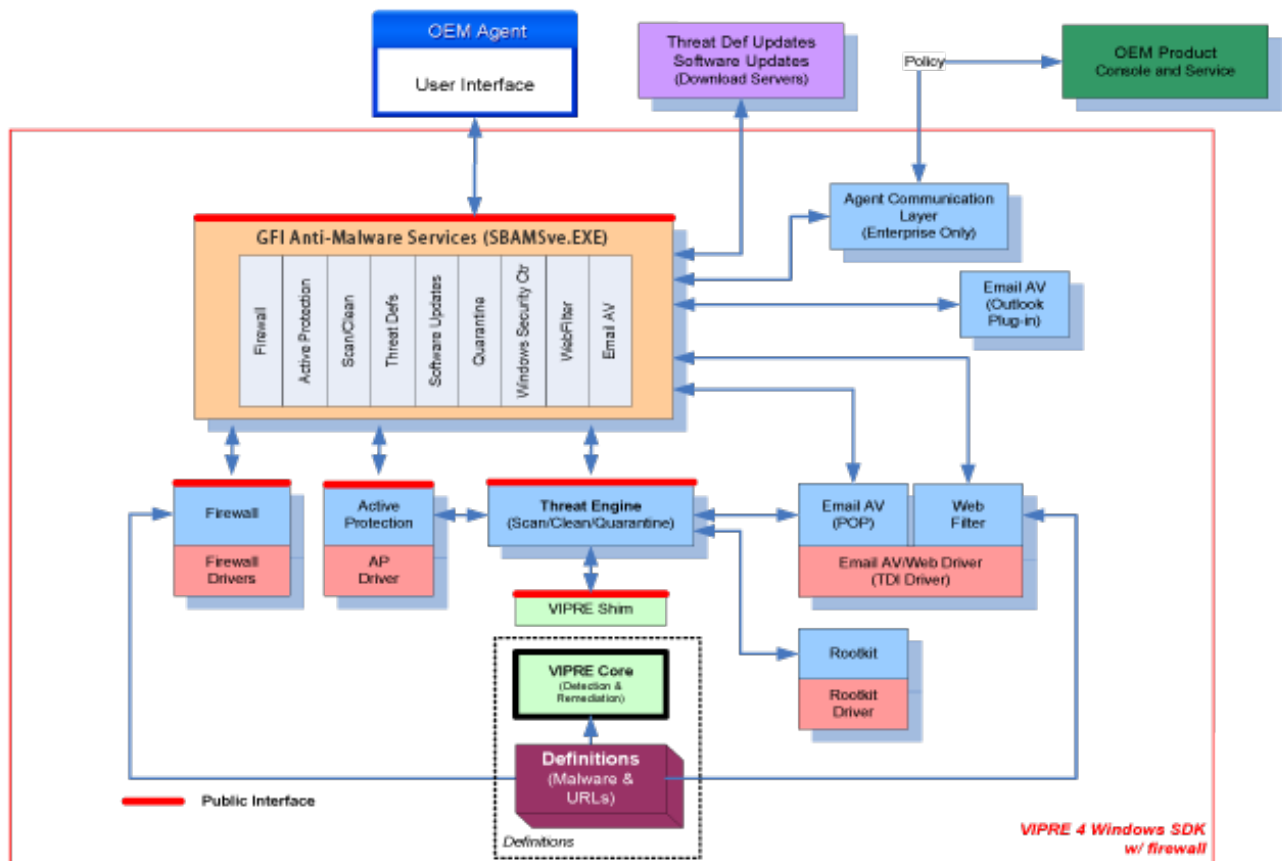
- Windows 2000 SP4 RollUp 1
- Windows XP 32bit
- Windows XP 64bit
- Windows Vista 32bit
- Windows Vista 64bit
- Windows 7 32bit
- Windows 7 64bit
- Windows Server 2003 32bit
- Windows Server 2003 64bit
- Windows Server 2008 32bit
- Windows Server 2008 64bit

**VIPRE Architecture**

The VIPRE SDK is comprised of the following components:

- **Core SDK**
  - o Detection and Remediation
  - o Threat Engine Shim
  - o Definitions (Core Updates, URLs, Malware)
- **Threat Engine SDK**
  - o Scan, Clean, Quarantine
  - o Rootkit Detection Driver

- **Service SDK (COM Interface)**
  - o VIPRE Public Interfaces
    - Scan and Clean
    - Software Updates
    - Quarantine
    - Active Protection (AP)
  - o Email Plug-in (MAPI, IMAP, POP, SMTP)
- **Firewall SDK**
  - o Host IPS Driver
  - o IM Driver
  - o Firewall Driver
  - o Email Driver
  - o Web Filter



## Endless Possibilities: Placing the Protection Where It Matters

With malware and other malicious activity becoming quite sophisticated and the perimeters surrounding our information systems and data dissolving, we are seeing a trend where malware protection is being placed not just at the system levels of the gateway, server, and endpoint, but also at the web application layer, often embedded directly within the application. This is especially true in the instances where the systems, applications, and data are hosted and managed by 3rd-party service providers where traditional perimeter protections may not be enough in the eyes of the consumer using the service.

A cloud-based file storage and collaboration service with anti-malware technologies directly built in to them would be one example of enabling an organization to place the desired anti-malware protections as close as possible to the points where it matters most – right where the data is uploaded, stored, accessed, and manipulated.

## In Closing: It's About the Partnership

The decision to integrate malware protection into your product offerings is not one that can be taken lightly. When taking steps to integrate malware protection into your offering, it is critical that the best technology be coupled with top-notch service and support. The right partner can make or break your success. Choose wisely to ensure you get the most out of your integration, delivering the best possible protection-enabled solution to your customers.

**Start Now: Begin using VIPRE, the award-winning antivirus SDK that has been designed and built from the ground up to be easily integrated into enterprise and consumer offerings, delivering best-of-breed protection supported by a best-in-industry team.**

## About GFI Software | Advanced Technology Group

GFI's Advanced Technology Group (ATG) is a leading provider of critical security software and services to enterprises needing specialized tools for threat analysis and defense. ATG leverages the research and technology of GFI Labs, the engine behind our award-winning security products such as VIPRE. The tools and data produced by our research are used by many of the Global2000, as well as leading web portals, telecoms and government defense agencies around the world. Consumer and Enterprise software and appliance vendors count on our VIPRE technology as their front line of protection against malware.

### More information please contact the GFI Advanced Technology Group at:

Web: [www.gfi.com/ATG](http://www.gfi.com/ATG) | Email: [atg@gfi.com](mailto:atg@gfi.com)  
Telephone (U.S. and Canada): 888-688-8457 ext.650  
Telephone (International): (01)727-562-0101 ext.650

## Appendix A | Product Comparison

This is a comparison matrix of VIPRE Antivirus Business Premium with several other popular antivirus products on the market. The side-by-side comparison provides a quick synopsis into the key features and advantages on how VIPRE matches up against other offerings.

	AV Software					
	Vipre Premium 4.0	Kaspersky Internet Security 2011	McAfee Internet Security 2011	Norton Internet Security 2011	Trend Micro Internet Security 2011	Webroot Internet Security Essentials
<b>Licenses:</b>	Unlimited	3	3	3	3	3
<b>Antivirus &amp; Anti-Spyware</b>						
Detects Viruses, Worms, Trojans	✓	✓	✓	✓	✓	✓
Detects Spyware, Adware, Keyloggers	✓	✓	✓	✓	✓	✓
Anti-Phishing	✓	✓	✓	✓	✓	
Email Scanning (Malware Protection)	✓	✓	✓	✓	✓	✓
Rootkit Protection (Detection & Removal)	✓	✓	✓	✓	✓	✓
Real-time protection	✓	✓	✓	✓	✓	✓
Signature Detection	✓	✓	✓	✓	✓	✓
Unknown Malware Detection	✓	✓	✓	✓	✓	✓
“Next-Generation” Anti-Malware Technology	✓					
Dynamic Binary Translation	✓					
USB Scanning on insertion	✓	✓		✓		
First-Scan/Boot-scanner	✓					
Command-Line Scanner	✓	✓				
Scans compressed files	✓	✓	✓	✓	✓	✓
Detailed Virus information	✓		✓	✓		✓
Anti-Phishing	✓	✓	✓	✓	✓	
Blocks Unknown Application Activities	✓	✓	✓	✓	✓	✓
Key Logger Protection	✓	✓	✓	✓	✓	✓
<b>Firewall</b>						
IDS- Intrusion Detection Systems	✓	✓	✓	✓	✓	✓
HIPS- Host Intrusion Prevention	✓	✓	✓	✓		✓

System						
Web-Filtering	✓	✓	✓	✓	✓	✓
Bad website blocking	✓	✓	✓	✓	✓	
Ad blocking	✓	✓	✓	✓	✓	✓
Two-way protection	✓	✓	✓	✓	✓	✓
Boot-time protection	✓	✓	✓			
Network Activity Monitor	✓	✓		✓		✓
<b>Features</b>						
Automatic Updates	✓	✓	✓	✓	✓	✓
Reports & Logs	✓	✓	✓	✓	✓	✓
Threat Level / Outbreak Notice	✓			✓	✓	
Editable Whitelist/Always Allow	✓	✓		✓	✓	
MX-V Advanced Malware Behavior Analysis	✓					
<b>Compatibility</b>						
Windows 2000 SP4 RollUp 1	✓		✓			
Windows XP 32bit	✓	✓	✓	✓	✓	✓
Windows XP 64bit	✓	✓				
Vista 32bit	✓	✓	✓	✓	✓	✓
Vista 64bit	✓	✓	✓	✓	✓	✓
Windows 7 32bit	✓	✓	✓	✓	✓	✓
Windows 7 64bit	✓	✓	✓	✓	✓	✓
Windows Server 2003 32bit	✓					
Windows Server 2003 64bit	✓					
Windows Server 2008 32bit	✓					
Windows Server 2008 64bit	✓					
<b>Certifications</b>						
VB100	✓	✓	✓	✓		✓
West Coast Labs Checkmark	✓	✓	✓	✓	✓	✓
ICSA Labs	✓	✓	✓	✓		✓
OESIS OK Certified	✓	✓				✓
Intel Certified	✓	✓				✓
PC Security Labs	✓	✓			✓	
AV-Test	✓	✓		✓	✓	✓
<b>Technical Support</b>						
U.S. based Tech Support	✓	✓				✓
Phone Support	✓	✓	\$	✓	✓	✓
Email Support	✓	✓	✓	✓	✓	✓
Chat Support	✓	✓	✓	✓	✓	
User Forums	✓	✓	✓		✓	
FAQ/Knowledgebase	✓	✓	✓		✓	✓

## Awards and Certifications

