

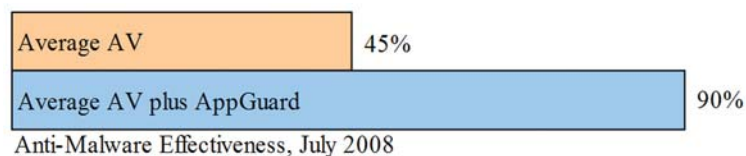


BLUE RIDGE/SECURE APPGUARD™

AppGuard supplements legacy anti-malware technologies by stopping the zero-day and re-crafted malware they miss. Unlike traditional solutions, such as HIPS, users are never required to make security decisions based on prompts from their security products. In addition to delivering transparent protection, AppGuard's small footprint and resource requirements has minimal impact on system performance and end-user productivity. The objective of AppGuard is to strike a balance between security and usability. Novice and power users should not be distracted by their security software.

Legacy Anti-Malware Products Are In-effective

- Typical PC defense inadequate¹
- Signature-based-only defenses ineffective²
- PCs have vulnerable applications (28%)³
- Users lack sophistication to effectively make knowledge-dependent security decisions

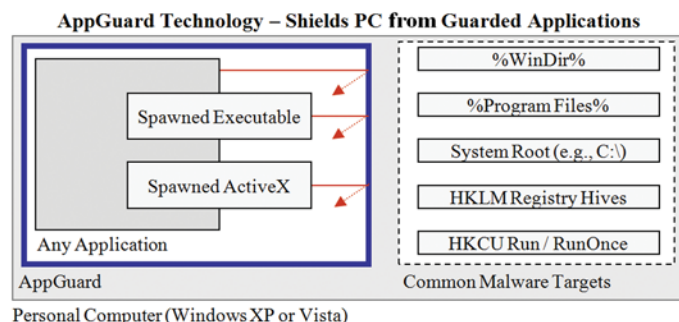


AppGuard Protects Endpoints and the User Experience

- Stops malware that typical PC defenses miss
- Nullifies ActiveX vulnerabilities
- Protects without signatures
- Suppresses drive-by downloads
- Blocks USB malware launches
- Reduces risks from PCs run in admin mode
- Designed to support novice users
- Protects without user-questions
- Generates no false positives
- Runs efficiently, occupies small footprint
- Allows applications to run normally

How Does AppGuard Work?

AppGuard prevents alterations to critical system resources, such as registries, that are common malware targets. For instance, when an application is attacked, the AppGuard blocks the actions necessary for the attackers to achieve their goals. In addition, AppGuard dynamically guards any ActiveX control or executable spawned by the guarded application. The thick-lined box surrounding the example application illustrates the technology in action.



1. Cyveillance Inc. reported in August 2008 that typical AntiVirus defenses intercepted 34% - 55% of malware found active in July 2008.

2. Secunia reported in October 2008 that signature-based only defenses detected less than 5% of the zero-day malware test samples developed by Secunia

3. Secunia reported in May 2007 that 28% of all applications found on PCs are missing important security patches

Reduce Admin Rights Risks

When users run their PC with admin rights, the goals of the attackers are easier to achieve because the operating system does not restrict where these attacked applications can write in the PC. However, AppGuard blocks such actions, reducing the risks inherent from running PCs with admin rights. These blocks do not require users to answer questions about whether to allow an action to proceed. AppGuard was designed so users would not have to make knowledge-dependent security decisions.

Suppresses Drive-By Downloads and USB Malware Launches

AppGuard intercepts operating system file system actions to decide whether they may proceed or not. This mechanism eliminates the ability to launch malware attacks from user space. It also prevents malware hidden within a USB thumbdrive from launching an attack on a PC. When users must run applications from a thumbdrive or from user-space, such as GotoMeeting.exe for a webinar, users can suspend blocking for a set time so they do not have to remember to re-enable blocking.

Comparing AppGuard

HIPS and Group Policy

AppGuard starts protecting endpoints out-of-the-box - unlike access control list (ACL) and discretionary ACL (DACL) mechanisms found in host intrusion prevention system (HIPS) products and operating systems. Implementing these products represents a monumental task, accounting for every possible permutation and exception to application behavior. These approaches are further complicated by applications that are not well behaved desktop applications. We have seen Microsoft Office 2003, Microsoft Office 2007, and IE7 requiring different access rights, and when running in admin mode, request full write access to system directories and HKLM hives. A simple ACL/DACL mechanism denies such privileges, crippling the applications. AppGuard lets the applications 'think' they have maximum system access, when in fact, they do not. This innovative approach provides maximum protection while allowing applications to operate normally and safely.

VISTA UAC

Vista users can disable user account control (UAC) without losing protection. Users that keep UAC on will

benefit from additional protections provided by AppGuard. For example, many well known products that extend Internet Explorer 7 functionality do so with ActiveX controls implemented in compatible mode. Even with UAC enabled, these ActiveX controls would be able to access any system directory or HKLM key. However, AppGuard blocks this access.

Example: A Zero-Day Attack

A user operating her PC with admin rights is lured to a website to download a fake AntiVirus tool. The user clicked on prompts within Internet Explorer 7, spawning a process called Secure2009[1].exe, which dynamically became a guarded application too. The AppGuard blocked the installation process, illustrated below on left. At the time of this attack, only 3 out of 36 AntiVirus products were able to detect this malware.



File: TotalSecure2009_2_exe received on 09.11.2008 07:44:00 (CET)
 Current status: finished
 Result: 3/36 (8.33%)

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.9.6.0	2008.09.11	-
AntiVir	7.8.1.28	2008.09.11	-
Authentium	5.1.0.4	2008.09.11	-
Avast	4.8.1195.0	2008.09.10	-
AVG	8.0.0.161	2008.09.10	-
BitDefender	7.2	2008.09.11	-
CAT-QuickHeal	9.50	2008.09.11	-
ClimAV	0.93.1	2008.09.11	-
DrWeb	4.44.0.09170	2008.09.11	-
eSafe	7.0.17.0	2008.09.10	-
eTrust-Vet	31.6.6083	2008.09.10	-
Ewido	4.0	2008.09.10	-
F-Prote	4.4.4.56	2008.09.10	-
F-Secure	8.0.14332.0	2008.09.11	-
Fortinet	3.113.0.0	2008.09.11	-
GData	19	2008.09.11	-