WHITE PAPER

AppGuard™

Technology Background

21 September 2009

Written by:
Fatih Comlekoglu
Tom Gilbert
Eirik Iverson

What is AppGuard™ Technology?

AppGuard Technology is client security software that blocks malware attacks, preventing harm when end-users:

- Browse Hacked/Malicious Websites
- Open Malicious Email Attachments
- Insert Infected USB Drives
- Open Tainted Documents (pdf, xls, doc, etc.)
- Played Spiked Multimedia Files (jpg, avi, wmv, etc.)
- Run UnPatched Software

AppGuard Technology employs a different approach from that of legacy defenses, which rely on signatures to identify incoming malware. In principle, this signature-based approach does not trust the practically infinite variety of files and communications of a computer. AppGuard Technology, on the other hand, does not trust the applications that process these files and communications. It blocks write operations by these applications to system and application resources as wells as prevents unknown applications from launching from user-space or USB drives.

Further, AppGuard Technology differs from other technologies that counter zero-day malware attacks, which rely on heuristics, protocol filtering, and extensive rule-sets. Instead, users merely need to identify any applications by name that are not already guarded by default. Careful attention has been devoted to striking a balance between usability and security.

AppGuard Technology is found in Blue Ridge / Secure AppGuard, Blue Ridge / Secure AppGuard Enterprise, and Blue Ridge / Secure EdgeGuard™. Adding either to a computer with any generic signature-based software, would on average triple its effective protection to over 90% of 'current' malware attacks. Operationally, AppGuard and EdgeGuard require less effort to configure and maintain than the legacy tools they complement.

Today's Malware is Too Agile for Legacy Security Software Alone

The prospect for signature-based defenses alone protecting computers is literally hopeless. Signature-based tools can only intercept malware that has been previously identified. But hackers can re-craft a malware sample into dozens of mutations in less than a minute. These mutations (i.e., different signatures) elude these defenses. AV vendors typically take at a month to discover, develop, and distribute a new signature for new malware. Long before then, however, malware makers abandon over half of their recently created binaries within 48 hours, pressing their advantage over the signature-based vendors.

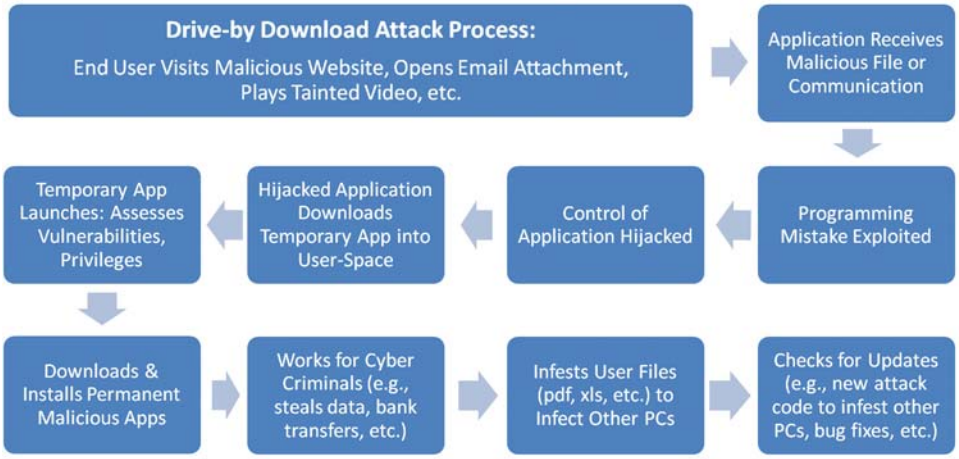
A recent study by Cyveillance measured the effectiveness of leading signature-based tools on malware that was found in the wild between May 12 and June 10, 2009, excluding all previous malware. This provides a more realistic evaluation than other methodologies that include the millions of historic samples rarely found in the wild but for which signatures have long existed. Cyveillance found that on average leading signature-based defenses stops 29% of 'current' malware. A year ago, this figure was 45%. The dramatic one year drop is due to a higher percentage of malware-makers using malware mass production tools as well as changing their attack code every 48 hours each to avoid discovery. Malicious web servers leverage such tools to alter their outbound malware every 10 minutes. Signature-based technologies cannot keep up.

> **Tested Anti-Virus/Spyware Missed 71% of Malware**
>
> Cyveillance, June 2009

Malware Preys on the Mistakes of Software Application Developers

Over 90% of malware attacks target software applications rather than the operating system. These attacks are made possible by programming flaws in the applications themselves, supporting library components, or helper applications. These mistakes enable attackers to coerce the object that processes their file, communication, or other object into harming the PC. These malicious objects reach their target via malicious/compromised websites, email attachments, USB thumb drives, and countless other delivery vehicles.

An application hijacked in this manner most often downloads an executable from the Internet, places it in user-space, and launches it. This executable is usually temporary. It assesses its environment, determines the best course of action, downloads the appropriate payload, and launches it. If the attack cannot root itself deep into the operating system to plant a nearly invisible full-time malicious executable, it systematically selects the next best thing.


Drive-by Download Attack Process:
End User Visits Malicious Website, Opens Email Attachment, Plays Tainted Video, etc.
Application Receives Malicious File or Communication
Programming Mistake Exploited
Control of Application Hijacked
Hijacked Application Downloads Temporary App into User-Space
Temporary App Launches: Assesses Vulnerabilities, Privileges
Downloads & Installs Permanent Malicious Apps
Works for Cyber Criminals (e.g., steals data, bank transfers, etc.)
Infests User Files (pdf, xls, etc.) to Infect Other PCs
Checks for Updates (e.g., new attack code to infest other PCs, bug fixes, etc.)

Computers run by an end-user logged in with a limited user account (LUA) are not immune to persistent (i.e., launches with Windows automatically) malware infestations. LUA does, however, make it considerably more difficult to root malware deep into the operating system, which would require an escalation attack, something this staged infestation process also can conduct.

Some application hijacking does NOT employ an intermediary executable but instead coerces the hijacked application to directly implant the permanent malware.

Once implanted, malware can update itself, and of course steal data and serve in a Botnet. Additionally, more and more malware will embed or corrupt files, documents, and USB thumb drives so that other computers may become infected. Months after infection, the malware may download something that enables it to embed or corrupt a certain file or document type. The malware maker relies on the familiarity of friends, families, and peers, who are likely to open these files or documents received from this machine/user.

History: Blue Ridge Endpoint Security Evolution Over a Decade

Several years ago, Blue Ridge Networks began development of EdgeGuard™, an enterprise scale endpoint policy enforcement product for Windows platforms. Blue Ridge had over a decade of experience developing and supporting VPN remote access solutions and knew that mobile devices were the next battlefield for enterprise security. Strong authentication and a well designed VPN would be useless to our customers if the mobile endpoints were loosely configured or subject to the operating whims of an end-user. In fact, our first customer for our newly developed Windows 95 VPN client showed us in 1997 how they could hack into the Windows system from the public network and access the corporate network through the VPN tunnel.

Before the end of 1997, we had delivered a policy enforcement product that worked independently of our VPN client and closed the vulnerability the customer had demonstrated. If our VPN packet guard became disabled, the VPN tunnel would not establish. The experience focused us on the importance of controlling the endpoint as well as preventing the end-user from bypassing enterprise policies.

EdgeGuard is designed to solve difficult problems for endpoint security. Most of our R&D has revolved around secure mobile computing. We wanted EdgeGuard to provide iron-clad policy enforcement on mobile platforms attached to hostile networks and with administratively privileged end-users. The effectiveness of leading security products degrades in these situations, particularly the latter.

EdgeGuard includes innovative self-protection features that resist the best efforts of a local admin to bypass policy. It also effectively prevents malware running in admin context from damaging our subsystem. Blue Ridge found that the EdgeGuard self-protection technology could readily block a large percentage of malware attack vectors, including self-mutating and other zero-day malware that eludes signature-based security software.

Blue Ridge also found other EdgeGuard features designed to lock-down endpoints further contributed to blocking major malware attack vectors. The EdgeGuard mechanism designed to render USB devices read-only, inaccessible, or unrestricted could also be used to block the most sophisticated USB malware attacks, which account for over 10% of all successful infestations. This could even stop the socially engineered attack where an end-user was tricked into clicking an executable on a USB device.

Similarly, another EdgeGuard feature for locking down an endpoint that renders file directories read-only, inaccessible, or unrestricted, regardless of end-user privileges, could be used to block yet another common attack vector: drive-by download attacks. A drive-by download attack is made possible by a flaw in an application that allows the attacker to 'drop' a standalone executable into user-space (e.g., 'My Documents') where it can launch and unleash its payload.

Risk Prioritization and Usability

AppGuard Technology is an illustration of setting security priorities, including usability. It's not designed to stop every possible attack vector. Diminishing returns for the rare attack vectors, less than 10% of malware samples, typically translate into enormous operational costs for administrators and productivity hits on confused and bewildered end-users.

In over a decade of building security solutions for the world's most security conscious organizations, Blue Ridge has learned that complexity itself is a security risk. Complex security systems are generally under-utilized, providing substantially less risk mitigation than their owners realize. This phenomenon is manifest in the heavy security suites offered by large endpoint security vendors. The host intrusion prevention system (HIPS) features included in these suites are typically disabled completely or drastically under-utilized.

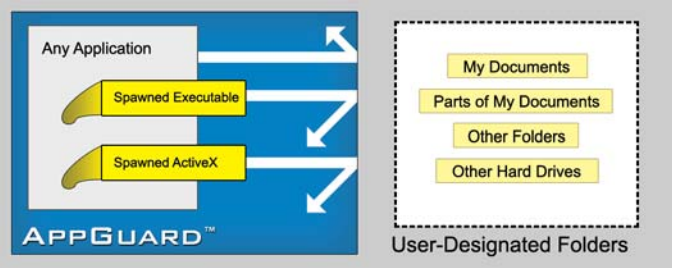
Consequently, Blue Ridge factored end-user and administrator usability into every design decision for AppGuard Technology. The resulting AppGuard and EdgeGuard security software solutions protect computers from over 90% of malware threats at 10% the effort of HIPS products. They do not ask end-users to make security decisions or read numerous technical prompts because end-users are ill-prepare and uninterested in making informed security decisions. Further, AppGuard and EdgeGuard endpoint protection consume extremely little CPU.

How does AppGuard Technology Protect Endpoints?

Any computer application has one or more programming flaws in it that could enable an attacker to implant malware. AppGuard Technology guards at-risk computer applications, preventing them from writing to critical system resources such as Windows directories, Program Files, HKLM registry hives, and select HKCU keys (e.g., Run, RunOnce).

Consider a scenario where AppGuard Technology is guarding Microsoft Office and Internet Explorer. An end-user clicks on a spam E-mail that launches Internet Explorer to a malicious Web site. The website exploits a flaw in an ActiveX control. Because AppGuard Technology dynamically guards any executable or ActiveX control spawned by a guarded application, AppGuard Technology prevents the flawed ActiveX control from placing a rootkit into the System32 directory.

AppGuard Technology - Sheilds PC from Guarded Applications



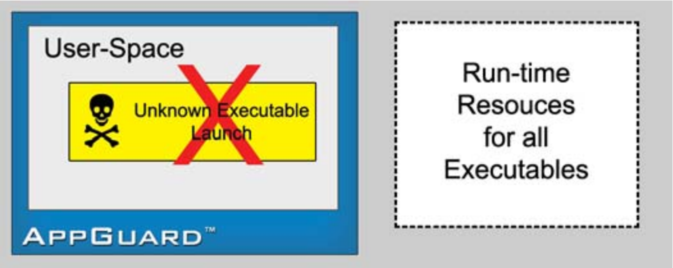
Personal Computer (XP or Vista)

Afterwards, when the end-user runs Internet Explorer to remotely access the home office via an SSL VPN gateway that utilizes an ActiveX control, AppGuard Technology does nothing to inhibit its normal operation. Note, the ActiveX control in this example was not located in user-space (i.e., Documents and Settings\user_login).

AppGuard Technology uses kernel and user level protections to intercept the relevant file system actions of every guarded executable and either allows or blocks them. The same applies to any process, including ActiveX controls, spawned by a guarded application.

Blue Ridge recommends using AppGuard technology to guard cmd.exe (e.g., .bat files), regsvr32.exe, and rundll32.exe. Attackers cannot use these Windows facilities to harm the PC. However, this protection must be suspended for legitimate uses, such as software installations/updates.

Next, an end-user runs a malicious video file that exploits a flaw in Windows Media Player to 'drop' an executable somewhere in user-space such as 'My Documents'. This executable, because of its location, is not allowed to launch, no matter how it's triggered. It cannot launch even when the end-user carelessly double-clicks on it in Windows Explorer.


User-Space
Unknown Executable Launch
Run-time Resouces for all Executables
APPGUARD™

Windows XP SP2 thru Windows 7

AppGuard Technology intercepts file system actions originating from user-space and blocks all executable launches, except for those explicitly guarded. For example, if Internet Explorer launched GotoMeeting.exe, which was placed on the 'Desktop', GotoMeeting.exe would not launch at all. However, if GotoMeeting.exe was 'guarded', then it could launch. As a 'guarded' executable, GotoMeeting.exe can run normally but it cannot implant malware.

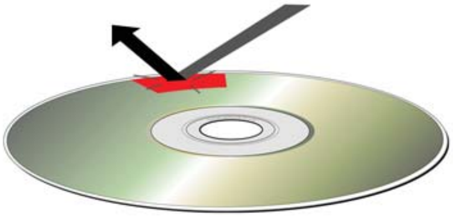
Afterwards, the end-users friend drops by with a USB thumb drive that contains another version of the video that he hopes will play on this laptop. Unknown to either, the other friend's machine was successfully infected. The implanted malware places attack code onto every USB drive inserted into it that automatically launches when inserted into another machine.

All Executable Launches are Suppressed, whether Auto-Run or Manually Launched by End-user

However, when the infected USB thumb drive is inserted, the attacking executable is not allowed to launch. Even when the end-user double clicks on it, nothing happens. AppGuard Technology blocks USB malware attacks by intercepting all file system actions originating from USB devices and either allowing or blocking them.

The most recently added AppGuard Technology protection is called MBRguard™, which blocks all write operations (e.g., Direct Kernel Object Hooking, IRP hooks, and more) to the master boot record (MBR) on the system drive (i.e., the hard drive with the Windows operating system). Malware such as 'KillDisk', Mebroot, Rustock.C, and other MBR-targeting malware are blocked without fan fare.

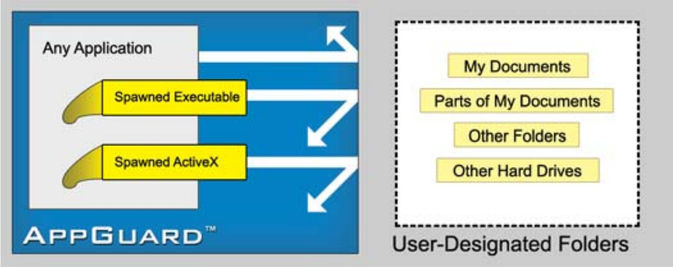
Blocks All MBR Write Operations



PC 'System' Hard Drive

How AppGuard Technology Plugs Malware-Caused Data Leaks

The protections discussed thus far contribute to data leak prevention by preventing malware from executing. However, a hijacked application can also be coerced to steal, delete, or ransom (i.e., encrypt) valuable user files. AppGuard Technology, guards web browsers in "privacy mode", by default. Web browsers are most at risk. Users can choose to do so for other applications as well. An application "guarded in privacy mode" cannot access designated directories without the end-user first suspending "privacy mode" for that application.

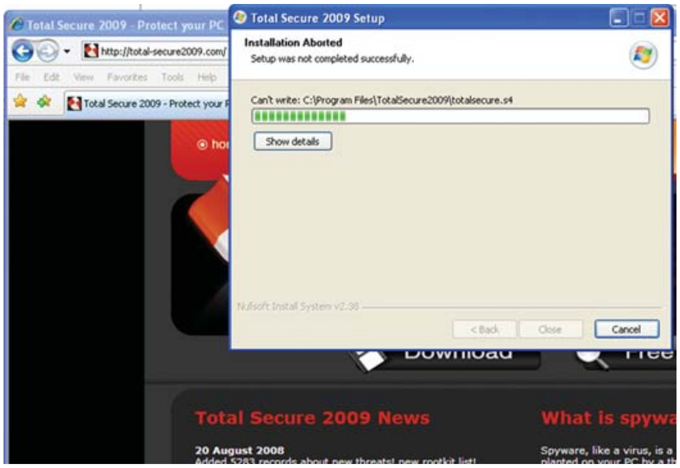


Personal Computer (Windows XP or Vista)

End-users conveniently suspend "privacy mode" for a specific application via a tray icon. Like all suspended protections, should the end-user forget to re-enable a protection, AppGuard Technology does so automatically (after 10 minutes by default).

Zero-Day Malware Example: Fake Antivirus Software

A local administrative user was lured to a Web site to download fake Antivirus software.



Total Secure 2009 Setup

Installation Aborted

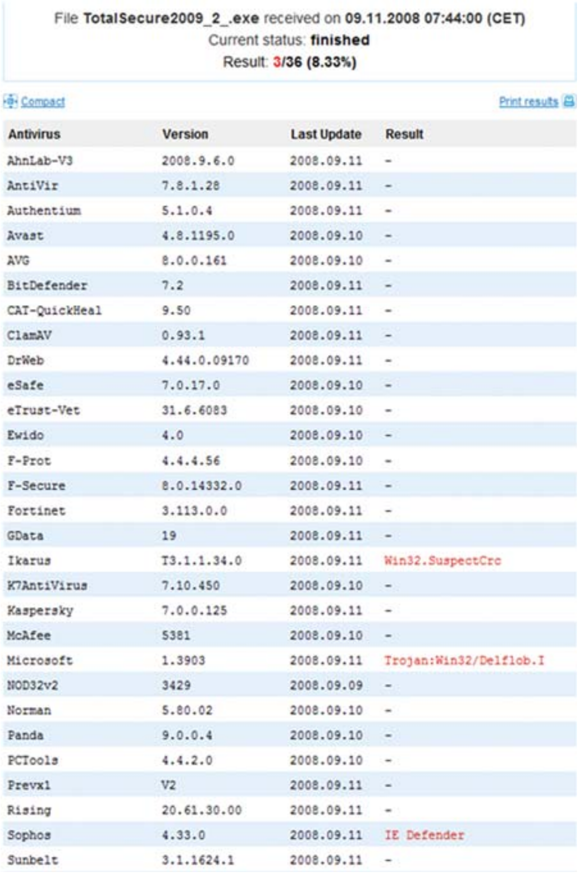
Setup was not completed successfully.

Can't write: C:\Program Files\TotalSecure2009\totalsecure.s4

Total Secure 2009 - Protect your PC
http://total-secure2009.com/
File Edit View Favorites Tools Help
Total Secure 2009 - Protect your P
Show details
Nullsoft Install System v2.38
< Back
Close
Cancel
Download
Free
Total Secure 2009 News
20 August 2008
Added 5283 records about new threats! new rootkit list!
What is spywa
Spyware, like a virus, is a
planted on your PC by a th

In this example, the end-user is lured to click on a fake Antivirus tool, which actually implants malware into the PC. Even though the user has local admin rights, the installation is blocked. The descendent processes (Total Secure2009[1].exe) of the AppGuard Technology protected IE7 process is also dynamically added to AppGuard Technology protection.

As shown in the following table, at the time, only 3 out of 36 AntiVirus products were able to detect the malware.



File **TotalSecure2009_2_.exe** received on **09.11.2008 07:44:00 (CET)**
Current status: **finished**
Result: **3/36 (8.33%)**

Compact
Print results

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	-
ClamAV	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-Prot	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	-
Ikarus	T3.1.1.34.0	2008.09.11	Win32.SuspectCrc
K7AntiVirus	7.10.450	2008.09.10	-
Kaspersky	7.0.0.125	2008.09.11	-
McAfee	5381	2008.09.10	-
Microsoft	1.3903	2008.09.11	Trojan:Win32/Delflob.I
NOD32v2	3429	2008.09.09	-
Norman	5.80.02	2008.09.10	-
Panda	9.0.0.4	2008.09.10	-
PCTools	4.4.2.0	2008.09.10	-
Prevx1	V2	2008.09.11	-
Rising	20.61.30.00	2008.09.11	-
Sophos	4.33.0	2008.09.11	IE Defender
Sunbelt	3.1.1624.1	2008.09.11	-

Consider the Windows Media Player example earlier, AppGuard Technology did not prevent the vulnerability from being exploited in memory. Instead, it prevented that attack from successfully creating a persistent foothold in the computer. Simply restarting Windows Media Player restores it to its pre-attack state.

To prevent the Windows Media Player vulnerability from being exploited at all would require a mechanism to intercept every API call, every interaction with another process, and every communication payload.

Attempting to regulate these actions is where HIPS products do far more harm than good. The idiosyncrasies of these interactions vary per application, change with each update or patch to the application, and alter with the presence of other applications and processes on the host. The resulting complexity and uncertainty requires HIPS products to guess as to what is a normal. Unless explicitly turned off, HIPS products include end-users in the guess-work, presenting them with highly technical 'do you want to allow this' questions.

To spare end-users, HIPS administrators must devote considerable effort to fine-tune the HIPS to these application idiosyncrasies and tune-out the mountains of false positives generated. With every application update and patch, however, administrators must re-tune.

HIPS vendors try to simplify this by providing default settings for the operating system and some of the applications typically found. However, HIPS products are considerably less effective with default settings than with finely tuned settings by a professional.

HIPS vendors introduced low, medium, and high operating modes to simplify usability. The high mode is typically very disruptive to the end-user, who is inundated with questions and cryptic event messages. Most deployments utilize medium or low. However, these modes are considerably less effective at stopping zero-day attacks than the high mode. This distinction is seldom reported.

The HIPS concept failed because of a fundamental lack of prioritization and upfront focus on usability.

Comparing AppGuard Technology with ACLs

On the surface, AppGuard Technology looks similar to access control list (ACL) or discreationary access control list (DACL) technologies found in many HIPS products and in operating systems. This perception is false for two reasons.

First, ACL/DACL per application is not practical. Creating ACL/DACL rules per application is a monumental task. The idiosyncrasies of each application, plus those from other applications on the host, require a myriad of exception rules to allow normal application use. This requires thorough use-case testing of each application to identify each exception rule.

Second, the static nature of ACL/DACL rules make them interolerant of applications that fail to conform to operating system best practices. For example, Microsoft Office, Internet Explorer 7, and Quicktime Player demand full write access to system directories and HKLM hives when running under administrative privilege. A simiple ACL/DACL mechamism that denies such privileges cripples these applications.

AppGuard Technology, however, fools such as applications into believing they have these privileges when in fact they do not. This innovative approach resolves all the incompabitibilty issues we have seen with legacy ACL/DACL approaches.

Comparing AppGuard Technology with Virtualization

AppGuard Technology is not a virtualization mechanism, or a sandbox. Additional abstractions and/or clones of resources (e.g., files, directories, APIs, etc.) are generated in virtualization/sandbox environments. This is done to protect the real resources of the host from harm. Unfortunately, this confuses users and applications. AppGuard Technology simply protects the critical host resources from the primary source of risk: applications with programming flaws exposed to external influences (e.g., documents, communications, etc.). Consequently, its focused, prioritized approach results in an extremely low CPU utilization.

Does AppGuard Technology Replace Anti-Virus/Spyware Products?

Yes. However, Blue Ridge has delivered high-end security solutions for over a decade. Philosophically, we advocate defense in-depth, or layered defenses. Consequently, we recommend that customers supplement a anti-virus/spyware product with an AppGuard Technology product. Anti-virus/spyware products excel at stopping malware over a month old. AppGuard Technology stops what it misses. Then again, it stops the old malware too.

Conclusion

AppGuard Technology is unique in its approach to deterring zero-day malware. It represents a prioritized defense with a focus on usability. End-users are not asked to make security decisions.

Blue Ridge / Secure AppGuard, Blue Ridge / Secure AppGuard Enterprise and Blue Ridge / Secure EdgeGuard complement existing security solutions by boosting overall protection to over 90% from today's and tomorrow's malware. Organizations can literally downgrade their signature-based protection to generic products to lower costs without sacrificing protection.

	AppGuard	AppGuard Enterprise	Managed EdgeGuard	EdgeGuard
Protection Against				
Vulnerable Software Applications	✓	✓	✓	✓
Infected USB Devices	✓	✓	✓	✓
Drive-by Download Attacks	✓	✓	✓	✓
Set-Up Protection in Minutes	✓	✓	✓	✓
Control				
User-Space White List Application Control	✓	✓	✓	✓
All Policies Supersede User Admin Rights		✓	✓	✓
Application Control (system-wide)			✓	✓
USB Drive Read/Write Control		✓	✓	✓
Assess/Remediate 3rd Party Security • Software • AntiVirus • Anti-Spyware • Personal Firewall • Disk Encryption			✓	✓
Assess/Remediate Microsoft Patches			✓	✓
Assess/Remediate PC Configuration Settings			✓	✓
Lock / Update 3rd Party Software Preference Files			✓	✓
Self-Quarantine of Non-Compliant PC			✓	✓
Network Access Protection (NAP): Policy Driven Trigger of Network-based Quarantine			✓	✓
Location Aware Policies			✓	✓
Custom Script (Assess or Modify PC)			✓	✓
Audit				
Protection Event Logs	✓	✓	✓	✓
Policy Event Logs	✓	✓	✓	✓
Audit, Compliance, and Remediation Event Logs			✓	✓
Central Management				
Centralized Policy Management		✓	✓	✓
Secure, Automated, Remote Agent Policy Updates		✓	✓	✓
Secure, Automated, Remote Agent Software Updates		✓	✓	✓
Centralized Event Database		✓	✓	✓
Managed Security Service			✓	