



# BLUE RIDGE/SECURE APPGUARD™ ENTERPRISE

## Stops the NEW Malware that Eludes Traditional Security Products

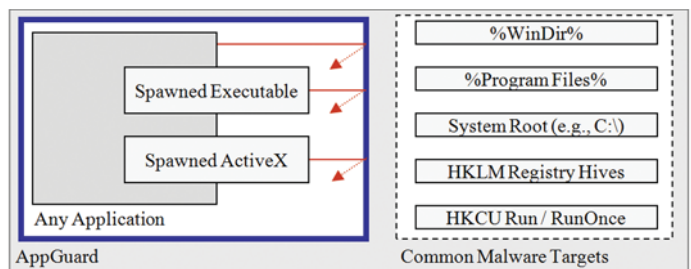
Traditional anti-virus/spyware products rely on signatures to protect computers from malware attacks. The creation of NEW signatures typically takes weeks to months from initial discovery to distribution. Cyber-criminals, however, require minutes to re-craft old malware such that it's unrecognizable to signature-based anti-virus/spyware security software, which excel at stopping OLD malware. Computers are exposed to OLD and NEW malware everyday. Consequently, anti-virus/spyware security software has been measured to stop only 45% of current malware in the wild. Adding AppGuard boosts protection to over 90%. AppGuard protection is realized for a fraction of the operational costs of alternatives.

## Stops NEW Malware using a Different Approach

The OLD way of protecting computers from malware attacks involves comparing an infinite variety of inbound files and communications to an exponentially growing 'most wanted' list. AppGuard Technology employs a far more practical approach involving three attack vectors.

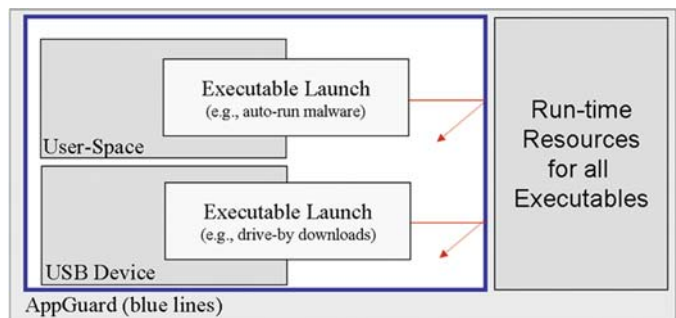
- Guards the applications that malware targets, preventing malware from coercing these applications into harming their computer
- Suppresses the launch of any unguarded or unknown executable from user-space (e.g., My Documents, Desktop, etc.), eliminating drive-by download attacks
- Prevents code execution from infected USB devices to prevent PC harm

AppGuard Technology - Shields PC from Guarded Applications



Personal Computer (Windows XP or Vista)

AppGuard USB and User-Space Executable Suppression



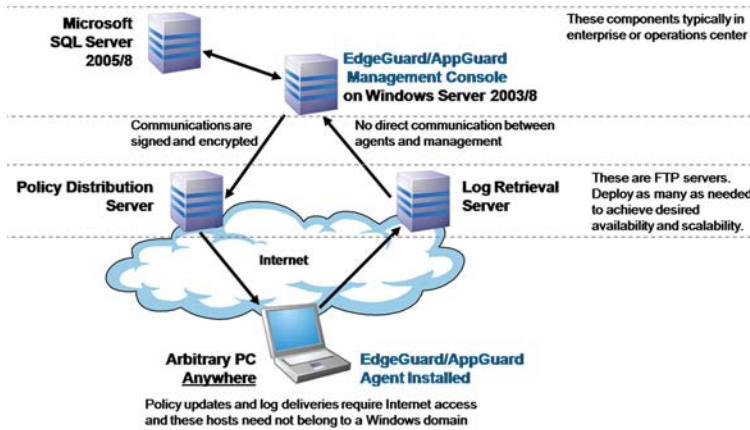
Windows XP SP2 - Vista SP1

## Protected Computers can Safely

- Browse Hacked Websites
- Open Malicious Email Attachments
- Insert Infected USB Drives
- Open Tainted Documents (pdf, xls, doc, etc.)
- Play Spiked Multimedia Files (jpg, avi, etc.)
- Use Software Requiring Security Patches

## AppGuard Enterprise Architecture

AppGuard Enterprise leverages the management technology infrastructure of our EdgeGuard product. Protection policies are centrally defined and pushed out through a PKI-based publication model that scales to support 100,000's of computers. Administrators can push out policy changes, upgrade agents, and pull logs from endpoints located anywhere as often as required, providing operational awareness and agility needed for tomorrow's threats.



## Organizational Flexibility

Administrators are provided a range of options and tools. They can choose to endow select groups of end-users with the discretion to suspend one or more protections as needed. Or, computer protections can be completely locked down, even to users with local admin rights. Similarly, the client graphical user interface can be hidden from users. With mobile users, administrators can implement protections that vary based on location.

## Local and Remote Computer Audit in Near Real-Time

Administrators have operational awareness over endpoints everywhere including activity spanning multiple malware attack vectors. Protection policies can be updated per insights gained from these audit reports. Risk assessments can be revised per actual AppGuard protection event data.

