WEBROOT
SecureAnywhere® Business Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection is an innovative, next-generation solution for preventing malware infections. Its unique, real-time, cloud-driven collective security intelligence is powered by the Webroot BrightCloud® Threat Intelligence Platform and is superbly effective at countering unknown malware. SecureAnywhere Business Endpoint Protection replaces outdated, less effective, reactive antivirus that needs constant updates and hogs system resources with an always up-to-date Smarter Cybersecurity™ solution that never slows users down and reduces operational overhead to almost zero.

CONVENTIONAL AV

There are almost 50 different vendors who offer cybersecurity solutions. Many still follow the conventional approach of requiring regular updates and using signature files to detect malware. They work at the point of detection, not the point of infection approach that Webroot SecureAnywhere Business Endpoint Protection uses.

Established	within the past ~20 years
Headquarters	US and Europe
Revenue	Varies
Company Status	Public/Private
No. of Employees	Varies
No. of Endpoint Customers	Varies

Deployment	Webroot	Average
Agent Deployment Size	<1MB	~300+ MB
Full Installation Time	5 seconds	~7 minutes
Full Installation Size	2 MB	1148 MB
Memory Used Initial Scan	13 MB	210 MB
Scheduled Scan Time	91 seconds	29+ minutes
Memory Usage - Idle	5.5 MB	137 MB
File Write, Open, Close	19.2 seconds	2 minutes

Positioning Webroot SecureAnywhere® Business Endpoint Protection	
Key Differentiators	**Supporting Messages**
Smallest Endpoint Security Client	Full installation software package is less than 1 MB in size.
	Lowest scanning RAM usage of any endpoint solution.
Fastest Scan Times Easy to Deploy, Configure and Use	Ultra-fast scan times, typically < 2 minutes. Doesn't slow user endpoints down or impede user productivity.
	Very fast and easy to deploy, typically ~2-3 minutes, including initial scan. Deployment Tool, MSI, Group Policy options
	No-conflict agent, compatible with existing antivirus software, no need to uninstall old software to trial or install Endpoint Protection.
	Easy-to-use cloud management console, no hardware/software required.
	Auto-updating software generates minimal network traffic – typically <250KB per day, per endpoint.
Powerful Threat Protection and Remediation	Real-time threat detection leverages behavior, file reputation, monitored execution, and BrightCloud platform to stop unknown threats.
	Complete system journaling provides ability to roll back systems to pre-infected state – saving time/cost of reimaging.
	Intelligent outbound firewall that uses BrightCloud intelligence to improve on user decisions and minimize interruptions
	Offline protection: local disk, USB, CD and DVD devices.

De-Positioning Conventional Endpoint Security	
Average Position	**Supporting Messages**
Strengths	Established reputation, better global branding than Webroot and more established with the Channel and in local markets
	Better detection test results
	Wider platform support, i.e., Linux
	Wider range of included security, i.e., encryption, DLP, web filtering, etc.

De-Positioning Conventional Endpoint Security (continued)

Average Position	Supporting Messages
Vulnerabilities	May test well for malware detection, but actual efficacy low, as is admins opinion
	High TCO, requires considerable management and operational time commitment so the true cost of ownership includes management server, updating, reimaging and help desk support.
	Endpoint security & productivity problems. Scans and updates are too resource intensive and cannot occur during normal working hours, if at all, and little or no individual protection against unknown malware, real-time interception is minimal compared to our solutions
Sales Tactics	Use the fact that we happily run alongside existing endpoint security to demonstrate install and initial scan times
	Show web portal and ease of management/reporting, plus integration with mobile. Show via portal the threats that others have recently missed
	Use our high customer satisfaction and NPS scores in conjunction with our testimonials on efficacy, cost of ownership etc. to support our being different and more effective
	Unlimited Trial: Offer instant free 30-day trial to run alongside existing antivirus so our capabilities shine through.

Features	Webroot	Conv. Sol.	Notes – How to Win
Deployment & Intallation			
Fast installation	Yes	No	Conventional antivirus is slow to install because of large clients, typically 100s of MB
Fast scheduled scanning	Yes	No	Scheduled scans sometimes take hours to run and hog resources
No-conflict compatibility with all software	Yes	No	SecureAnywhere Business Endpoint Protection runs alongside other antivirus, others can't
Minimal system resource usage - Memory, CPU & Disk	Yes	No	On every major performance benchmark, SecureAnywhere Business Endpoint Protection has minimal system impact
Support for Mac, PC, Server, VMware & Citrix	Yes	Partly	Some support more, some less. Only Webroot offers a single agent for ALL platforms
Threat Detection and Remediation			
Global security & threat intelligence network	Yes	Yes	Most vendors have some form of threat intelligence network, but few are real-time
Advanced zero-day/unknown malware detectio	Yes	Partly	None categorize into good/bad/undetermined like Webroot; only detect bad
Protection against viruses, Trojans, worms, spyware & rootkits	Yes	Yes	Other vendors offer protection of varying effectiveness
Advanced file pattern & behavior recognition technology	Yes	Yes	Most cybersecurity solutions now use file pattern & behavior recognition technology
Adjustable heuristics for Age, Popularity, Uniqueness	Yes	Partly	Most solutions lack tailored settings for their heuristics, so are not as flexible or powerful
Intelligent cloud-based outbound firewall	Yes	Partly	Most solutions offer a firewall, but few are totally automated or as intelligent at filtering traffic
Comprehensive range of System Protection shields	Yes	Partly	Most solutions offer shields but only a few offer the wide range found with Webroot
Automatic journaling of unknown processes	Yes	No	Conventional solutions rarely offer built-in journaling, some offer a similar but external tool
Automatic malware remediation & removal	Yes	No	Conventional solutions do not offer full remediation and removal to uninfected state
Comprehensive application override controls	Yes	Partly	Conventional solutions offer some controls, but not the same flexibility and scope
Dwell Time	Yes	No	No conventional solution alerts or reports on infection dwell time
Web Browser Security			
Browser vulnerability protection	Yes	Yes	Conventional solutions do offer browser hardening and protection
Identity Shield, sensitive data safe-mode	Yes	Partly	Some offer web identity shields to protect sensitive browsing transactions
Real-Time Anti-Phishing protection	Yes	No	Conventional solutions offer phishing protection, but not real-time or as effective
Secure Web Gateway service option	Yes	Partly	Some conventional vendors offer web gateway solutions, too (Symantec, McAfee, Sophos etc.)
Management and Reporting			
Cloud-based management console	Yes	Partly	Some conventional vendors offer cloud-based mgmt consoles
Advanced management reporting & analytics	Yes	Partly	Some conventional vendors offer advanced reporting and analytics
Zero client/agent definition file updates	Yes	No	Conventional solutions need regular definition/signature updates, or else protection is compromised
Device policies for Network, Disk, USB, CD/DVD Usage	Yes	Yes	Most solutions offer some level of attached device control
System Cleaner & System Analyzer performance tools	Yes	No	Most solutions do NOT offer system analysis reporting and endpoint performance optimization controls
System viewer, control and file submission tools	Yes	Partly	Most solutions offer some type of file submission; many are complex and time consuming
Full range of remote endpoint Agent Commands	Yes	No	Outside of policy controls, most solutions do NOT offer a full range of remote commands via the agent

Key Conventional Solution Findings

Conventional solutions are easily overwhelmed by the vast amount of new malware (over 390,000 items per day) and the high degree of targeting that makes getting samples for signature updates very difficult

Conventional solution efficacy against malware is very poor (regardless of detection test results), meaning many organizations are adding second antimalware tools or looking for next-gen solutions like Webroot that stop malware at point of infection, or even before infection occurs

Notes and Comments

Webroot customer satisfaction statistics are some of the best in the cybersecurity industry

Extensive customer references are available to support the sales process as are customer testimonials

MSPs and Enterprises prefer Webroot for deployment, efficacy and lower operational costs, as well as granular visibility into individual endpoints

* PassMark Software, "Webroot SecureAnywhere® Business Endpoint Protection vs. Seven Competitors", (August 2015)