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 SecureAnywhere Business Endpoint Protection replaces outdated, less effective, reactive antivirus that needs constant updates and hogs system resources with an always up-to-date Smarter Cybersecurity™ solution that never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.

SOPHOS

Sophos entered the antivirus market in the 90s to diversify from the encryption market. They now offer a portfolio of software and appliances, including antivirus, encryption, email, web, NAC, and mobile security. Innovative technology, such as their Behavioral Genotype Protection and rapid signature updates, stop new and unknown malware.

Established	1985
Headquarters	Abingdon, UK
Revenue	FY14 $379MM
Company Status	Private
No. of Employees	2,000+
No. of Endpoint Customers	100M+ users in 150 countries

Deployment	Webroot	Sophos
Agent Deployment Size	<1MB	unknown
Full Installation Time	5 seconds	7 minutes
Full Installation Size	2 MB	2973 MB
Memory Used Initial Scan	13 MB	507 MB
Scheduled Scan Time	91 seconds	23 minutes
Memory Usage - Idle	5.5 MB	497.8 MB
File Write, Open, Close	19.2 seconds	49.1 seconds

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 Sophos Endpoint Security

Sophos Position	Supporting Messages
Strengths	Global Presence. Well-known brand in EMEA, less in US, often an alternative to Symantec/McAfee/Trend, primarily enterprise focused
	Offers highly focused range of endpoint protection & web, email, NAC, DLP, and encryption solutions, bundles with user pricing available
	Integrated admin console for single-pane-of-glass mgmt over a wide range of endpoint controls
	Support for Windows, Mac, Linux, Virtual machines

De-Positioning Sophos Endpoint Security (continued)

Sophos Position	Supporting Messages
Vulnerabilities	Antimalware performance and detection of hidden malware are below average
	Uses a lot of resources, may slow performance and impede productivity
	Not as well known as Webroot in the US. Smaller antivirus market share too, and are seen as traditional solution
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
	Unlimited Trial: Offer instant free 30-day trial to run alongside existing antivirus so our capabilities shine through.

Features	Webroot	Sophos	Notes – How to Win
Deployment & Intallation			
Fast installation	Yes	No	SP – 7 minutes vs. 5 seconds for SecureAnywhere Business Endpoint Protection
Fast scheduled scanning	Yes	No	SP – 23 minutes per scheduled scan vs. 91 seconds for Webroot
No-conflict compatibility with all software	Yes	No	SP – Installed security must be removed, Webroot needs no removal
Minimal system resource usage - Memory, CPU & Disk	Yes	No	SP – Massive PC resource usage and very slow compared to Webroot
Support for Mac, PC, Server, VMware & Citrix	Yes	Yes	SP – Wide Wintel support plus Hyper-V, Windows, Mac, Linux.
Threat Detection and Remediation			
Global security & threat intelligence network	Yes	Yes	SP – SophosLabs and Live Protection with Live antivirus, URL Filtering and Spam elements
Advanced zero-day/unknown malware detectio	Yes	Yes	SP – Cloud threat database and Live Protection, still poor stats against hidden malware
Protection against viruses, Trojans, worms, spyware & rootkits	Yes	Yes	SP – Scores highly against known malware. Has built-in HIPS and Live Protection
Advanced file pattern & behavior recognition technology	Yes	Partly	SP – Has disinfection tools but little else built into server-based console
Adjustable heuristics for Age, Popularity, Uniqueness	Yes	Partly	SP – Available, but unclear if they offer more than enable/disable
Intelligent cloud-based outbound firewall	Yes	Partly	SP – Some protection from reputation database but only against known malware
Comprehensive range of System Protection shields	Yes	Yes	SP – Two-way location aware firewall (on vs. off-network)
Automatic journaling of unknown processes	Yes	No	SP – No journaling
Automatic malware remediation & removal	Yes	No	SP – SMaRT process for remediation, which is really a quarantine/deletion method
Comprehensive application override controls	Yes	No	SP – Standard exclusion method with some options
Dwell Time	Yes	No	SP – Dwell time is not measured or reported
Web Browser Security			
Browser vulnerability protection	Yes	Yes	SP – Basic web filtering, less capable than SecureAnywhere Web Security Service
Identity Shield, sensitive data safe-mode	Yes	No	SP – Nothing in this area except their firewall
Real-Time Anti-Phishing protection	Yes	Yes	SP – Off-network roaming user support
Secure Web Gateway service option	Yes	Yes	SP – Built-in URL filtering, and application usage controls for IM and P2P
Management and Reporting			
Cloud-based management console	Yes	Partly	SP – Centralized console, offers cloud-based and on-premise
Advanced management reporting & analytics	Yes	No	SP – Requires an upgrade to endpoint client
Zero client/agent definition file updates	Yes	Yes	SP – Offers dashboard within Enterprise server
Device policies for Network, Disk, USB, CD/DVD Usage	Yes	Yes	SP – Same as Webroot, plus Bluetooth, Wi-Fi and monitoring/reporting on usage
System Cleaner & System Analyzer performance tools	Yes	Yes	SP – Offers this through its Enterprise Server
System viewer, control and file submission tools	Yes	No	SP – Does not offer technical tools apart from remediation
Full range of remote endpoint Agent Commands	Yes	No	SP – Standard command list, not as comprehensive as Webroot

Key Sophos Findings

Cloud-based mgmt console with limited functionality, does not include role-based administration, DLP, malicious traffic detection, integrated Android security, or mobile web filtering

No rollback remediation

Does not run alongside other security products

Still a traditional antivirus with heavy footprint and high scan times

Extensive OS coverage on mobile—Android, iOS, Windows, BlackBerry

Notes and Comments

Biggest weaknesses are poor on device performance and pretty average efficacy against all types of malware

SC Magazine notes Management console takes 45 minutes to install

Offers Endpoint bundle with Mobile

Gartner Magic Quadrant Leader in Endpoint, Niche or Visionary in Mobile depending on category—MDM or EMM

Email encryption included

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