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 SecureAnywhere Business Endpoint Protection replaces outdated, less effective, reactive antivirus that needs constant updates and hogs system resources with an always up-to-date Smarter Cybersecurity™ solution that never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

KASPERSKY lab

Kaspersky Lab offers antimalware, controls, encryption & mobile security, patch management & automatic vulnerability scanning, efficiency-boosting systems management functionality and security for email, internet gateway, virtualization & collaboration. They are ranked sixth in worldwide security software vendors. Kaspersky technology is licensed by ~120 global technology companies.

Established	1997
Headquarters	Moscow, Russia
Revenue	FY13 $672M
Company Status	Private
No. of Employees	3,000+
No. of Endpoint Customers	c.5.5% of global (OPSWAT, 1/14), >400M

Deployment	Webroot	Kaspersky
Agent Deployment Size	<1MB	500+ MB
Full Installation Time	5 seconds	270 seconds
Full Installation Size	2 MB	1563 MB
Memory Used Initial Scan	13 MB	188 MB
Scheduled Scan Time	91 seconds	~22 minutes
Memory Usage - Idle	5.5 MB	39.1 MB
File Write, Open, Close	19.2 seconds	~25 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 Kaspersky Endpoint Security

Average Position	Supporting Messages
Strengths	Brand Recognition. Global brand with strong presence in 200 countries across consumer and enterprise markets
	Has a highly focused range of endpoint protection and is favored by our target audience too. Also have strong strategic partnerships with many other security vendors. Windows, Mac & Linux security
	Consistently performs well in antimalware tests, regularly a top 3 performer. Gartner Magic Quadrant: Leaders

De-Positioning Kaspersky Endpoint Security (continued)

Average Position	Supporting Messages
Vulnerabilities	KL malware performance comes at a price. They are resource hogs and get in the users way
	Combines signature-based and cloud-assisted technology. KL is constantly looking to update itself and uses a lot of resources to do so, again slowing performance and getting in the way
	Hides complexity through automation, but remain complex if you want to change anything, and hackers heavily test against circumventing KL
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 and KL priced higher—nearly double for EP, $9/user for UP.
	Unlimited Trial: Offer instant free 30-day trial to run alongside existing antivirus so our capabilities shine through.

Features	Webroot	KL	Notes – How to Win
Deployment & Intallation			
Fast installation	Yes	No	KL – Over 50 times slower than SecureAnywhere Business Endpoint Protection
Fast scheduled scanning	Yes	No	KL – Averages ~22 minutes compared to Webroot (91 seconds)
No-conflict compatibility with all software	Yes	No	KL – Old security must be removed before installing
Minimal system resource usage - Memory, CPU & Disk	Yes	No	KL – Very heavy resource usage
Support for Mac, PC, Server, VMware & Citrix	Yes	Yes	KL – Wide Support: Windows, Linux, Mac, Android, iOS, Windows, Symbian, BlackBerry
Threat Detection and Remediation			
Global security & threat intelligence network	Yes	Yes	KL – Global Research and Analysis Team. Has strong reputation in threat intelligence
Advanced zero-day/unknown malware detectio	Yes	Yes	KL – Have high detection rates of zero-hour malware detection
Protection against viruses, Trojans, worms, spyware & rootkits	Yes	Yes	KL – One of the best traditional defenses against both known and unknown malware.
Advanced file pattern & behavior recognition technology	Yes	Yes	KL – Uses traditional signature-based as well as heuristics for recognition
Adjustable heuristics for Age, Popularity, Uniqueness	Yes	Partly	KL – Not really. Divided into Static and Dynamic scanning
Intelligent cloud-based outbound firewall	Yes	Partly	KL – Firewall, yes. Outbound, no. Adjustable incoming block capability though limited
Comprehensive range of System Protection shields	Yes	Partly	KL – Basic set of shields and not much mentioned in product support pages
Automatic journaling of unknown processes	Yes	Yes	KL – Offers rollback remediation. System Watcher logs system and resources
Automatic malware remediation & removal	Yes	Partly	KL – No remediation per se, but disinfection is top notch compared to other antivirus
Comprehensive application override controls	Yes	Yes	KL – Application control includes a fully categorized app DB and trusted sources of change
Dwell Time	Yes	No	TM – No dwell time reporting or measurement
Web Browser Security			
Browser vulnerability protection	Yes	Yes	KL – Offers basic web filtering, a lot less capable than SecureAnywhere Web Security Service
Identity Shield, sensitive data safe-mode	Yes	Partly	KL – Offers Safe Money feature for secure transactions
Real-Time Anti-Phishing protection	Yes	Yes	KL – Improved phishing capabilities
Secure Web Gateway service option	Yes	Yes	KL – Offers built-in URL filtering, up and download controls; very basic service
Management and Reporting			
Cloud-based management console	Yes	No	KL – Uses on-premise management PC as server
Advanced management reporting & analytics	Yes	Yes	KL – Available with update in 2014
Zero client/agent definition file updates	Yes	No	KL – Near real-time, Urgent Detection System database updated with newly discovered malware
Device policies for Network, Disk, USB, CD/DVD Usage	Yes	Yes	KL – Select product offers device lock
System Cleaner & System Analyzer performance tools	Yes	Partly	KL – Cleaning tools built in
System viewer, control and file submission tools	Yes	Partly	KL – Offers basic system monitoring and limited application controls
Full range of remote endpoint Agent Commands	Yes	No	KL – Very little information about remote agents except updating and reporting

Key Findings

- Well-known vendor that delivers some of the best traditional cybersecurity
- Kaspersky is very system resource intensive, has limited remediation
- Kaspersky is the 'geek favorite,' and consistently in top 3 for efficacy, but it's a resource hog and the poor device performance is noticeable
- Does not offer a cloud-based mgmt console

Notes and Comments

- Use Endpoint Security for Business Select rather than Endpoint Antivirus as the fairest like-for-like comparison
- New Business bundles Core, Select, Advanced and Complete are half way house to user protection and to compete with Sophos and others like Webroot
- Big drawback still is on device performance, which is very poor
- Select product excludes data encryption

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