WEBROOT
Smarter Cybersecurity™

BATTLE CARD

WEBROOT SecureAnywhere® Web Security Service

The Webroot SecureAnywhere® Web Security Service offers website access and content filtering controls, as well as advanced protection against web-based malware for both on and off-network users. As a 100% cloud-based service, there is no management hardware or software to maintain, resulting in a lower Total Cost of Ownership (TCO) than on-premise or hybrid secure web gateway solutions. Backed by the Webroot BrightCloud® Threat Intelligence Platform, the service delivers leading-edge industry components (licensed by 35+ vendors) including URL filtering, IP reputation, real-time anti-phishing, and zombie/botnet detection. This intelligent secure web gateway solution replaces on-premise alternatives and delivers powerful security, improved user productivity, and regulatory compliance to protect every users' online experience.

zscaler® Secure. Everywhere.

Zscaler entered the cloud (SaaS) secure web gateway market in 2008. They have invested resources in an architecture that disconnects policy administration, reporting, and enforcement, to let each scale independently. They offer APT, web, email, and mobile security.

Established	2008
Headquarters	San Jose, CA, USA
Revenue	Unknown
Company Status	Private
No. of Employees	1,500-1,600
No. of SaaS Customers	12M, c.5,000 enterprises

Deployment	Webroot	Zscaler
Availability	99.99% Uptime	Unknown
Antmalware	100% Known Malware	Unknown
Antisyware	100% Known Spyware	Unknown
Web Latency	Milliseconds	90% in <90 seconds
Policy Propagation	99.9% Updates within 5 mins	Within seconds

Positioning the Webroot SecureAnywhere® Web Security Service	
Key Differentiators	**Supporting Messages**
Desktop Web Proxy (DWP)	Easily deployed, lightweight, tamperproof agent, ensures transparent user authentication + automatic acct creation
	Seamless roaming user support, even over Wi-Fi hotspots
	Fully configurable through the mgmt console. Configure sites to bypass, PAC files, gateway caching proxies, etc.
	Persistent cookie alternative for non-managed devices
Ease of Deployment, Configuration & Use	Preconfigured multi-choice policies and group settings to help configure user accounts quickly and easily
	Intuitive policy interface without complex policy interactions
	Optimized performance with split tunneling, global load balancing, auto compression, and option to strip ads/pictures
Threat Protection	Cloud sandbox with antimalware and antispyware protection
	Signature-less heuristic protection for JavaScript, Shellcode, XSS, and phishing attacks
	Detects anonymous proxies and applies appropriate policies, even for obfuscated URLs. No service bypass, DWP locking
	Real-Time Anti-Phishing uncovers phishing sites 3-5 days before the other solutions, counters no. 1 web threat

De-Positioning Zscaler	
Average Position	**Supporting Messages**
Strengths	Global Data Centers: Over 100 distributed data centers allow for private node / private cloud deployments
	Web 2.0 Features: Social media, P2P, and IM controls (but IM & P2P are on par with, not better, than Webroot)
	Gartner Leader: Ranked well with Gartner, but real substance behind many of their capabilities is dubious/untested

De-Positioning Zscaler (continued)

Average Position	Supporting Messages
Vulnerabilities	Mobile User Support: Uses a PAC file with no lockdown, creating major security & policy enforcement issues for customers. No dynamic hotspot management
	Lack of Info: No SLAs and little efficacy testing to support their claims
	Poor File Type Controls: Only scans MS Office, PDFs and ZIP files
Sales Tactics	Cost: APT and NanoLog come at an extra cost, so what are customers buying?
	Superior URL Filtering/Anti-phishing: Webroot BrightCloud URL filtering and anti-phishing is more accurate, Zscaler uses unknown tech
	No Endpoint Protection: Zscaler only offers cloud layer security, nothing for devices. Webroot offers both
	Trial: Offer free trial to let our capabilities shine through

Features	Webroot	Zscaler	Notes – How to Win
Roaming User Support			
Roaming User Authentication without Server/Key Mgmt	Yes	Yes	ZS – Easily bypassed, not tamperproof
Automatic Hotspot Mgmt	Yes	Yes	ZS – Users may need to disable proxy to connect, then re-enable
Roaming User Config via Mgmt Console	Yes	Partly	ZS – Available but options are much more limited than Webroot offers
PAC Files Mgmt and Storage within Service	Yes	No	ZS – Not available
Threat Detection			
Antimalware Protection (Viruses, Trojans, Spyware, etc.)	Yes	Yes	ZS – Available, APT protection is extra cost
Real-Time Anti-Phishing	Yes	No	ZS – Offers IP reputation scoring (PageRisk), not real-time checks
Proprietary Detection for Malicious JavaScript, XSS & Shellcode	Yes	Yes	ZS – Claim sandboxing and APT but detail and extent are very light
Scan Ahead & Safe Search Protection	Yes	No	ZS – No Safe Search or Scan Ahead
Threat Protection Included in Pricing	Yes	No	ZS – APT protection is extra cost
Botnet Detection & Zombie Alerting	Yes	Partly	ZS – Unknown detection efficacy, no alerting despite claims
HTTPS/SSL Decryption & Scanning	Yes	Yes	ZS – Available, but unreliable
Web Filtering			
Reputation & High Categorization Web Filter	Yes	Yes	ZS – Less accurate than Webroot BrightCloud Threat Intelligence
Split Tunneling Bypass Option	Yes	No	ZS – No split tunneling
Coaching Option for Web Filtering	Yes	No	ZS – No coaching
Granular URL Filtering Categories	83+	90+	ZS – Less accurate than Webroot BrightCloud Threat Intelligence
File Type & Streaming Media Control	Yes	Yes	ZS – Available, but only by blocking files
Social Media/Web 2.0 Post Blocking	Partly	No	ZS – Available, but no selective control over social networking sites
Management			
Transparent User Auth. for Citrix & Terminal Server Users	Yes	No	ZS – Not available
Independent User Alerts, Admin Alerts & Blocking Options	Yes	Yes	ZS – Not available
Policy Groups Configuration in UI	Yes	No	ZS – Only imports from LDAP, no option to create groups in UI
Granular Role-Based Admin Controls (Group, Policy & Feature Specific)	Yes	No	ZS – Not available
Reporting/Logging/Alerting			
Detailed Logging Capabilities	Yes	Yes	ZS – NanoLog Streaming Service available (extra cost), SIM/SIEM integration
Flexible Scheduled Reporting/Charts	Yes	Yes	ZS – Available, but only 6 months of log history
Configured Chart Saving for Repeat Viewing	Yes	No	ZS – Not available
Customized End User Notifications for Malware, Filtering, Quotas, Alerts	Yes	No	ZS – Not available

Key Points

- Over 3,500 customers globally have used the SecureAnywhere Web Security Service
- Webroot is a member of Internet Watch Foundation and is US CIPA compliant
- Webroot is West Coast Labs, ICSA, VB100 certified and SAS70 audited

BrightCloud Stats

- 27B+ Classified URLs, 600M Classified Domains, 9B+ File Behavior Records, 4B+ IP Addresses, 37M+ Connected sensors
- 4.7M URLs classified daily, 25K new malicious URLs daily, 237K+ daily phishing checks, 6K+ new phishing sites daily, 5.2B file lookups daily, 120K+ new malware items (inc. PUA), 790K+ new files daily

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