

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.



OpenDNS specializes in using predictive intelligence and Big Data to provide DNS lookup services aimed at protecting users and networks. Umbrella is their security solution, split into Professional, Insights and Platform variants. Security is delivered in the cloud layer and is protocol agnostic, which OpenDNS maintains is better for malware prevention. They also offer web filtering using proxies version.

Established	2006
Headquarters	San Francisco, CA, USA
Revenue	Unknown
Company Status	Private
No. of Employees	Unknown
No. of Customers	~50M users, consumers & 10K+ businesses

Deployment	Webroot	Umbrella
Availability	99.99% Uptime	100% Uptime
Antimalware	100% Known Malware	100% Known Malware
Antispyware	100% Known Spyware	None
Web Latency	Milliseconds	None
Policy Propagation	99.9% Updates within 5 mins	100% Updates within 10 mins

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 Umbrella	
Average Position	Supporting Messages
Strengths	Brand presence and market share: 50M daily users, 2% internet traffic. Widely known in network services industry
	Fast Setup: small Win/Mac agent for roaming clients (except Umbrella Enterprise). Provisioning & configuration ~20 minutes, comes with 50+ content filters
	Active Directory Support: Insight or Everywhere product. Uses a Virtual Appliance within internal network that acts as a DNS forwarder

De-Positioning Umbrella (continued)

Average Position	Supporting Messages
Vulnerabilities	Limited URL filtering: only 60 categories, which is just above the minimum that Gartner recommends in its Secure Web Gateway criteria (58)
	Antivirus/spyware scanning: Umbrella relies on IP reputation and domain. No antimalware scanning; uses search algorithms to gather intelligence and prevent breaches instead
	In-Depth User Access Controls: Umbrella offers little or no quota, time of day, bandwidth or other advanced user access controls
Sales Tactics	Single layer defense: only blocks bad IPs and domains, nothing else
	No data file content controls: doesn't look at attachments or data posts, so no DLP
	No malware scanning: Webroot is specialist web security vendor. BrightCloud services exceed those of OpenDNS, as security is only a part of what they offer, and their threat research is very limited and very NEW
	Not a Secure Web Gateway: Lacks features of a secure web gateway

Features	Webroot	Umbrella	Notes – How to Win
Roaming User Support			
Roaming User Authentication without Server/Key Mgmt	Yes	Yes	OD – Uses local agent to enforce policy on remote users
Automatic Hotspot Mgmt	Yes	Yes	OD – Not needed by OpenDNS
Roaming User Config via Mgmt Console	Yes	Yes	OD – Via policy group
PAC Files Mgmt and Storage within Service	Yes	No	OD – Not needed by OpenDNS
Threat Detection			
Antimalware Protection (Viruses, Trojans, Spyware, etc.)	Yes	No	OD – None available
Real-Time Anti-Phishing	Yes	Partly	OD – Also uses site rep and associations, but not as in-depth
Proprietary Detection for Malicious JavaScript, XSS & Shellcode	Yes	No	OD – None available
Scan Ahead & Safe Search Protection	Yes	Partly	OD – Provides block page informs
Botnet Detection & Zombie Alerting	Yes	Yes	OD – Basic detection
HTTPS/SSL Decryption & Scanning	Yes	No	OD – None available
Web Filtering			
Reputation & High Categorization Web Filter	Yes	Partly	OD – Similar predictive technology to BrightCloud intelligence
Split Tunneling Bypass Option	Yes	No	OD – No split tunneling for remote users
Coaching Option for Web Filtering	Yes	Yes	OD – Does provide coaching
Granular URL Filtering Categories	83+	60+	OD – URL categorization is much less sophisticated
File Type & Streaming Media Control	Yes	No	OD – Provides media type policy controls AS COST OPTION
Social Media/Web 2.0 Post Blocking	Partly	No	OD – Provides application controls AS COST OPTION
Management			
Transparent User Auth. for Citrix & Terminal Server Users	Yes	No	OD – None available
Independent User Alerts, Admin Alerts & Blocking Options	Yes	Partly	OD – Offers Block Pages only, no inform pages
Policy Groups Configuration in UI	Yes	Yes	OD – Enterprise platform offers policies at Global/Group/User levels
Granular Role-Based Admin Controls (Group, Policy & Feature Specific)	Yes	No	OD – Admins at large companies can't manage specific groups/functions
Built-in Remote Access for Customer Support	Yes	No	OD – None available
Reporting/Logging/Alerting			
Detailed Logging Capabilities	Yes	Yes	OD – Continuous detailed logs with up to 2 years' data, not as rich as what Webroot provides
Flexible Scheduled Reporting/Charts	Yes	Yes	OD – Available via mgmt console
Customized End User Notifications for Malware, Filtering, Quotas, Alerts	Yes	No	OD – None available

Key Points

- Webroot is consistently chosen over Umbrella/OpenDNS by customers who compare the two services in trial
- 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