WEBROOT®
Smarter Cybersecurity™

Webroot SecureAnywhere® DNS Protection vs. Cisco Umbrella

DNS Feature or Capability	Cisco Umbrella	Webroot	Comment	Planned	Benefit(s)
Web filtering & Protection					
Block or Allow URL Category Filtering	60+	82+	Webroot has more, and more accurate categories than Cisco Umbrella		Create policies to control unproductive, uncompliant or dangerous web usage
Internet Watch Foundation (IWF) Black List	✓	✓	Webroot is a member of IWF. Black list included in Adult/Porn and Illegal Cat		Policies specifically for Education, or other regulated access. Webroot already compliant.
Block by Domain	✓	✓	Block at the domain level		Manage (user) access by brninging up a Block Page
Allow - Whitelist by Site or Domain	✓	✓	Allow by Domain or sub-domain		Ability to correct miss-categorizations, specify sites NEVER to be blocked, even in blocked categories
Block - Blacklist by Site or Domain	✓	✓	Block by Domain or sub-domain		Ability to enforce a block, specify sites always to be blocked even in allowed categories
Group, User-Level Allow or Block	✓	✓	Policy at Group or user level control		Group-level control allows MSPs greater flexibility in designing policies based on client needs.
Timed Access	✓	✗	Policy control over either time of day or time period	✓	Policy specifically around the duration or the time of access to the Internet.
White List Only - Lockdown Feature	✓	✓	Block all categories of URL and only allow specified white list		For highly limited Internet access use cases
On-Network Control	✓	✓	Control access to Internet for devices connected through the network		Control all devices connecting through any part of the on-site premises network
Off-Network Control	✓	✓	Control access to Internet for devices not connected through the network		Control all access by user devices, regardless of location.
Real-Time - Block Malicious URL Domains	✓	✓	Standard policy blocks malicious sites		Part of URL filtering categories
Real-Time - Block Outbound Traffic to Malicious Sites	✓	✓	Stops exfiltration to known malicious sites		BrightCloud Web Classification stops this vector
Policy by Static IP Address, or Address Range	✓	✓	Allow policy control of network traffic by specific IP addresses		Enables admin to set policy for different network segments and devices i.e., guest network
Policy by Dynamic IP Address	✓	✓	Allow policy control of network traffic by dynamic IP addresses		Enables admin to have policy control without concern for fixed or static IP addresses
Handle HTTP and HTTPS Traffic	✓	✓	Over 50% of web sites use encrypted traffic, DNS accommodates this		Other web filtering often needs browser certificate management to allow encrypted traffic
Reporting & Logging					
Reporting on Cloud Services	✓	✗	Report on SaaS services and applications i.e., Drobox, Salesforce		Detailed reporting on cloud services requires a proxy service, which introduces latency for clients.
Ability to Retain Logs	✓	✓	Log retention so reports and intelligence can be seen		Logs will be automatically stored for 12 months. This information can be found within the Active Host report.
On-Demand Drill Down Reporting	✓	✓	Reporting focused on Corp/Guest Network protection with five pre-made reports		“Top Blocked” Reports available across a variety of parameters
Scheduled Reporting	✓	✓	Reporting focused on Corp/Guest Network protection with five pre-made reports		Reports available on-demand and with flexible scheduling.
Policy » AntiVirus Schedule					
Fast Deployment	✓	✓	Simple re-direct of network internet traffic		Quick time to benefit for MSP and customer
Domain Layer Protection and Prevention	✓	✓	Attacks thwarted at the domain layer		Keeps threat outside the network and vulnerable endpoints (PCs and Servers)
Primary Protection	✓	✓	First line of defense		Threat mitigation is bi-directional: inbound (infiltration) and outbound (exfiltration)
Support for Network Devices	✓	✓	Supports environments where multi-device and non-agent devices exist		Helps manage environments like hospitals and schools. Avoids tampering and circumvention.
Reduced Bandwidth	✓	✓	Reduced bandwidth consumption		May help reduce costs of ISP connectivity and any need to upgrade the network
Visibility of Traffic	✓	✓	Ability to look at internet traffic and report on usage		Improved visibility of web traffic decreases compliance concerns.
Visibility of Usage	✓	✓	Insight into traffic		Visbility of web usage allows admins to identify drains on productivity and bandwidth.
Visibility of Blocked Threats	✓	✓	Insights into impact of installing DNS Protection		Visibility of blocked threats allows admins to spot patterns of high-risk behaviors.
Granular Visibility into User Actions	✓	✓	Highlights productivity, misuse, and training needs		Monitoring device-level internet usage improves the ability of MSPs to refine access controls.
Uses BrightCloud Web Classification TI	✗	✓	Most up to date and accurate source on the Internet		This makes DNS Protection superior to Cisco Umbrella and more predictive
API Integration	✓	✓	API integration offers nearly unlimited options for managing and provisioning DNS Protection.		Featuring easier and faster integration into RMM/PSA platforms
Integrated Endpoint DNS Management	✗	✓	Primary reason MSPs will use Webroot instead of Cisco Umbrella		Lightweight integrated agent for both endpoint and network protection.
Securely Hosted DNS Servers	✓	✓	Both sevices offer carrier grade infrastructure		Securing DNS is essential for the modern business.
Customizable User Block Pages	✓	✓	Allow adminstrator to inform user why access is blocked		Webroot can personalize text and import logos
Tailored and Pre-made Policies	✓	✓	Faster deployment as standard policies are provided and easily tailored		Webroot supplies 3 standard policies: Low, Medium, and High Protection