WEBROOT
Smarter Cybersecurity™

FAQ | Migration Guide: From the Web Security Service to DNS Protection

Introduction

The Webroot SecureAnywhere® Web Security Service has been discontinued. This migration guide provides information to help you evaluate whether Webroot SecureAnywhere® DNS Protection would be a suitable migration choice for your business.

Key Differences

The Web Security Service is a bi-directional filtering service that controls different types of web content—including malware, certain file types, and URLs—so admins can control end users' internet traffic. It uses an on device agent to ensure all user device traffic is directed through secure Webroot web proxies. Because of its multiple content filtering roles, the service must act as an intermediary, inspecting all web traffic. By nature, the inspection processes introduce minor latency to users' web requests and responses.

SecureAnywhere® DNS Protection is designed to protect an organization's DNS connection by directing all DNS requests via Webroot's secure outbound DNS resolver servers. These secure DNS servers are hosted around the globe, and they prevent the DNS connection being attacked or hijacked by cybercriminals, while guaranteeing that users connect to the internet securely.

By handling all outbound DNS resolutions, DNS Protection will query outbound DNS requests and block access to URLs with a poor website category or reputation. Unlike the Web Security Service, DNS Protection does not filter or inspect the traffic content type, so introduces little to no latency.

Setting up DNS Protection

Administrators can set up DNS Protection quickly and easily. In just a few minutes, you can apply policies for corporate and guest networks, Wi-Fi in cafés and reception areas, and anywhere else devices might use one of your access points. DNS Protection is designed to complement SecureAnywhere Business Endpoint Protection to provide a comprehensive, effective cybersecurity solution.

Managing DNS Protection

Unlike the Web Security Service, which required a standalone management console, DNS Protection is managed via the same streamlined Global Site Manager console used to administer SecureAnywhere Endpoint Protection.

Next Steps

To migrate to DNS Protection, or to further evaluate this solution within your environment on a free 30-day trial, contact your Webroot Account Manager or open a support ticket at mysupport.webrootanywhere.com.

See reverse for a feature comparison chart.

Web Security Service vs. DNS Protection Feature Comparison

Features & Functionality	Web Security Service	DNS Protection	Comments
Operation & Deployment			
Fast Deployment	✗	✓	DNS Protection only requires an IP traffic redirect
Domain Layer Protection & Prevention	✓	✓	DNS Protection blocks and allows traffic at domain layer, outside the network
Pre-configured & Custom Filtering Policies	✓	✓	DNS Protection provides both standardized and easily customized URL policies
Network Device Support	✗	✓	DNS Protection IP filtering covers traffic from all devices, i.e., via a guest network
Customizable Block Pages	✓	✓	DNS Protection block pages work in tandem with Endpoint Protection block pages
Streaming Media Bandwidth Control	✓	✓	DNS Protection works by URL category filtering
Granular Visibility Of User Actions	✓	✓	DNS Protection agent users only
Visibility Of Traffic, Usage, Blocked Threats	✓	✓	Built-into DNS Protection reporting
Block Unclassified URLs	✓	✓	Fully available in DNS Protection
Integrated Endpoint and DNS Protection Management	✗	✓	DNS Protection is fully integrated into the GSM console
Securely Hosted Servers	✓	✓	DNS Protection is hosted by multiple datacenters
Reporting & Logging			
Cloud Services General Reporting	✓	✓	Built into DNS Protection reporting
Cloud Services User Reporting	✓	✓	DNS Protection agent users only
On-Demand Drill Down Reporting	✓	✓	Built into DNS Protection reporting
Scheduled Reporting	✓	✓	Built into DNS Protection reporting
Log Retention	✓	✓	User level reporting for DNS Protection agent users only
CSV Export Facility For Data Manipulation	✓	✓	Available for some DNS Protection reports, more to come
Customizable End User Notifications/Alerts	✓	✓	DNS Protection inform pages work in tandem with Endpoint Protection informs
Web Filtering & Protection			
Reputation & Categorization Filtering	✓	✗	DNS Protection offers URL category now, reputation in a future release
Anonymous Proxy Detection	✓	✗	Only by URL, not proxy server checks
Coaching Option For Web Filtering	✓	Partial	Partial information with DNS inform pages
Granular URL Filtering Categories	✓	✓	Both services use 82 URL categories from our BrightCloud Web Classification service
Streaming Media Control	✓	Partial	DNS Protection controls by URL category, not file type
Anti-Malware Protection	✓	✓	DNS Protection offers malicious URL category policies
Malicious Script Detection	✓	✗	DNS Protection does not scan inbound file content
HTTPS/SSL Decryption and Filtering	✓	✓	DNS Protection works by URL category, not file type
Internet Watch Foundation Integration	✓	✓	URLs supplemented by Internet Watch Foundation
Group Level Blocking	✓	✓	DNS Protection blocks by IP, IP Address Range, Agent policy
Machine-Level blocking	✓	✓	Future feature of the DNS Protection agent, currently in development
Timed Access	✓	✗	Future feature of the DNS Protection agent, currently in development
Mobile User Filtering	✓	Partial	DNS Protection filters all on-network devices, regardless of OS
Real-Time Blocking for Malicious Domains	✓	✓	DNS Protection works by URL category
Real-Time Blocking for Outbound Malicious Traffic	✓	✓	DNS Protection works by URL category
Assign Policy To Static IP or IP Range	✓	✓	DNS Protection policies are by single IP or IP range
Assign Policy To Dynamic IP Addresses	✗	✓	DNS Protection policies can be applied to dynamic IP addresses

About Webroot

Webroot delivers network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions, BrightCloud® Threat Intelligence Services, and FlowScape® network behavioral analytics protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

© 2017 Webroot Inc. All rights reserved. Webroot, BrightCloud, FlowScape, SecureAnywhere, and Smarter Cybersecurity are trademarks or registered trademarks in the United States and/or other countries. All other trademarks are properties of their respective owners. FAQ _ 101717 _ US