WEBROOT
Smarter Cybersecurity™

FAQ | Webroot SecureAnywhere® DNS Protection

What is Webroot SecureAnywhere® DNS Protection?

Webroot SecureAnywhere® DNS Protection is a new Domain Name Server (DNS) security solution that is easy to deploy and manage, and fully integrated into the Webroot Global Site Manager (GSM) console.

What is it designed to do?

SecureAnywhere DNS Protection enables MSPs to fine-tune their customers' web access policies by IP address, and limit access to websites that are considered a risk to their network.

How granular are the web access controls?

Webroot provides 82+ URL categories to allow MSPs to determine the right usage policies for each customer they wish to manage and protect.

What is the benefit?

By leveraging Webroot's industry-leading internet threat intelligence services, MSPs are able to automatically block malicious websites and filter undesirable websites. This drastically reduces the number of malware threats that could potentially infect a customer's network and endpoints. Because it operates at the domain layer, it offers protection at the most logical and effective place – outside the customer's network.

How does it work?

Webroot provides the MSP with a new license key and the customer then directs their internet traffic through the Webroot SecureAnywhere® DNS Protection service. The service is hosted and operated within secure datacenters and uses hardened domain name system security extension servers to check and control each customer's web access, regardless of the device type the user is using.

Will DNS Protection impact network speed?

SecureAnywhere DNS Protection does not introduce any internet connection latency. Connections to websites are checked instantly. In fact, because of the superfluous internet traffic DNS Protection stops, you are likely to see increased network bandwidth availability and performance.

What qualifies Webroot to offer this service?

Webroot has been securing the connected world since 1997; innovating, refining, and applying machine learning since 2007; and has been fully cloud-based since 2011. Our threat intelligence is extracted from the Webroot® Threat Intelligence Platform—our proprietary cloud-based security architecture specifically designed for advanced internet threat prevention and protection.

Our platform captures massive amounts of data from millions of global sensors and endpoints, as well as other fully verified sources (around half a trillion new objects per day) and then analyzes and classifies that data within the cloud using advanced machine learning and behavioral heuristics.

Webroot then applies deep contextual analysis to turn that data into relevant and actionable security to protect individuals, businesses, and our 40 plus technology partners against internet web, file, and mobile threats.

This huge reach enables Webroot to effectively categorize both known and unknown internet objects at a scale few other security vendors can match.

- We capture up to 10 million input characteristics for each internet object we classify
- We then use machine learning to assign up to 40 million weights to the input characteristics
- We classify millions of domains, URLs, IPs, files, and mobile apps daily
- We analyze the relationships between internet objects to determine highly accurate reputation scores

Who is Webroot SecureAnywhere® DNS Protection for?

Any business with internet connectivity will benefit from DNS Protection.

This service is designed to meet the needs of both MSPs and small businesses by creating a secure internet connection and giving them control of internet usage policies.

Roadmap for 2017

Webroot will follow Version 1 with Version 1.5 and Version 2 releases in 2017, which are planned during the June to October timeframe. We will then offer a device-based agent version to protect mobile and remote users accessing the web, regardless of their access location.

Our initial release will offer a global policy for all off-site devices, however we will continue to expand the functionality throughout the year to include more granular policy management and control.

How does SecureAnywhere DNS Protection compare to other DNS security solutions?

The service is brand new and uses the latest and most up-to-date cloud-based architecture to provide the best possible service levels to our partners and their customers. With a throughput of 30 billion requests per second per cluster, you can see latency and other issues are not a concern.

We are providing new secure DNS server resolvers and adding the market-leading accuracy, reach and breadth of our Webroot BrightCloud® Web Classification service and the computing scale of our Webroot Threat Intelligence Platform.

What are the benefits of Webroot SecureAnywhere® DNS Protection?

» Drops risky internet connections at the domain level

» Stops infections before they reach customers' networks or user devices

» Significantly reduces costs associated with infection remediation

» Provides detailed logging and reporting of overall web usage

» Works on any Windows®, Mac®, Linux, Android®, and iOS® devices that connect to the network

» Enforces acceptable use policies for staff and guest connections using 82 site categories

» Ensures a more trusted and secure internet connection

» Doesn't require on-premises hardware or software

» It's extremely fast and easy to deploy

» Pre-prepared policy templates automatically filter Phishing, Botnet, Malware, Adult, and other questionable site categories, such as Weapons and Gambling

» Easy to create and deploy both custom and pre-configured Webroot policies by IP

» On-demand drill-down management reporting covers the threats the network would have been exposed to without the DNS service

How is Webroot SecureAnywhere® DNS Protection priced?

Webroot SecureAnywhere DNS Protection is provided at the same price points as Webroot SecureAnywhere® Business Endpoint Protection. Similar MSP discount and pricing rules apply. Initially, the service will only be available to purchase under annual contract terms with monthly billing flexibility.

Does DNS Protection safeguard users when they are off-site?

Yes, DNS Protection offers agent-based protection with a global policy to ensure consistent protection for all devices leaving the network.

Do I need to install a second agent to manage DNS Protection?

No. Webroot has updated Global Site Manager (GSM) console, the management tool used for Business Endpoint Protection, to include DNS Protection. That means it's fast and easy to add network protection to existing endpoint protection.

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

WEBROOT
Smarter Cybersecurity™

Q&A

Webroot SecureAnywhere® DNS Protection

Add an Extra Layer of Security to Your Network

Security

Q: How can DNS Protection improve my security?
A: DNS Protection leverages the industry-leading Webroot BrightCloud® IP Reputation and Web Classification database. This protects all systems on your network from accessing known malicious sites, which significantly reduces exposure to threats and enhances your security.

Q: I already use Business Endpoint Protection. Does DNS Protection provide additional security?
A: It does. DNS Protection filters sites based on categories that are hand-picked by the administrator for each customer site. Webroot Business Endpoint Protection does feature a Web Threat Shield that's very effective at blocking low-reputation URLs, however it does not filter based on the categories of your choice.

Productivity

Q: Can DNS Protection regulate access to social media and other productivity-robbing sites?
A: Yes. Social media is an optional category that can be restricted, in addition to several others.

Performance

Q: Can DNS Protection help us resolve internet performance issues caused by users streaming video?
A: Streaming media can consume considerable bandwidth. DNS Protection can block these sites to improve performance. This is particularly valuable for offices or locations with limited bandwidth, as well as during times when there is high demand for streaming video (i.e., during major sporting events).

Usage

Q: Our office has limited available bandwidth and, at times, we can incur overage charges. Can DNS Protection help control the amount of bandwidth we use?
A: Yes, it can. By restricting sites that consume significant data—such as streaming, music, and torrent sites, data usage drops significantly. In particular, this helps reduce costs if you are billed for data or overages (such as on an LTE connection).

Q: Can DNS Protection help manage content on a guest wireless network as well?
A: Yes. As the devices on a guest network are generally not managed by your administrator, the ideal way to control content is through DNS security. Guest networks can be tightly controlled by limiting internet access to appropriate sites, thereby blocking inappropriate behavior and content.

Duty of Care

Q: HR standards require that sites with inappropriate content for the workplace be blocked. Is this possible with DNS Protection?
A: It is. DNS Protection can filter out sites based on 79 customizable categories. This includes categories designed for HR to help assure that Duty of Care requirements are met.

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