FAQ | Webroot® DNS Protection and DoH Privacy and Security

What is Webroot® DNS Protection?

Webroot® DNS Protection is a SaaS security solution that harnesses the domain name system (DNS) to securely filter all outbound DNS requests and secure DNS connections to the internet. It automatically filters all DNS requests to stop traffic going to, and responding from, domains known to be security risks.

Why do organizations need DNS protection?

Many organizations' DNS requests are handled by external DNS servers that are easily subjected to unknown attacks and compromises—like cache poisoning, redirection of requests, or DoS/DDoS attacks.

Additionally, most DNS requests are still made in clear/plain text. This provides a rich data log of who, what, where, and when internet requests are being made, potentially presenting a significant security risk.

So, with increasing numbers of unseen DNS server attacks, redirection of traffic, and the misuse of DNS request log data by hackers and ISPs, many organizations are realizing the importance of securing their DNS data at both the network and user levels. Therefore, many security auditors now recommend a fully managed DNS protected connection as an essential component for ensuring the security and privacy of internet connectivity.

How does Webroot® DNS Protection work?

Webroot® DNS Protection works by managing the DNS requests of the network and individual systems. These requests, regardless of whether they are traditional clear text or new, encrypted DNS over HTTPS (DoH) requests, are sent directly to our hardened and secured DNS resolver servers.

Webroot's resolver servers are hosted at the heart of the internet, in highly secure Google Cloud™ datacenters, so they deliver the maximum privacy, security, efficiency, and performance benefits of a managed DNS service.

Privacy is an important component of DNS over HTTPS (DoH), as it provides a mechanism to encrypt DNS requests. Webroot® DNS Protection combines privacy and security by leveraging this encryption, while also providing the secure logging and connection visibility, filtering, and security controls essential to managing and protecting DNS.

What is DNS over HTTPS (DoH)?

DoH is an initiative to prevent eavesdropping and manipulation of DNS request data by third parties, whether for malicious purposes, governmental control, or commercial reasons. DoH adds encryption to these requests, thereby hiding them from prying eyes and ensuring the privacy and security of the overall connection.

Why is DoH a problem for IT security?

Adding privacy can come at a cost. From a security perspective, the rapid adoption and usage of DoH could blindside security administrators and prevent them from extracting useful cybersecurity information by monitoring and analyzing their DNS request traffic logs.

Additionally, some applications can be configured to use DoH directly. As this bypasses the system's configured DNS server, it presents issues with filtering and accuracy of the DNS requests.

What does Webroot® DNS Protection offer that competitors don't?

Webroot has been securing the connected world since 1997; innovating, refining, and applying machine learning to domain and web classification since 2007; and has been a cloud-based, next-gen security provider since 2011.

Timely, accurate, and reliable internet threat intelligence lies at the core of effective DNS security at the network domain and user URL category levels. Webroot® DNS Protection is backed by our industry-leading Webroot BrightCloud® Web Classification intelligence—a core component of our BrightCloud® Threat Intelligence services. Our threat intelligence is trusted by over 100 leading security and network vendors around the globe to enhance the security and performance of their own products and services. That means, regardless of an organization's size or the number of dedicated security resources they may have, all DNS Protection customers benefit from the same high level of accuracy and breadth of coverage as industry leaders in the security appliance and services space.

Through the Webroot® Platform, our threat intelligence data is continuously updated every five minutes or less, helping us drive advanced internet threat prevention and protection for partners worldwide.

Does Webroot offer DoH support today?

Yes. Webroot strongly believes in the need for privacy of DNS requests and the benefits of DoH in reducing the threats from cybercriminals and those who misuse data.

Most other DNS filtering services don't truly leverage DoH. They either:

- Attempt to block DoH to maintain control
- Allow DoH, but lose security, visibility, and control

Webroot® DNS Protection leverages the privacy gained by DoH, and then adds the security, visibility, and control over DNS connections that administrators need.

How does Webroot maximize privacy?

The Webroot DNS Protection agent uses DoH to securely route DNS requests to our hardened DNS resolvers hosted on Google Cloud™. Furthermore, DoH support is available to fully protect your network, ensuring that every external DNS request is encrypted, protected and private.

How does Webroot maximize security?

Webroot BrightCloud® Threat Intelligence Services provide the essential threat data for Webroot® DNS Protection. This includes the identification of alternate DoH resolvers. These are automatically filtered, essentially preventing applications from making independent or rogue DNS requests.

Real-world results show that filtering outbound DNS requests through the Webroot service can stop malware and unwanted traffic before it ever hits endpoints or networks.

In terms of URL categorization, Webroot improves accuracy by assigning a confidence level to our categorizations. This granular categorization provides an additional threat intelligence data point for consideration. Our processes accurately categorize and score domains with an error rate of 1.5% or less, compared to an average expert human error rate of 8%.[1] (Note: the expert human error rate is the average error rate of a security professional's determinations.)

How does Webroot maximize performance and efficiency?

Architected as a SaaS solution that uses the Google Cloud Platform™, Webroot® DNS Protection maintains very low latency, efficient global connectivity, high availability, reliability, and secure hosting.

As a SaaS service, deployment from our cloud-based management console is easy, fast, and straightforward on network or roaming devices. RMM, PSA, and other integrations further help our customers automate operations and minimize operational costs.

Additionally, the Webroot® Unity API and Universal Reporter utilities provide flexibility by allowing admins to customize reports and data log extracts for further analysis.

What results can I expect from using Webroot® DNS Protection?

Webroot® DNS Protection is the first DNS service to combine privacy and security. Its benefits include:

- **Full support for DoH** at the network, user, browser, and roaming user levels
- **Full visibility** of your DNS requests provides insight into how the internet is used, enabling admins to make better-informed security and access policy decisions
- **Fewer infections and resulting costs** since, by lowering the number of responses from malicious and suspicious internet locations, DNS filtering drastically reduces the number of compromises and infections to which networks and systems are exposed
- **Granular and enforceable access policies** allow admins to take control of staff productivity, employer duty of care, HR, and compliance requirements through advanced, customizable policy controls by individual, group, or IP address.

For more information, or to request a FREE 30-day trial, visit webroot.com.

[1]Based on Webroot's internal testing.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.