CARBONITE an opentext company | WEBROOT an opentext company

Webroot® DNS Protection

The first DNS protection service to truly combine privacy and security for cyber resilience

Overview

A fully managed DNS security solution is an essential layer of every organization's cyber resilience strategy and is fundamental for ensuring the security and privacy of your internet connectivity. As more traffic is encrypted over HTTPS, firewalls lose the ability to inspect this communication, increasing the need to manage these connections as they are created. Furthermore, applications are increasingly managing DNS requests directly, rather than using the DNS servers configured on the system.

DNS requests are increasingly targeted by malicious actors because the content of each request is visible, and the integrity of the request can be compromised. Not only can DNS requests reveal what applications are in use, they also show which websites are visited, all in clear text.

As a result, organizations have realized how important it is to their security and privacy to use DNS-layer protection to secure their networks and individual users. When state actors use DNS request logs to prosecute citizens, or internet use is profiled for analytics or targeted advertising, it's clear why DNS is evolving to use the encryption with DNS over HTTPS (DoH).

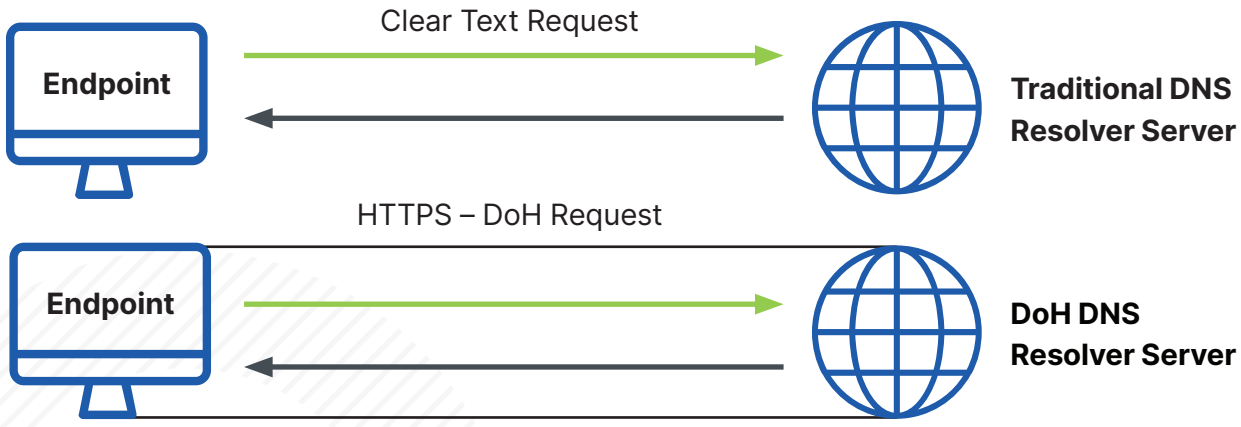
Unfortunately, when privacy is improved, security is often compromised. Solutions to filter and manage DNS requests can lose the visibility and control they once had. The use of DNS over HTTPS is expanding. Internet browsers and even operating systems are beginning to take advantage of the benefits of DoH, as it improves privacy while ensuring the source and content of the DNS request are genuine.

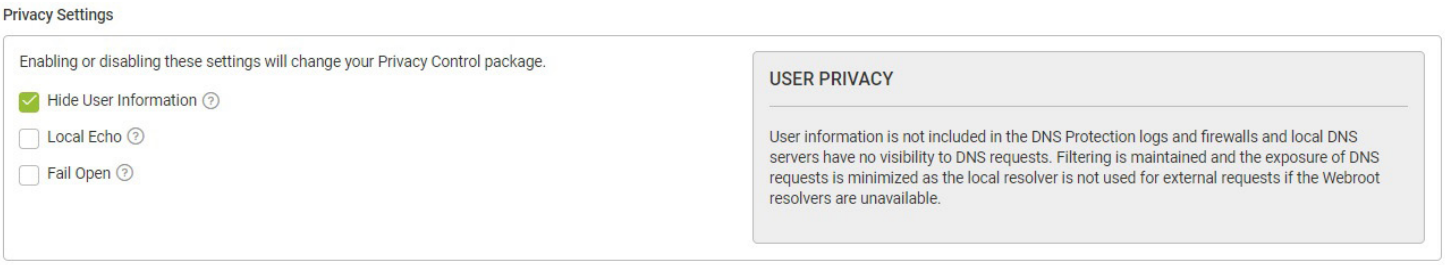
To combat this, most commercial and private DNS filtering solutions either:

1. Block the use of DoH in order to retain DNS filtering and visibility into the requests.
2. Allow DoH requests, but give up the ability to filter and use DNS requests for security.

First DNS Protection Service to Combine Privacy and Security

DoH is a logical evolution of DNS and should be embraced to improve privacy, security, and overall resilience against cyber threats. Webroot® DNS Protection fully supports DoH, while providing privacy and security as control options that ensure DNS request filtering and integrity continues to function, while DNS visibility and logging levels become customizable.





This means:

- DNS requests via DoH are fully filtered at the network and roaming user agent levels.
- All requests remain totally private to your organization and invisible to your ISP or other prying eyes.
- All DNS requests are filtered with high accuracy using market-leading Webroot BrightCloud® Threat Intelligence-based policies assigned at IP, Group, or User levels.
- Admins can control how all DNS requests are logged, allowing them to configure privacy to fully comply with GDPR, while still filtering those requests.
- Webroot® DNS Protection is securely hosted using Webroot's hardened DNS resolver infrastructure within Google Cloud™, leveraging the accessibility, reliability, stability, and performance of Google's global datacenters.
- By securely filtering all DNS requests for high-risk domains, businesses drastically reduce their exposure to threats.
- Admins can configure whether local DNS resolvers have visibility into all DNS requests by enabling the Local Echo setting so that data may be shared with other security or log analysis tools.

DNS requests should be encrypted to ensure their privacy and integrity. Additionally, DNS requests should be filtered to reduce exposure to potentially damaging internet domains.

Maximum Privacy

By directing all DoH internet requests through our hardened DNS servers, hosted in the highly secure Google Cloud™ service, Webroot® DNS Protection enables the maximum privacy and security benefits of DoH, while still providing the logging, visibility, filtering, and security controls you need to effectively protect and manage DNS requests.

Maximum Security

Fundamentally, DNS-layer security is about being able to accurately filter your outbound network/user traffic. To do that effectively, you need comprehensive, up-to-date web threat intelligence. Webroot BrightCloud® Threat Intelligence Services, which power Webroot® DNS Protection, correlate data between domains, URLs, IPs, files, mobile apps, and more to provide a comprehensive and continuously updated view of the internet threat landscape—not just URLs and IPs.

As applications begin to encrypt DNS requests directly, firewalls lose visibility and control into what is accessed on the internet. Webroot® DNS Protection tracks and filters DoH providers, stopping these connections when the request is first made, leaving you in control. Real-world results show that filtering outbound DNS requests through the Webroot service will stop malware and unwanted inbound network traffic before it ever hits endpoints or networks.

Via the Webroot® Platform, Webroot® DNS Protection leverages 6th generation machine learning to examine website domains and classify websites into accurate categories. Webroot takes accuracy a step further by assigning a confidence level to these categorizations to provide an additional 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.)

Maximum Efficiency and Performance

Architected as a SaaS solution and using Google Cloud™ to ensure low latency, reliability, and secure hosting, Webroot® DNS Protection is purpose-built to enhance an organization's resilience against cyberattacks. As a SaaS solution, deployment from the cloud-based Webroot management console is fast, easy, and straightforward, whether on network or roaming devices.

RMM and PSA integrations also help automate operations and minimize costs. The added flexibility of the Webroot® Unity API and Universal Reporter tool allows for the complete customization of reports and data log extracts for further analysis.

[1] Based on Webroot's internal testing.

DNS Protection at a Glance

- **Secure Google Cloud™ hosting** – Webroot's global network of hardened DNS resolver servers ensure privacy, security, and constant availability.
- **No on-site hardware to install** – Webroot® DNS Protection is a cloud-based network (domain) security layer that takes minutes to set up.
- **80+ URL access categories** – Extensive, granular, and highly accurate domain filtering categorizations enable enforcement of user access both on and off-network.
- **WiFi and guest on-network protection** – Webroot® DNS Protection secures all device types (including Windows, Linux, Apple®, and Android® devices) that access the internet via corporate Wi-Fi, LAN, and even guest Wi-Fi connections.
- **Roaming user protection** – A Windows agent is available for consistent off-network filtering for roaming users.
- **Policy by user, group, or IP address** – We offer flexible deployment options and policy controls for most connection situations.
- **On-demand, drill-down reporting** – Webroot® DNS Protection provides full visibility into all DNS requests.
- **Support for a wide range of firewall VPNs** – We designed the DNS agent to work with the tools businesses and managed service providers (MSPs) already use, and to support many popular VPNs, including SonicWALL and others.
- **Education and regulatory compliance** – Webroot® DNS Protection helps organizations comply with U.S. and E.U. privacy laws, HIPAA, PCI, the Family Educational Rights and Privacy Act (FERPA), and the Child Internet Protection Act (CIPA). Webroot is also a member of the Internet Watch Foundation.
- **Google SafeSearch** – Google SafeSearch is also available as an additional policy-based URL filtering option for better control over educational access and public Wi-Fi filtering.
- **GDPR regulations** – GDPR regulations in even the most restrictive compliance regions is easily supported using the Hide User Information function under Privacy Settings.

Results to Expect

Webroot® DNS Protection gives you visibility and DNS filtering access control benefits, including.

- Full support of DoH at network, group, device browser, user, and roaming user levels.
- Full internet usage visibility with complete insight into all requests made to the internet so admins can make better-informed access policy decisions.
- Fewer infections by lowering the number of responses for malicious and suspicious internet locations, meaning DNS filtering drastically reduces the number of compromises, infections, and associated remediation costs.
- Granular and enforceable access policies enable admins to address staff productivity, employer duty of care, and HR and compliance requirements through advanced, customizable policy controls by individual, group, or IP address.

Trial and Next Steps

For more information, contact your Webroot Account Manager or our sales department. Visit webroot.com to initiate a FREE 30-day trial. Existing Webroot customers can also start trials directly via the Webroot management console.

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.

Contact us to learn more – Webroot US

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

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.