WHITE PAPER

CARBONITE an opentext company | WEBROOT an opentext company

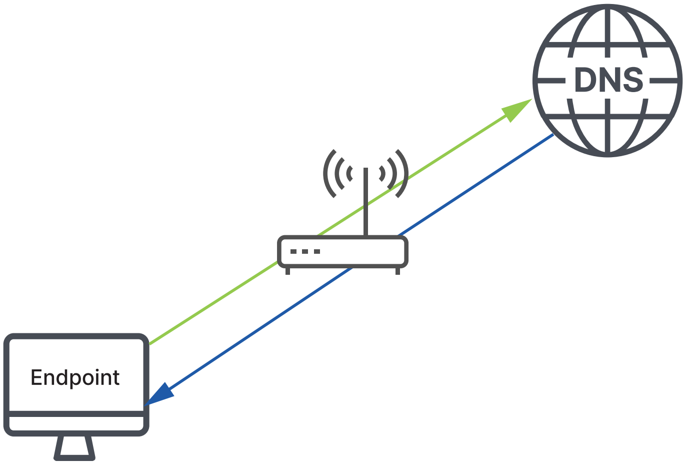
Make DNS over HTTPS (DoH) Work for You

How Webroot is harnessing DoH to ensure privacy, security, and cyber resilience

The domain name system (DNS) was designed to act as the internet's address book. Designed with scalability and performance in mind, little thought was given to how it could be compromised, abused, misused, or even harnessed for good.

As a fundamental component of the internet, the need for DNS security can no longer be ignored. DNS is frequently targeted by bad actors, and DNS-layer protection is increasingly regarded as an essential security control. In terms of making networks more resilient to cyberattacks, it is the perfect control point, since all internet resource lookups, network and user-based, need to be routed via external DNS servers.

Unfortunately, organizations are often content to let their ISP handle their DNS requests. Thus, they have no insight into which requests are being made and responded to.



Devices and applications depend on DNS

By adopting a DNS filtering solution, organizations can take control of their outbound internet traffic and benefit from several important security advantages, such as:

- Securely hosted DNS servers with many points of presence on the internet ensure reliable connectivity is never compromised
- Hardened and secured DNS resolvers that ensure your DNS requests are not intercepted, redirected, or easily attacked by malicious actors
- Access to accurate, timely, and continuously updated domain security threat intelligence
- Visibility into all DNS requests made, from which device and for which address—information which is invaluable for tightening security
- The ability to filter and block undesirable domains, either automatically or by policy

Filtering DNS requests can be extremely effective at reducing the exposure to threats. But DNS itself is potentially still flawed. As the original design focused on scalability and performance, components like encryption were left out. This leaves all DNS requests open to being intercepted, reviewed, and even altered.

Securing DNS Data

The starting point for controlling DNS requests is to fully encrypt this traffic. By doing so, you ensure which DNS resolver is fielding the DNS request, and that the DNS request has integrity and is protected. This will mean employing a service that offers a private, resilient, reliable, and scalable secure DNS resolver service.

Securing DNS Connectivity

DNS stability is integral for your internet access to be reliable. Achieving this reliability requires a resilient hosting infrastructure on which your service partner hosts their secured DNS resolvers.

In Webroot's case, we chose Google Cloud™ and run Webroot® DNS Protection within that high-redundancy, low-latency platform. Google Cloud advantages include a global presence, very secure datacenters, and the performance of leveraging the same infrastructure that supports Google Search.

Google's infrastructure also allows us to almost instantly create and auto-scale new Webroot DNS resolver clusters as needed. Located anywhere your users and Google are, these servers have the capacity to handle and scale to any necessary load.

Other major benefits of GCP are that request latency is minimized, connectivity is dispersed through multiple secure datacenters, and high-performance connectivity is maintained. DoS and DDoS attacks are also automatically identified and suppressed.

This overall platform flexibility ensures Webroot® DNS Protection delivers high service reliability, coupled with low latency and uninterrupted connectivity, regardless of traffic spikes or increased local loads.

Securing the DNS

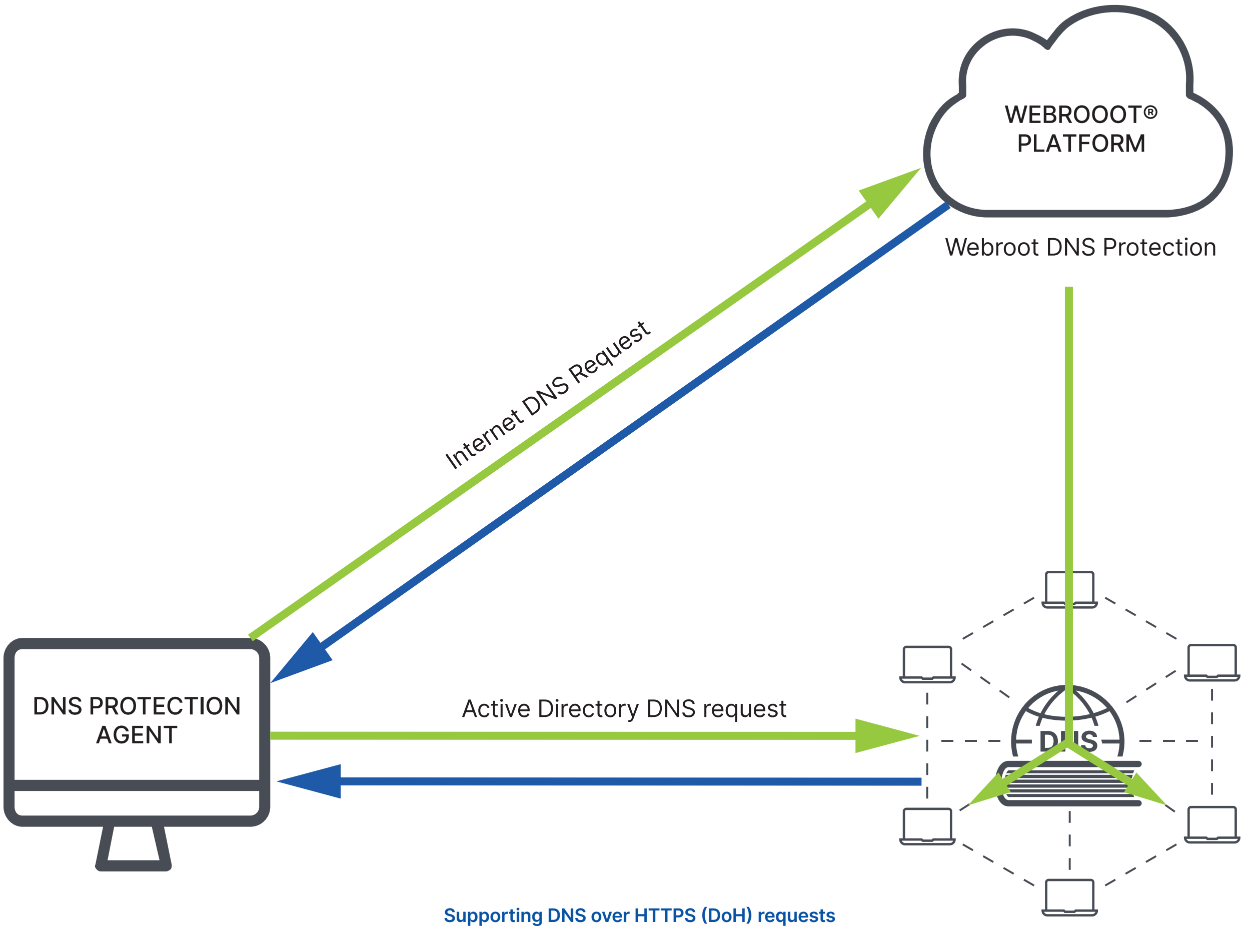
DNS exploits abound. Man-in-the-middle attacks, cache poisoning, redirection of traffic, tapping of traffic, and illicit logging of requests and destinations are all exploitable either commercially or by malicious actors.

Webroot® DNS resolver servers and infrastructure are security hardened and monitored. In this way, Webroot® DNS Protection offers better availability for organizations' critical internet connectivity, especially as compared to having no formal DNS management controls in place.

DNS over HTTPS (DoH)

Since its inception in 1983, the DNS has scaled to hold over 335 million domains which act as the gateways to billions of URLs. A far-seeing and brilliant solution, the DNS was built around performance and scalability.

By simply looking at organizations' or individuals' DNS requests, it is easy to determine how the internet is being used, from where and when websites are browsed, applications accessed, and even what devices and tools are in use on your network. And, since each of these requests are not encrypted (nor is the DNS resolver verified), clear text DNS not only exposes this information, but also exposes the integrity of the responses to compromise. Privacy and security were not a consideration. DoH looks to address that.



Supporting DNS over HTTPS (DoH) requests

DoH: Improving Privacy and Security

DNS over HTTPS is specifically designed to address the fundamental privacy and security limitations of DNS. Much like how a browser connects to a secure website through HTTPS, DoH allows DNS requests to be secured. First the resolving server is verified through a certificate, and then an SSL connection established. All DNS requests can then be communicated over this connection, encrypted and protected courtesy of HTTPS.

Privacy is improved as encrypted DoH requests are not easily monitored or intercepted. DoH also adds assurance that only the DNS provider of choice is aware of these DNS requests.

Likewise, security is improved by encrypting DNS requests. Not only does this verify that the DoH DNS resolver specified is the one providing resolution, but it also ensures that the requests themselves are protected and have not been altered or compromised.

DoH: How Encryption Causes Security Problems

Since DoH can manage DNS requests for applications directly, it has the potential to circumvent the configured DNS resolver provided on your network. This can cause new security and technical problems for organizations.

As an example, if a device is making DNS requests for a domain which hosts known botnet or malware sites, it would be important to have visibility into these actions and make corresponding security decisions. But, when these DNS requests are managed directly by an application through DoH, network logs no longer provide visibility into whether those DNS requests are occurring. Unmanaged DoH, in effect, blindsides existing security controls.

Furthermore, DoH can also circumvent most commercial DNS filtering solutions. When a DNS request is made directly by an application through DoH and not through the DNS resolver provided by the OS, filtering cannot be applied. Not only is the system exposed to the threat, but the event itself won’t be logged.

Losing the ability to filter and report on DNS requests considerably weakens overall network security.

How Webroot Harnesses DoH Benefits

DoH is the logical, essential evolution of DNS. When properly implemented, it greatly improves user and network privacy and security.

To correctly implement DoH and leverage the associated privacy and security gains, the admin must remain in control by being able select when DoH is used, while also ensuring that all DNS requests are filtered and logged.

DoH may seem to come with a high security price. But with Webroot, you can:

- Use DoH to communicate DNS requests to the Webroot resolvers, ensuring that Webroot is fielding the requests while also securely transmitting these requests so that they maintain their integrity cannot be intercepted.
- Block alternate DoH connections, thereby stopping applications from making rogue DNS requests.

We've specifically enhanced Webroot® DNS Protection to become the first DNS filtering service to combine security and privacy. Our new version of DNS Protection fully supports the new privacy DoH standard, yet also allows customers to retain the security advantages of controlling DNS requests, ensuring their internet connection is both private and secure. Your networks and devices will be protected, securely relaying DNS requests to the Webroot DNS resolvers via DoH.

In the future, we will offer more complex policy rules, taking advantage of the options provided by DoH to further support DoH privacy and security controls. This additional capability will allow organizations to calibrate the balance between privacy and security with more precision and control.

Conclusion

DoH is an important new protection for DNS requests. It will improve the overall privacy and security of the DNS requests every organization makes using the internet. But it's also important that organizations adopt this technology without losing the significant security benefits they get by managing and controlling DNS request traffic today.

By opting for a service like Webroot® DNS Protection, which allows for the benefits of DoH while maintaining appropriate visibility and filtering policy controls for all types of DNS requests and regulatory environments, businesses can enhance their overall security and become more cyber resilient.

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.