CARBONITE an opentext company | WEBROOT an opentext company

DNS over HTTPS (DoH): Helping your Clients with the NSA's Recommendation

In January 2021, the NSA released a guide that identified concerns around encrypted DNS, aka DNS over HTTPS (DoH). Although the NSA strongly recommends businesses protect their networks from rogue DNS sources to improve their network security, the question they don't really answer is: **how?**

"The enterprise resolver should support encrypted DNS requests, such as DoH, for local privacy and integrity protections, but all other encrypted DNS resolvers should be disabled and blocked."

– National Security Agency, "Adopting Encrypted DNS in Enterprise Environments"

What the NSA Guide Recommends

In its guide, Adopting Encrypted DNS in Enterprise Environments, the NSA recommends that, while encrypted DNS such as DoH has privacy and security advantages, businesses must carefully control available DNS resolvers on their networks and that all other DNS resolvers be disabled or blocked.

Why Your Clients NEED to Adopt DoH

Privacy is an important talking point. When you consider what can be exposed through clear text DNS requests, it is understandable why encrypting these requests will be important to your clients. Additionally, unencrypted DNS has become a popular attack vector for malicious actors who execute DNS hijacking attacks, in which they redirect legitimate traffic to their own malicious servers, exposing users to threats and potential loss of credentials and sensitive data. By encrypting DNS traffic, you can help prevent these types of attacks.

How to Help your Clients

Because DoH fully encrypts DNS requests, it can hide traffic from IT administrators who need to manage and filter requests. Your goal should be to make sure your clients can maintain control of DNS while still benefitting from the privacy benefits of DoH. To do so, the configured DNS resolver for the network should be the one used for all DNS resolution. For remote users, DNS requests should be fielded by DNS resolvers under your control.

By being able to secure DNS for your clients, reduce inbound malware and track web usage by individual and report that visibility to your clients, you're perfectly positioned to be your clients DoH guru, guiding them to achieve both privacy and security, without sacrificing visibility or control. That, in turn, differentiates you as a stronger choice of partner for prospective clients.

Why You Should Deploy Webroot® DNS Protection

Following the NSA's recommendations is very challenging without a tool specifically designed for the task. Webroot® DNS Protection natively supports the privacy and security benefits of encrypted DNS. It uses DoH for agent communication and supports DoH for network resolution. By leveraging the power of Webroot BrightCloud® Threat Intelligence, it enables you to identify and block alternate DNS connections, keeping you and your clients in direct control of DNS.

Webroot DNS Protection also allows you to log or hide user information with each DNS request, ensuring the visibility you need when potentially harmful requests are made, and better enabling you to keep customers safe from DNS-related threats. Additionally, the Local Echo feature is available to make sure requests stay visible.

Next Steps

Visit webroot.com to request a free trial and see Webroot® DNS Protection and DoH in action. Existing partners can also activate free trials directly in 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.