opentext™ | Cybersecurity

DATASHEET

Webroot® DNS Protection

Protective filtering that combines security and privacy

Domain Name Service (DNS) is the address book for the Internet. 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. Malicious actors increasingly target DNS requests 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, but they also show which websites are visited in clear text.

Webroot® DNS Protection fully supports DNS over HTTPS (DOH) as per NSA recommendations while providing privacy and security as control options that ensure DNS request filtering and integrity continue functioning. In contrast, DNS visibility and logging levels become customizable. 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 data centers.

Protective DNS service to offer nativeDoH privacy and security

Powered by world-class real-time threat intelligence

Architected as a SaaS solution 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 it can be deployed as a Standalone DNS Protection agent or in combination with Webroot Endpoint Protection. For both options, deployment from the cloud-based Webroot management console is fast, easy and straightforward, whether on a network or roaming devices. This means DNS requests via DoH are fully filtered at the network and roaming user agent levels. Admins can control how all DNS requests are logged, allowing them to configure privacy to comply with GDPR while still filtering those requests entirely.

Webroot® DNS Protection leverages 6th generation machine learning from BrightCloud® Threat Intelligence to examine website domains and classify websites into accurate categories. BrightCloud® Threat Intelligence Services correlate data among domains, URLs, IPs, files, mobile apps and more to provide a comprehensive and continuously updated view of the internet threat landscape.

Benefits

- ~75% reduction in malware being downloaded with our DNS-based network filtering service
- Full internet usage visibility with complete insight into all requests made to the internet including control of DNS over http (DoH)
- Fewer infections by lowering the number of responses for malicious and suspicious internet locations
- Granular and enforceable access policies
- Roaming protection : A Windows agent is available for consistent off-network filtering for roaming users.
- Flexible deployment options: Standalone DNS Protection agent or in combination with Webroot Endpoint Protection

SaaS solution with fast and easy deployment whether on network or roaming devices

How it works

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, and visibility, filtering and security controls you need to protect and manage DNS requests effectively. As applications begin to encrypt DNS requests directly, firewalls lose visibility and control of 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.

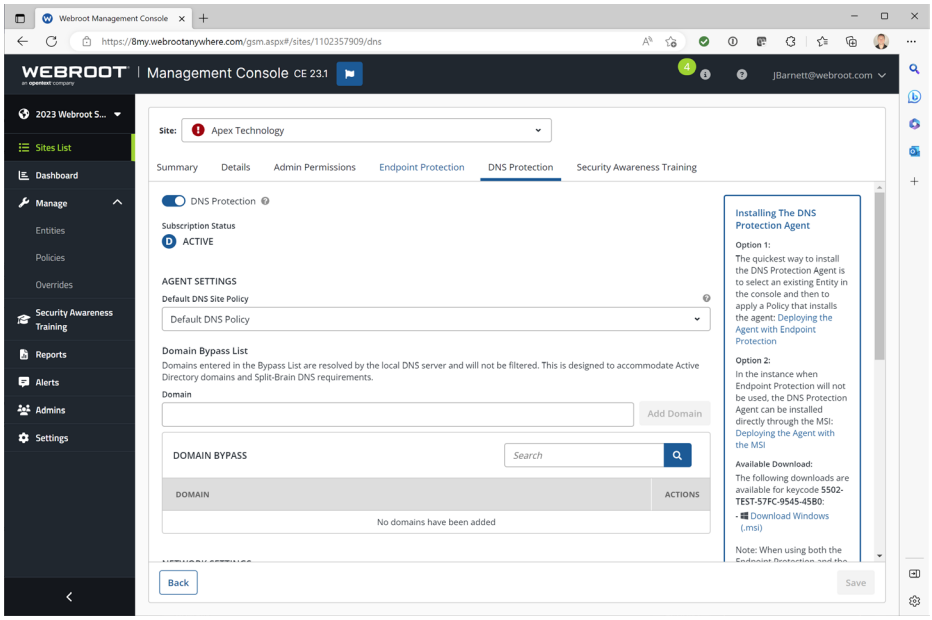
DNS requests via DoH are fully filtered at the network and roaming user agent levels. With the help of Webroot® DNS Protection, all DNS requests remain private to your organization and invisible to your ISP or other prying eyes. Webroot® DNS Protection secures all device types, including Windows, Linux, Apple® and Android® devices that access the internet via corporate Wi-Fi, LAN and even guest Wi-Fi connections. It also lets partners and customers easily protect the entire network without requiring a static IP address. Webroot® DNS Protection enhances DNS functionality while connected through the most popular VPN solutions.

Purpose-built to enhance an organization's resilience against cyberattacks

Policy-based, granular access control benefits resulting in reduction in the number of compromises

OpenText Cybersecurity brings together best-in-class solutions to help your business remain cyber resilient. Carbonite and Webroot can help you prevent and protect from threats happening in the first place, minimize the impact by quickly detecting and responding, recover the data seamlessly to reduce the impact, and help you adapt and comply with changing regulations.

Webroot® DNS Protection gives you visibility and DNS filtering access control benefits, including full support of DoH at the network, group, device browser, user and roaming user levels. It also provides 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. Overall, Webroot® DNS Protection enables you to maintain privacy without compromising security and operational efficiency.



opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_030623