DATA SHEET

### CARBONITE<sup>\*</sup>+ WEBROOT<sup>\*</sup>

OpenText Security Solutions

## Webroot<sup>®</sup> DNS Protection Combine privacy and security for cyber resilience

### **Overview**

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<sup>®</sup> DNS Protection fully supports DNS over HTTPS (DoH) 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<sup>®</sup> DNS Protection is securely hosted using Webroot's hardened DNS resolver infrastructure within Google Cloud<sup>™</sup>, leveraging the accessibility, reliability, stability and performance of Google's global data centers.

### Protective DNS service to offer native DoH 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<sup>®</sup> 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 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<sup>®</sup> DNS Protection leverages 6th generation machine learning from BrightCloud<sup>®</sup> Threat Intelligence to examine website domains and classify websites into accurate categories. BrightCloud<sup>®</sup> 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—not just URLs and IPs.

### **Key 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
- Fewer infections by lowering the number of responses for malicious and suspicious internet locations
- Granular and enforceable access policies
- Maximum privacy without compromising security and operational efficiency

# 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<sup>™</sup> service, Webroot<sup>®</sup> 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<sup>®</sup> 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<sup>®</sup> DNS Protection, all DNS requests remain private to your organization and invisible to your ISP or other prying eyes. Webroot<sup>®</sup> DNS Protection secures all device types, including Windows, Linux, Apple® and Android<sup>®</sup> 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<sup>®</sup> 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 Security Solutions 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<sup>®</sup> DNS Protection enables you to maintain privacy without compromising security and operational efficiency.

Sikes () Apex Technology		*	
Summary Details Admin Permissions B	ndpoint Protection DNS Protection Security Awareness	Training	
DNS Protection			DNS Quick Setup
Subscription Status			Step 1: Create DNS Enabled Group
O ACTIVE			<ul> <li>Navigate to the Entities page and sell the site you are configuring DNS Protection for, then expand it to view</li> </ul>
AGENT SETTINGS			groups.
Default DNS Site Policy Demo Policy		© *	<ul> <li>Create a new group that will be used manage the DNS agents selecting "Recommended DNS Enabled" for the endpoint policy.</li> </ul>
Domain Bypass List			
	ocal DNS server and will not be fittered. This is designed to accommon	late Active Directory	Step 2: Deploy the Agent - Move the desired endpoints into this group, ensuring they inherit the grou
Domains entered in the Bypass List are resolved by the domains and Split-Brain DNS requirements.	ocal DNS server and will not be filtered. This is designed to accommo	Add Domain	Snp-2: Deploy the Agent - More the desired endpoints into this group, ensuring they inherit the grou policy, - The DNS Protection Agent will install
Domains entered in the Bypass List are resolved by the domains and Split-Brain DNS requirements.	ool DNS server and will not be filtered. This is designed to accommo		Step 2: Depiny the Agent - Move the desired endpoints into this group, exounting they interest the group policy. - The ONE Protection Agent will install next time the endpoint checks in write
Domains entered in the Bypas List are resolved by the domains and Split-Brain Dris requirements. Domain		Add Domain	Skep 2: Depiny the Agence - Move the desired employers into the group, and any other the group pholo, - The Drick Transaction Agence will install read to may the Amplitude and any other doctors Skep 3: Add a Downert Typess (sproved) - Add group internal doctors, e.g.
Domains extered in the Bypas LTB are resolved by the is domains and Split-Brain Drid requirements. Demain Domain BYPASS		Add Domain	Step 2: Depiny the Agent - Million the decision demographics into the pro- position of the decision of the pro- sent of the analysis of the analysis of the next the the analysis of calculars in well contains. Step 3: And a Consume Rysens improved - Add groun reterminal domains age. - your instructions in the Decision Bysens field and circlicates. - More deall and contractes on a next stating
Domains entered in the Bypas Lite are included by the domains and spit-drain Drid requirements. Detection DOMAIN BYPASS		Add Domain	Sep 3: Depiny the Agence - Move the decined endpoints into this provide analysis of the provide the second of the analysis of the second - the OSE Protection space call install react the the endpoint called an install - Sep 3. And a General Regional General - Sec - Add yours Internet of General - Sec - Add yours Internet of General - Sec - Sec 3. And a General Regional General - Sec - Sec 3. And a General Regional General - Sec - Sec 3. And a General Regional General - Sec - Sec 3. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And a General Regional General - Sec - Sec 4. And - Sec 4. And - Sec - Sec 4. And - Sec 4. And - Sec - Sec 4. And - Sec 4. And - Sec 4. And - Sec - Sec 4. And - Sec 4. And - Sec 4. And - Sec 4. And - Sec - Sec 4. And - Sec 4. A
Domains entered in the Bypas Lite are visibled by the domains and spit-Brain Drid requirements. Densin DOMAIN BYPASS DOMAIN *webbroot.com		Add Domain	Step 2: Depiny the Agence - Move the desired engligibility into the time groups, and any step of the provident of the prov- phology - - The Earl Projection Agent will install the Earl Projection Agent will install the Earl Projection Agent will install a And by contentrating the provident of the Step - And by contentrating the provident of the Step - And by contentrating the step of the Step - And by contentrating the step of the Step - And by contentrating the step of the Step - And by content and by the Step of the Step - And by content and custom of provident of the Step of the Step of the Step of the Step - And by content and custom of provident of the - And by content and custom of provident of the - And by content and custom of contents of - And - An
Domains entered in the Digrass List are vectored by the domains and split drain Drd requirements. Device DOMAIN BYPASS DOMAIN BYPASS DOMAIN *webroot.com *webroot.com *webroot.com		Add Domain	Step 2: Depiny the Agent - Million the decision density of the provide profile. - The CHS 4-Protection Agent with installing - Age your intermed Agents Installing - Age your intermed Agents Installing - Age documents agents and agents agents - Age documents agents agents agents - Agent agents agents agents - Agent agents agents agents - Agent agents agents - Agent agents agents - Agent agents agents - Agent agent - Agent
Domains entered in the Bypas Lite are visible by the domain and split dram DrS requirements. Demain DOMAIN BYPASS DOMAIN BYPASS DOMAIN *-wsbrod.com *-wsbrod.com		Add Domain	Step 2: Depiny the Agent - Million the decision demolphisms into the pro- position of the provide the prov- position of the analysis of the analysis of the analysis - The COS # Protection Agent with integration - The COS # Protection Agent with integration - Step 3: A disc downame Registers integration - Add groun integrant downame, age- - show the analysis of the Downam Registers and - Add groun integrant downame, age- - show the analysis of the Downam Registers and - Cost agent and cost costs on installing - Cost agent and cost costs on installing in - Cost agent and cost costs on installing in - Cost agent and costs on installing in - Cost agent a

#### 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.

© 2022 OpenText. All rights reserved. OpenText, Carbonite, and Webroot are each trademarks of OpenText or its subsidiaries. All other trademarks are the properties of their respective owners. DS \_071522

Learn more at webroot.com

