CARBONITE + WEBROOT
opentext Business Solutions

Webroot®
Business Endpoint Protection

Intuitive, automated cybersecurity that helps businesses become more resilient

Overview

Today, businesses of all sizes are under constant attack. While some attacks are opportunistic, automated, and indiscriminate in nature, many are highly targeted, invasive, and precise. With the variety, volume, and velocity of attacks, it's never been more critical to use an effective, broad-spectrum endpoint security that works in conjunction with other defenses to stop malware, ransomware, phishing, cryptomining and the other damaging attacks aimed at your users and systems.

The security challenges businesses of all sizes face are the same: reduce complexity, integrate solutions into existing tools, help solve the problem of the highly variable security skills administrators have at their disposal, and ultimately become more resilient in the face of cyberattacks.

Webroot® Business Endpoint Protection solves these problems and more by delivering an award-winning[1] intuitive management console, over 40 third party integrations, a RESTful API, plus fully automated endpoint detection, prevention, protection, and remediation for a comprehensive cyber resilience strategy. It uniquely harnesses the power of cloud computing and real-time machine learning to continuously monitor and adapt each individual system's endpoint defenses to the unique threats that system and user faces.

By taking a patented proactive, predictive, and multi-layered approach to security, Webroot Business Endpoint Protection offers highly effective defenses against today's cyber threats.

Webroot's Unique Approach

Webroot® Business Endpoint Protection is diametrically different from other endpoint security solutions. As a software-as-a-service (SaaS), cloud-driven endpoint security solution, it offers a variety of benefits, including:

Hassle-free deployment

The small (<5MB) agent takes an average of 3 seconds to install[2] and is designed not to conflict with other security software. This compatibility makes deploying Webroot and replacing legacy security software much faster and easier than with other solutions, as admins no longer need to worry about impacting user productivity to roll out effective endpoint security.

Fully remote endpoint management and control

Our cloud-based management console gives you visibility and control over any device with the Webroot agent installed. You can manage multiple sites and locations and leverage powerful remote agent commands. There is no on-premises server management and the console also lets you easily trial, deploy, and manage other Webroot solutions like Webroot® DNS Protection and Webroot® Security Awareness Training, should you so wish.

Highly automated, low-cost operation

Webroot® Business Endpoint Protection was built from the ground up to be easy to deploy, manage, and maintain. You can take advantage of granular pre-configured policy templates or, easily modify them to create your own. There are never any signatures or definitions to update as threat prevention occurs in real time from the cloud. Webroot agent updates are automated, typically taking 3 seconds[2] while being completely transparent to the user. Infection alerting and remediation are automated, while regular reporting is scheduled for content, timing, and circulation. These qualities result ensure very low operational cost.

Protection online and off

Webroot uses propriety technology to monitor, journal, and contain infections even when an endpoint is offline. System and user data is protected offline too. Rather than using Windows® Volume Shadow Copy, which may be compromised by malware, Webroot protection uses a patented approach to preserving device data and protect the local host drive from being compromised or needing reimaging.

Independently benchmarked low system overheads

A key benefit of our cloud-driven approach is that the intense processing of malware discovery and analysis is performed in the cloud. Independent testing by PassMark Software shows Webroot protection has the lightest overall system resource usage among leading competitor products.[2] Full scheduled scans are transparent to users and system CPU and RAM usage are lightweight and don't hog resources.

1 G2.com. "Usability Index for Endpoint Protection Suites" (Fall 2019)
2 PassMark Software. "Webroot SecureAnywhere® Business Endpoint Protection vs. Eight Competitors." (March 2019)

Innovative detection technology
Unlike traditional approaches, which only have one opportunity to detect and stop a threat, next-generation Webroot protection works in multiple stages. First, it looks to predictively prevent malware from infiltrating the system. Then, it works to prevent malware and unknown files from executing if they display malicious behavior. Then, if a previously-unknown file (i.e. potential infection) does execute, Webroot protection monitors and journals the file's activity until it can classify it appropriately. If the file is deemed a threat, any changes it made to local drives are automatically rolled back to their pre-infected state. Not only is this multi-stage strategy more effective against modern threats, but it also reduces the chance of false positives.

Powered by world-class real-time threat intelligence
All Webroot solutions are backed by the Webroot® Platform, which integrates the same global Webroot BrightCloud® Threat Intelligence trusted by more than 100 network, security, and technology vendors to enhance the security of their products and services. Our 6th-generation machine learning architecture processes over half a trillion threat objects per day from a variety of vetted sources, as well as tens of millions of real-world customer endpoints, allowing us to generate around 1,000 new or revised machine learning models per day to help customers and partners all over the world achieve cyber resilience.

Webroot® Business Endpoint Protection at a Glance

- **Secure and resilient distributed cloud architecture** – Uses multiple secure data centers globally to support customers and roaming users with full-service resilience and redundancy.
- **Layered user and device defenses** – Stops attacks that take advantage of poor user awareness, not just those that target device vulnerabilities.
- **Malware detection and prevention** – Blocks viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, script-based, and fileless attacks, and a wide range of other threats.
- **Multi-shield protection** – Webroot's multi-shield protection includes Real-Time, Behavior, Core System, Web Threat, Identity, Phishing, Evasion, and Offline shields for detection, prevention and protection from complex attacks.
- **Malicious script, exploit and APT protection** – Patented Webroot® Evasion Shield technology detects, blocks and remediates (quarantines) evasive script attacks whether they are file-based, fileless, obfuscated or encrypted. It also prevents malicious behaviors from executing in PowerShell, JavaScript and VBScript with its Script Shield. Plus, the new Foreign Code Shield component stops exploits and advanced persistent threats (APTs).
- **User identity and privacy protection** – The Identity Shield (browser and application isolation) is trusted by the world's leading banks to stop attacks like DNS poisoning, keylogging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software.
- **White and blacklisting** – Offers direct control over application execution.
- **Intelligent firewall** – The system-monitoring and application-aware outbound firewall augments the built-in Windows® firewall to protect users both on and off corporate networks.
- **Infrared dynamic risk prevention** – Analyzes individual user behavior to dynamically tailor malware prevention heuristics.
- **Powerful heuristics** – Lets admins adjust heuristic detection based on risk tolerance for file execution.
- **Full offline protection** – Stops attacks even when offline and enables admins to create separate file execution policies for local disk, USB, CD, and DVD drives.
- **Multi OS, virtualization, terminal server, and Citrix support** – Supports MacOS® devices, Windows® computers and servers, virtualization, terminal server, and Citrix environments.
- **Multi-language support** – The installed agent supports 13 languages.
- **Free, award-winning telephone support** – Our in-house support team is standing by to resolve issues with a 95% customer satisfaction rate.
- **Transparent usage and billing** –Webroot My Usage and My Billing portals within the management console make tracking and payment transparent.

What Results to Expect

Webroot® Business Endpoint Protection helps businesses achieve cyber resilience by delivering advanced protection against the ever-increasing and evolving onslaught of modern attacks. Its highly automated and effective endpoint security means you no longer need dedicated IT security resources or experts on hand to ensure the digital fitness of your business. And, with fewer infections and security-related incidents—not to mention fewer remediation cases and productivity losses—admins can focus on what matters most: being successful.

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.

Contact us to learn more – Webroot EMEA
Email: carb-salesemea@opentext.com
Phone: 1 800 303 388

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.

CARBONITE + WEBROOT
opentext Business Solutions

Webroot® DNS Protection

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

Overview

A fully managed protective DNS security solution is an essential layer of every organization's cyber resilience strategy and is fundamental to 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 a protective DNS (PDNS) layer 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).

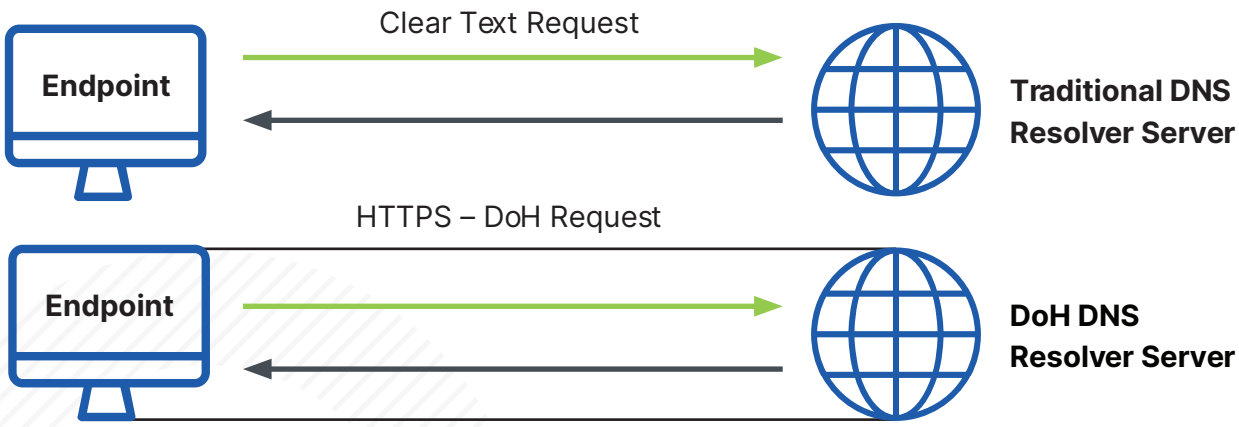
Unfortunately, when privacy is improved, security is often compromised. Solutions to filter and manage DNS requests can lose the visibility and control they once had. The use of DNS over HTTPS is expanding. Internet browsers and even operating systems are beginning to take advantage of the benefits of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

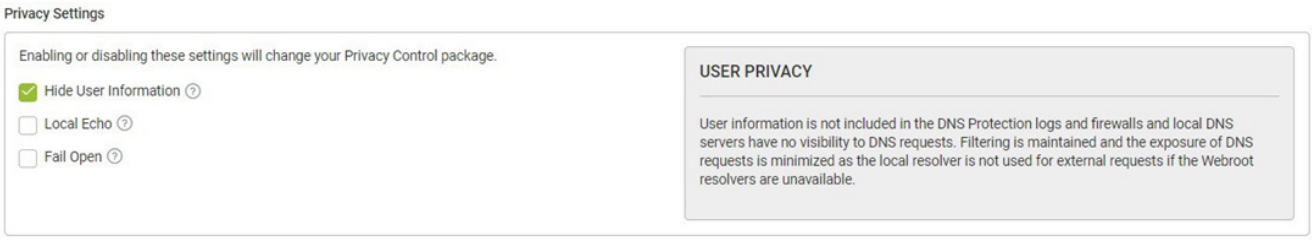
To combat this, most commercial and private DNS filtering solutions either:

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 protective 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.

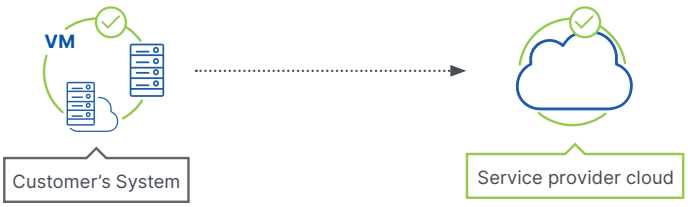
Via the Webroot® Platform, Webroot® DNS Protection leverages 6th generation machine learning to examine website domains and classify websites into accurate categories.

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.

MSP 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 and supports dynamic IPnetworks.
- **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 protective 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 their 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 EMEA
Email: carb-salesemea@opentext.com
Phone: 1 800 303 388

Contact us to learn more – Webroot APAC
Email: carb-apac_sales_team@opentext.com
Phone: 1 800 013 992

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.