WEBROOT
an opentext company

Webroot® DNS Protection

A More Secure Way to Connect Your Business to the Internet

Overview

It's easy to take the security of your internet connection for granted, many internet service provider (ISP) connections are neither secure nor safe. Their domain name system (DNS) servers simply take each internet request, look it up, and make the connection. They don't check where the request is being routed to or whether the resolver servers are hardened or secured. If these servers are attacked, you could completely lose the internet, or worse, have your data intercepted or requests redirected without knowing it. Fortunately, there is a far better and more secure way for businesses to connect to the internet.

Webroot® DNS Protection

As an innovator in cloud-based IT security services and a supplier of internet threat intelligence to over 100 network, security, and technology vendors, Webroot is uniquely positioned to offer your organization world-class DNS-layer security. Webroot® DNS Protection is an easy, effective way to secure every internet connection request being made on your network. With Webroot, you can greatly minimize the chance of simple, everyday DNS requests turning into a major security risk.

Hosted on the Google™ Cloud Platform

The Webroot DNS Protection resolver servers are hosted within the Google Cloud Platform (GCP), the same place where the majority of search requests are made. Webroot is the first and only DNS service to operate in the GCP, which brings many unique benefits, including:

Security - Preventing denial of service (DoS) attacks is a core benefit of Webroot DNS Protection, and our service now benefits from Google Cloud load balancers with built-in DoS mitigation and dynamic DoS management.

Reliability and Scalability - Webroot DNS Protection now runs on the GCP's high-redundancy, low-latency networks in 16 regions worldwide. We can also quickly auto-scale and provision more Google-based DNS servers in any region. This flexibility ensures high service reliability coupled with low latency and uninterrupted internet connectivity regardless of traffic spikes or increased local loads.

Filters HTTP, HTTPS, IPv4, and IPv6 requests

An important benefit of making requests through our DNS service is that resolve and policy filter those requests near instantly, whether they are HTTP or encrypted HTTPS. Webroot DNS Protection is also currently the only such service that filters all IPv4 ***and*** all newer IPv6 requests, which now account for nearly 25% of all internet requests.

Filters on-network and off-network requests

DNS Protection filters both on and off-network requests, and for all devices making WiFi connection requests. Finely tunable access control policies are supported at network, access point, group, and individual user levels, as is filtering for roaming users.

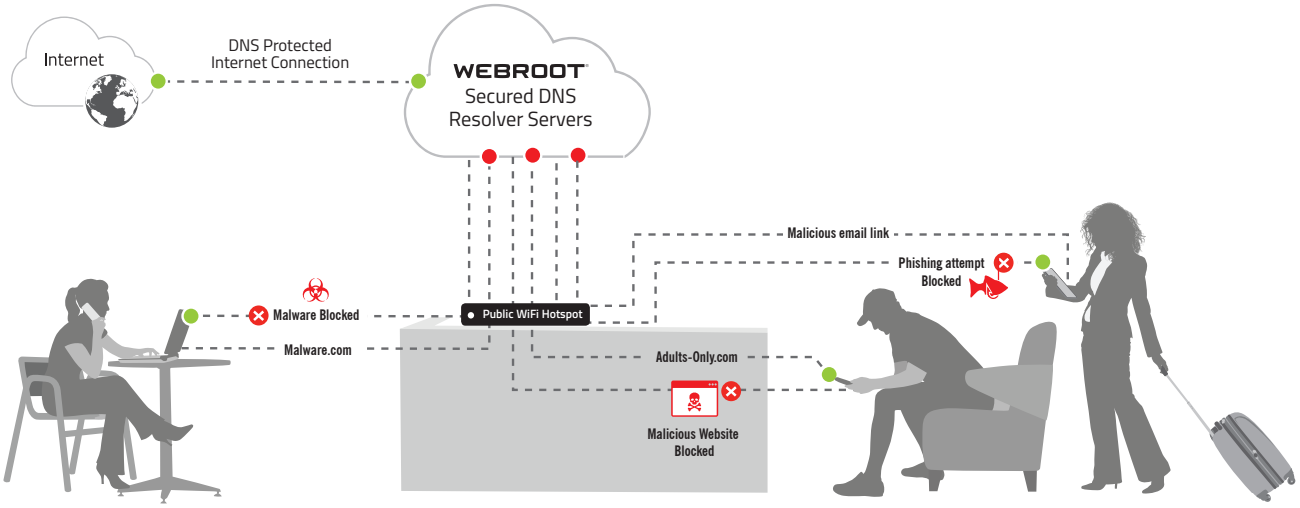
Powered by world-class threat intelligence

Webroot DNS Protection is powered the Webroot BrightCloud Web Classification Service, which is continually updated to ensure it provides the most accurate web classification intelligence available. Webroot threat intelligence informs all Webroot solutions, and is trusted by over 100 other network and security vendors to enhance the security of their own solutions.

Webroot's advanced, 6th-generation machine learning processes internet threat data from a wide variety of vetted sources, as well as real-world data from technology partners and customers. Webroot scans the internet continuously, correlating and contextualizing global threat data in real and near-real time. This timely, accurate, and reliable data ensures DNS requests to suspicious or malicious address are blocked quickly and accurately, before they can cause damage.

Prevents up to 88% of malware

Cryptojacking is a great example of how users may safely browse a cryptojacking website since DNS filtering automatically rejects requests to cryptojacking addresses. More dangerous requests to command-and-control servers, spam relays, botnets, phishing sites, and malware sites are also blocked automatically. By blocking outbound requests, DNS Protection can stop up to 88% of malware* before it even hits your network or endpoints.



Simple DNS Protection Setup

DNS Protection at a Glance

» **Secure Google™ Cloud Platform hosting** – Google's global network of hardened DNS resolver servers ensures security and availability.

» **No on-site hardware to install** – DNS Protection is a cloud (domain) based network security layer that takes only minutes to set up.

» **IPv4, IPV6, HTTP, and HTTPS filtering** – Advanced traffic filtering covers all devices and users requesting an internet connection.

» **80 URL website categories** – Our extensive and accurate URL filtering categorizations enable granular, enforced internet access controls.

» **Roaming and mobile user protection** – A Windows® OS agent is available for consistently DNS filtering off-network roaming laptop users.

» **WiFi and Guest network protection** – Webroot® DNS Protection secures all device types (including Windows, Linux, Apple® and Android® devices) that access the internet via WiFi or corporate LAN connections.

» **Policy by user, group, or IP address** – We offer flexible deployment options and policy controls for most connection situation.

» **On-demand drill-down reporting** – Webroot® DNS Protection provides full visibility into all Internet requests and connections.

» **Support for a wide range of firewall VPNs** – The Webroot agent works with a wide range of VPNs, including SonicWALL and many other vendors.

» **Regulatory policy compliance** – DNS Protection can help businesses comply with US and EU 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.

What Results to Expect

Webroot® DNS Protection offers significant security, visibility, and internet access control benefits, including:

» **Full internet usage visibility** – With complete insight into all the connection requests being made to the internet, admins can make better informed access policy decisions.

» **Fewer infections** – By lowering the number of responses from malicious and suspicious internet locations, DNS filtering drastically reduces the number of compromises and infections that would have entered your network and resulted in remediation costs.

» **Granular and enforceable access policies** – Take control of staff productivity, employer duty of care, HR, and compliance requirements through advanced, customizable policy controls by Individual, Group, or IP address.

For more information, or request a FREE 30-day trial, visit webroot.com.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

*Based on threats identified by Webroot after scanning real-world network traffic.