WEBROOT
Smarter Cybersecurity™

Webroot DNS Protection

A Stronger, More Secure Way to Connect to the Internet and Protect the Network

Overview

These days, it's easy to take the security of an internet connection for granted. But that's a huge problem. Most internet services provider (ISP) connections are neither secure, nor safe. The ISP's domain name system (DNS) servers simply take each URL request, look it up, and make the connection. They don't check where the request is being routed. Even worse, the ISP's DNS servers themselves may not be hardened or secured. That means that, if they are attacked, they and all of their customers could lose all internet connectivity. There's a smarter solution to these problems.

The Webroot Approach

As an innovator in cloud-based IT security services, Webroot is uniquely positioned to offer next-generation DNS-level protection. Webroot DNS Protection is a straightforward and highly effective way to secure networks, control internet usage, and prevent everyday browsing from becoming a major security risk.

Connectivity, reliability, and scalability
We built our DNS Protection resolver servers at multiple points of presence around the globe, with automatic load balancing and automatic failover. No matter where a request originates, it is handled instantaneously at the nearest datacenter, or, if there is an issue, the nearest global point of presence.

Our DNS resolver servers use the latest hardware and are fully hardened against DNS cache poisoning, DDoS, and other attacks that target DNS servers. Finally, they have massive processing capacity and headroom to handle internet requests; each cluster can process 30 billion requests per second. Webroot DNS Protection is a very secure and reliable way for businesses to ensure an always-on connection to the internet.

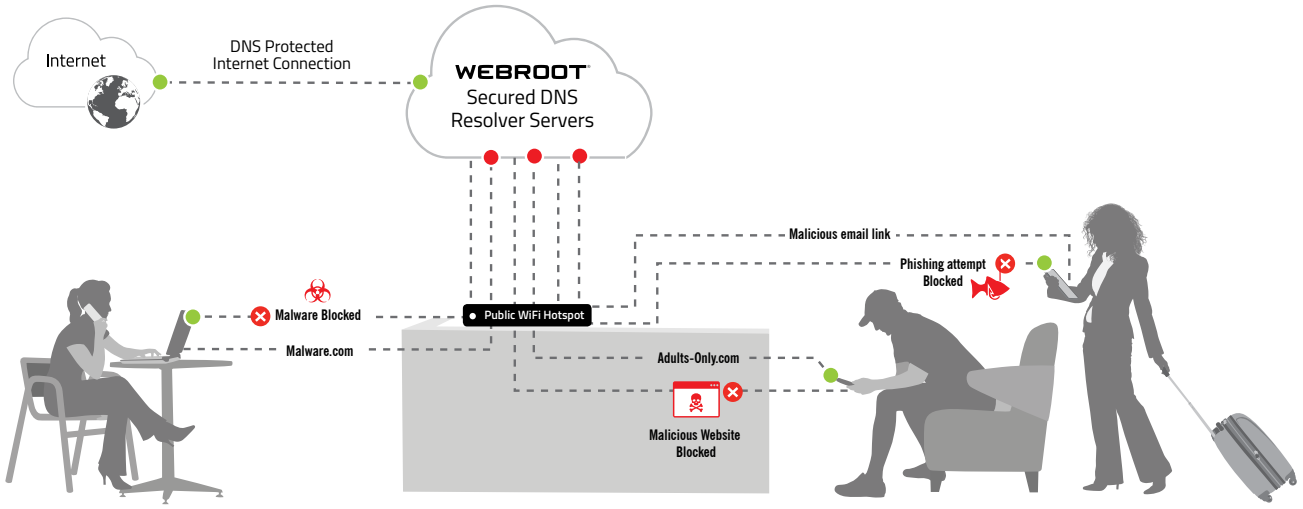
IPv4, IPv6, HTTP, and HTTPS traffic filtering
A significant security benefit of routing your internet traffic through Webroot DNS Protection is that it instantly resolves requests, no matter if they are HTTP or HTTPS requests. Filtering covers all internet traffic for any network device or user making a connection request. Webroot DNS Protection is also the only DNS service that fully covers both IPv4 and IPv6, which now accounts for nearly 25% of internet traffic.

Universal filtering for WiFi and on- and off-network access
DNS Protection can filter on- and off-network requests, as well as guest and visitor WiFi connection requests. Finely tuned access control policies are supported at the network, access point, group, and individual user access levels, as is filtering for roaming users.

Powered by world-class threat intelligence
Webroot DNS Protection is powered by Webroot BrightCloud® Web Classification Service, which is updated every 5 minutes or less to ensure the most accurate web classification intelligence possible. Webroot threat intelligence and BrightCloud services back all Webroot protection solutions, and are trusted by 90+ network and security vendors worldwide to enhance their own solutions.

Webroot has been using machine learning to classify and categorize URLs since 2007. Our advanced 6th-generation machine learning architecture processes web threat data sourced from a variety of vetted sources, as well as our own real-world customers and users of our technology partners' solutions. Webroot scans the entire internet at least 3 times per day, continuously correlating and contextualizing global threat data in real and near-real time. Using this very timely, accurate, and reliable data, any internet request to a suspicious or malicious address can be blocked automatically and accurately.

Stops 88% of internet-borne malware
As an example of the kind of access control and security DNS Protection provides, consider cryptojacking, a threat which has recently become very prevalent. With DNS Protection, users can still navigate to a website hijacked with cryptojacking scripts and consume their content, but the connection requests from the cryptojacking addresses are automatically rejected, thereby neutralizing the threat. More dangerous requests—including those to command and control servers, spam relays, botnets, phishing sites, and malware sites—are also automatically blocked. With DNS Protection, businesses and managed service providers (MSPs) who serve them can stop up to 88% of malicious inbound network traffic.



Simple DNS Protection Setup

DNS Protection at a Glance

- **Secure and reliable internet connectivity** – Our worldwide network of hardened DNS resolver servers ensures availability.
- **No on-site hardware to install** – This cloud-based network security layer takes just a few minutes to set up.
- **IPv4, IPV6, HTTP, and HTTPS filtering** – Advanced traffic filtering covers all devices and users requesting an internet connection.
- **80 web categories** – Our extensive web categorization options enable granular user access controls.
- **Roaming and mobile user protection** – We offer an optional Webroot software agent for off-network/roaming users.
- **WiFi and guest network protection** – DNS Protection secures all device types, including Windows®, Linux, Apple® and Android® devices, across guest, WiFi, and corporate LAN connections.
- **Policy control by user, group, or IP address** – We offer flexible deployment options and policy controls for any connection situation.
- **On-demand drill-down reporting** – DNS Protection admins gain full visibility into their network and connections.
- **SMB- and MSP-friendly integrated security** – Admins can trial, deploy, and manage Webroot Business Endpoint Protection, DNS Protection, and Security Awareness Training via the same intuitive online console for a single-pane-of-glass experience.
- **Regulatory compliance** – Achieve compliance 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 a member of the Internet Watch Foundation.

What Results to Expect

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

- **Full network visibility** – With complete insight into the connection requests being made and by whom, admins can make better-informed access policy decisions.
- **Fewer infections** – By reducing the number of requests to malicious and suspicious internet locations, you drastically reduce the number of infections and resulting cost of remediation.
- **Granular and enforceable access policies** – Take control of productivity, employer's duty of care, HR and compliance requirements, and more with advanced, customizable policy controls by individual, group, or IP address.

Trial and Next Steps

For more information, contact your Webroot Account Manager, our Sales department, or request a FREE 30-day trial at webroot.com. Existing Webroot customers can also access free 30-day trials directly via their management console.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.