WEBROOT
Smarter Cybersecurity™

Webroot SecureAnywhere® DNS Protection for MSPs

Provide DNS security that reduces threats and costs

Introduction

Allowing uncontrolled internet access is a high-risk activity for any business, regardless of size, but it is particularly true for small to medium sized businesses (SMEs). Internet Proxy solutions are expensive to maintain and manage, while cost-effective alternatives are few and far between. That often leads to your clients relying solely on endpoint security to protect their business from web threats that should be stopped before they even reach their networks.

Many MSPs know that finding a cost-effective internet threat vector solution that is easy to manage, reliable, and provides superior protection is a huge challenge. Webroot SecureAnywhere® DNS Protection is purpose-built to help MSPs solve the need for better internet security. By providing cloud-based, domain layer security that protects users externally, rather than relying entirely on the endpoint, providers can ensure that most internet threats are contained before they even reach the client's network.

Protection Straight from our DNS Cloud

The domain name system, or DNS, is a hierarchical naming convention for services, computers, and any other resources connected to the internet or a private network. DNS servers take text-based browser inputs and translate them into the unique internet protocol (IP) addresses that direct devices and services to the desired website. By redirecting clients' web browsing through the Webroot DNS cloud, MSPs gain immediate control of users' internet activity. The most dangerous websites are blocked automatically and all the other sites are under real-time URL category policy control.

Webroot SecureAnywhere® DNS Protection offers a simple yet effective way to prevent everyday web usage from becoming a major security risk. The DNS Protection management console is directly integrated into the Global Site Manager endpoint security console for MSPs. It appears as a separate option against each client site, and enables administrators to finely tune web access policies using both global and site-based policies. By using the intuitive drop-down menu to fill in a few client and site IP address details, then performing an easy command line service validation test, the service is live and operational right away. Each client IP address can be given a different policy, so securing a client's guest network or applying more granular site policies is smooth and straightforward.

A Simple Service with Sophisticated Intelligence

Webroot SecureAnywhere® DNS Protection is backed by the Webroot® Threat Intelligence Platform—our proprietary cloud-based security analysis architecture designed for multi-vector protection across all our solutions and services. This platform captures massive amounts of data from millions of global sensors and real-world endpoints, as well as other verified sources, then analyzes and classifies that data within the cloud using advanced machine learning and behavioral heuristics.

In particular, DNS Protection's URL filtering is supported by Webroot BrightCloud® Web Classification data. This URL database is the largest of its kind, and the service continually classifies over 600 million domains to update the database in near-real time. Webroot analyzes and categorizes websites at the rate of over 5,000 URLs per second. In fact, Webroot scans the entire IPv4 space and in-use IPv6 addresses and classifies over 95% of the internet at least three times per day. We continually analyze and classify over 4 billion IP addresses, 27 billion URLs and uncover at least 25,000 malicious URLs, 6,000 new phishing sites, and over 100,000 new malicious IP addresses per day. Our threat intelligence services are trusted by over 40 leading network and security vendors worldwide.

Webroot scans the entire IPv4 space and in-use IPv6 addresses to classify over 95% of the internet at least three times per day.

Webroot offers over 82 URL categories to allow service providers to determine the right usage policies for their clients. By leveraging industry-leading Webroot intelligence and services to automatically block malicious websites and filter undesirable website types, you can drastically reduce the number of malware threats that infect your clients' networks and endpoints.

SecureAnywhere DNS Protection at a Glance

» **Fully Integrated into the Global Site Manager (GSM) Console**
Streamlines management with a single view of all deployments across multiple sites

» **No Hardware or Software to Install**
Sets up in just minutes within the GSM console to secure clients' corporate and guest networks

» **Multi-platform Protection**
Secures Windows®, Mac®, Linux, Android®, and iOS® devices connecting to the network

» **Fast, Easy Deployment**
Simply redirect clients' network configuration to Webroot DNS Protection server IPs, it takes only minutes

» **Securely Hosted DNS Servers**
Scalable DNS resolver servers provide a secured DNS connection to the internet

» **Instant Connectivity**
Our DNS Protection service processes 30 billion user requests per second, per node, and we have over 30 nodes.

» **Low User Latency**
Performs filtering based on domain categorization, not full proxy scans, eliminating latency

» **Policies by IP, Dynamic IP or both**
Pre-configured Webroot and custom policies protect clients quickly, easily, and effectively

» **On-demand Drill-down Reporting**
Reports on the threats the network would have been susceptible to without Webroot SecureAnywhere DNS Protection

» **Customizable User Block Pages**
Use your own or client-specific block pages when end users try to access blocked content

» **Allow/Block (Whitelist/Blacklist) Support**
Create customize overrides based on clients' specific needs

» **Preset Policies and Granular filtering options**
Block websites according to 82 specific site categories (Security, Adult, Productivity, etc.)

Benefits

Aside from the obvious benefits of a cleaner network, implementing Webroot SecureAnywhere DNS Protection brings:

» **Better Network Speeds**
By blocking undesirable traffic, such as media streaming, and other unwanted or malicious content at the domain layer, you can drastically improve network bandwidth.

» **Accurate URL Filtering**
Because DNS Protection uses real-time threat intelligence that is continuously checked and updated, categorizations are always as current and accurate as possible, reducing user support calls.

» **Higher Overall Malware Efficacy**
By reducing user traffic to malicious or undesirable websites, you significantly reduce the likelihood that clients' endpoints and networks will become infected. Up to 90% less malware is possible.

» **Lower TCO and Better Margins**
DNS Protection is competitively priced and requires minimal expenditure for operation and delivery, which means better profitability and margins for MSPs. Additionally, the overall reduction in infection rates means MSPs don't have to devote as many man-hours to remediation and other lost productivity costs.

» **Client Satisfaction & Visibility**
With reduced infection rates and online distractions due to productivity policies, your clients will enjoy significant improvements in user productivity. Clients also gain immediate visibility into overall web usage and threats DNS Protection has prevented.

Easy Trial and Purchase

To set up a trial, simply call your account manager, or complete the contact form on our website. DNS Protection trials are free and unlimited for up to 30 days. DNS Protection is also available for purchase through your normal channels.

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