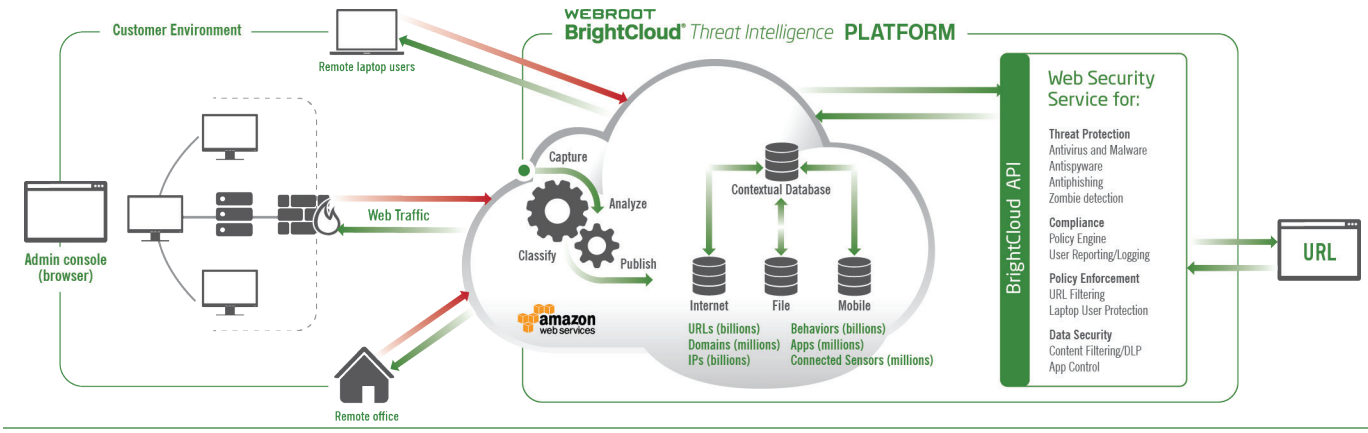
Webroot SecureAnywhere® Web Security Service

THE SMARTER WAY TO SECURE YOUR NETWORK

Today's online landscape offers great advantages to modern organizations but also brings significant risks. To ensure the success of your business, you need to effect the right mix of security checks and balances on internet use. But providing the necessary protection without impeding the everyday web usage needs of employees can be complex and costly, especially when you factor in multiple office locations and remote and mobile workers. These considerations may make some IT security managers reluctant to take on managing of employees' internet security.

But we've changed all that. Now there's a web security solution that's straightforward and highly cost-effective. The cloud-based Webroot SecureAnywhere Web Security Service enables organizations to achieve the right level of secure and productive web access for their employees. The service stops web abuse, minimizes web-borne malware risks, and consistently enforces content and access policies that optimize productive web usage. Because it's cloud-based, it's easy to manage, and can secure workers no matter where they connect, without the need for VPN backhauling or on-site hardware.

Webroot SecureAnywhere® Web Security Service Overview



PREVENT BREACHES AND INFECTIONS

Antivirus, Antispyware, Real-time Anti-phishing, and Zombie Protection

The Webroot SecureAnywhere Web Security Service incorporates Webroot BrightCloud® URL, IP, and phishing data to ensure that every type and size of organization can filter web traffic according to their own unique security needs using up-to-the-minute collective threat intelligence. Webroot BrightCloud services are trusted by over 35 leading network and security vendors, including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, and RSA, underscoring the accuracy, reliability, and timeliness of the intelligence that backs the Web Security Service.

The Service scans all HTTP and HTTPS traffic in the cloud, blocking malware before it reaches your network or users. By inspecting SSL/HTTPS traffic by URL category, it even protects against malware that is hidden in encrypted web traffic. Additionally, it offers real-time anti-phishing technology supported by BrightCloud Real-Time Anti-Phishing Service, which provides unique, nearly instantaneous assessment of every website. Even if websites have only been live for a few seconds, or were changed very recently, Webroot BrightCloud Threat Intelligence determines their legitimacy with 99%+ accuracy. This ensures that employees only connect to genuinely safe websites, thereby preventing phishing attacks that continue to be the most successful way for attackers to fool users and infiltrate networks.

The Web Security Service also automatically alerts, identifies, reports on, and blocks infected users acting as zombies from communicating with their botnet. This prevents user endpoints from being used as ingress and egress points within your network, and from being leveraged to attack others.

REDUCE OPERATIONAL RISKS

Industry-leading URL Content Filtering Plus New Social Networking Controls

The third-generation Webroot BrightCloud URL categorization and filtering engine is widely recognized as being at the top of its class. Using a highly sophisticated combination of global threat sensors, machine learning algorithms, and human classification, BrightCloud Threat Intelligence services continuously scan the entire internet—each scan taking under 8 minutes. This level of monitoring means we are able to integrate up-to-the-minute website classification data into our security services to provide proactive protection against even never-before-seen attacks.

The breadth and accuracy of the BrightCloud® URL categorization filter enables administrators to confidently enforce acceptable web access policies without the hassle of constant site categorization requests or helpdesk calls. Administrators can easily filter websites by URL category, file type, and file size using over 83 categories and subcategories.

New social network controls also let administrators set granular usage policies around Facebook, Twitter, YouTube, and WordPress. For instance, with Facebook, admins may set access policies around posting, commenting, photo updates, apps, chat, and video uploads.

The Web Security Service also includes the ability to block advertisements from websites and reformat these pages on the fly before delivering them to users, which saves bandwidth and benefits users with limited connectivity. For Web Security Service customers, this adds up to easily-enforced, accurate internet usage policies that mitigate data losses, protect users from inappropriate content, and facilitate improved user productivity.

Anonymous Proxy Prevention and Tamperproof Internet Access Control

With Webroot, you set internet access policies at the group or individual level and apply access rules by time and location. Administrators can also enable "coached" web access to inform users about policies and help them better manage their usage. Further internet access controls are available through custom URL allow and deny lists.

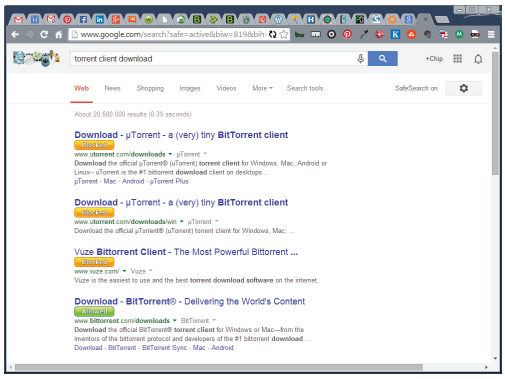
Additionally, our unique anonymizing proxy detection and prevention capability ensures internet usage policies remain enforced, even when users attempt to circumvent controls with VPNs or well-known anonymizing proxy sites. Our Desktop Web Proxy (DWP) client may be deployed so it is transparent to users and completely tamperproof.

Complete Remote User and Guest Network Support

With its tamperproof client and anonymous proxy prevention, the Webroot SecureAnywhere Web Security Service can enforce policies regardless of an employee's location—at home, in the airport, or in a café. Remote, off-network users are fully provisioned to receive automatic, uninterrupted policy-controlled protection even outside the corporate network. Because the service operates in the cloud, remote users authenticate directly, without needing to backhaul their web traffic through a VPN. Furthermore, intelligent split tunneling provides a constantly updated DWP cache of major safe sites that enables mobile users to visit approved sites directly. Finally, the guest network support option allows admins to set up guest network access via an IP-based group setting. All of these service capabilities drastically increase remote and mobile user management flexibility, improve productivity, and enhance security without sacrificing control.

Proactive Scan Ahead and Safe Search Integration

Webroot provides secure scan-ahead technology that examines all search engine queries and returns color-coded search results based on each user's individual internet access policy rules. This intelligent search feature helps users better understand their organization's internet usage policies and proactively mitigates threats by blocking access to harmful content.



Scan-ahead Safe Search Results

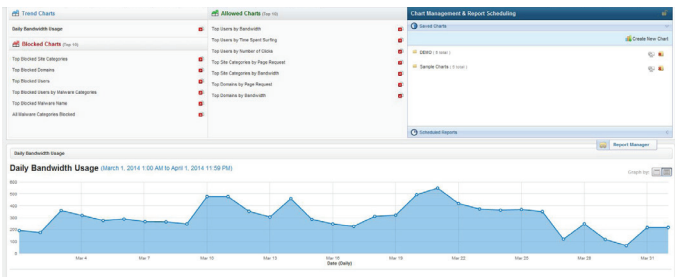
The Web Security Service can also be used in conjunction with the safe search browser feature to protect users from exposure to undesirable content, such as inappropriate thumbnail images.

MINIMIZED MANAGEMENT COMPLEXITY

Simplified Administration

Webroot provides secure scan-ahead technology that examines all search engine queries and returns color-coded search results based on each user's individual internet access policy rules. This intelligent search feature helps users better understand their organization's internet usage policies and proactively mitigates threats by blocking access to harmful content.

The Web Security Service can also be used in conjunction with the safe search browser feature to protect users from exposure to undesirable content, such as inappropriate thumbnail images.



Interactive Drill-down Reporting

Seamless Authentication – New Persistent Cookie Option

The Webroot DWP agent is lightweight and easy to deploy and manage. Once installed, it enforces seamless authentication and ensures all web traffic is automatically routed through Webroot SecureAnywhere Web Security Service. The DWP agent also handles more complex authentication at public Wi-Fi hotspots and other tricky access points, so remote users are always able to get online. Webroot also offers the persistent cookie option, which is ideal for guest networks and limits users to a one-time sign-on.

Comprehensive Logging and Reporting

Near real-time logs display the sites and downloads users have attempted to access, as well as whether these were acceptable under their web access policy. Webroot logs are available for 365 days, so access to historical log information for generating management reports remains at hand.

Detailed reports may be run ad hoc or on a scheduled basis, providing timely and accurate monitoring of internet usage. Reporting graphs include web traffic trends, top blocked URLs, blocked malware, bandwidth usage, and more. Administrators can easily set up scheduled reporting, as well as automatic distribution via email to chosen recipients. Numerous charts may be combined for maximum executive and management visibility into overall and individual internet usage.

Support for Citrix and Terminal Services Servers

The Web Security Service supports both Citrix and Terminal Services environments, as well as Windows systems. This extended platform support provides a convenient enhancement over other solutions. All Citrix and Terminal Services users are individually authenticated, so unique policies can be applied to separate users on a single Citrix or Terminal Services server, while user activity is logged individually.

Rapid Deployment

Deploying the Web Security Service is very straightforward, and requires no costly hardware or software. Using a Wizard UI, admins can quickly deploy the DWP agent using MSI via GPO and other methods. The DWP automatic user creation feature is enabled by default. It creates accounts for new users as they authenticate to the service for the first time from associated IP addresses and places them into a policy group for easy administration. All necessary credentials are stored in the local registry, so multiple users can share a machine and still maintain the correct policy restrictions, while logins are seamless and transparent. Once installed, DWP reconfigures all local browsers to use the correct proxy address, ensuring security and compliance.

Note: DWP is currently only available for the Windows operating system.

Fast Browsing with Minimal Latency

The Webroot SecureAnywhere Web Security Service uses a globally distributed, multitenant, fully redundant data center infrastructure served through global server load balancing (GSLB) to minimize latency. By using GSLB to automatically route users' web traffic through the nearest data center, Webroot ensures performance and rapid browser request response times. In addition, our propriety and unique web content download acceleration technology, combined with high-performance proxies, further improves user experience and ensures policy compliance.

Key Benefits	Key Features
Reduced Total Cost of Ownership (TCO)	» No management hardware or software to support » Low ongoing administration overheads » No switching fees, or other up-front costs » Pay-as-you-go, per user/per year, subscription model
Proactive Web Security	» Stops web malware before it reaches network or users » Multiple security layers protect against unknown threats and attacks » Real-time integration with BrightCloud Threat Intelligence » Smart URL filtering and content blocking with Social Network controls » Smart and unique real-time anti-phishing protection » Smart auto-detection of anonymizing proxy circumvention » Zombie detection and blocking
Easy to Manage	» Intuitive cloud-based management console » Internet access by account, group, or user level » Full AD and LDAP integration for smarter use management » Detailed ad hoc and scheduled reporting » Support for Citrix and Terminal Services » Auto-updating Desktop Web Proxy (DWP) agent
Reliable Service	» Fault-tolerant data centers eliminate single point-of-failure risks » Seamless authentication and protection for remote users » Webroot is a global IT security leader » Comprehensive 24x7x365 web and telephone based support included

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at www.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