No Hardware. No Software. No Malware.

Today’s criminals generate over 40,000 malware samples a day. Webroot® Web Security Service provides better protection by blocking threats before they reach your network. You can easily protect mobile users, enforce Internet use policies, track web trends, and detect software vulnerabilities—a unique feature not offered by any other software as a service solution. And with no hardware or software to manage, your IT team saves time and money.

**WHAT’S NEW: Vulnerability Scanning & Spyware Detection**

*Extra protection only offered by Webroot Web Security Service*

- Find holes in your security before an attacker does
- Quickly identify software & operating system vulnerabilities
- Gain visibility into spyware infections
- Reduce risk without buying & managing a separate vulnerability scanner
- Prevent data breaches and theft

**Webroot Web Security Service**

<table>
<thead>
<tr>
<th>Key Benefits</th>
<th>Key Features</th>
</tr>
</thead>
</table>
| **Reduced Total Cost of Ownership (TCO)** | • No hardware or software to purchase & maintain  
• Lower administration overhead  
• No switching fees or other upfront costs  
• Pay-as-you-go subscription model |
| **Proactive Web Security** | • Stop known & unknown virus, phishing & malware attacks before they reach your network  
• Multiple heuristic filters protect against zero-hour attacks  
• Integrated antispyware protection provided by award-winning Webroot Spy Sweeper® technology  
• URL filtering & file/content type blocking prevent unwanted content  
• Automatic detection of anonymising proxy sites to enforce company security & Internet use policies |
| **Easy to Manage** | • Intuitive Web-based management console  
• Set Internet use policies according to group or user level  
• Import & configure users through LDAP integration  
• Detailed real-time & scheduled reporting  
• Support for Citrix & Terminal Services  
• Automatic updates to client Desktop Web Proxy (DWP) |
| **Reliable Service** | • Service Level Agreements (SLAs) ensure uptime & performance  
• Fault-tolerant data centres eliminate single point-of-failure risk  
• Seamless authentication & protection for mobile laptop users  
• Service, security & support is provided by a global security leader |

**Customer Environment**

**Webroot Global Data Center Network**

- **Webroot Security Service**
- **Threat Protection**
  - Antivirus
  - Antispyware
  - Antiphishing
- **Data Security**
  - Outbound Content Filtering/DLP
  - APP Control
- **Policy Enforcement**
  - Web Access Control
  - Mobile User Protection
- **Compliance**
  - Policy Engine
  - User Reporting/Logging

**Internet**

**WEB TRAFFIC**
Service Management
Simplified Administration
Manage company Internet use and security policies via an intuitive web-based management console. Administrators can securely access Webroot’s powerful rules engine to facilitate user, group and account level access policies. A real-time Web traffic summary dashboard displays company Web site access by category and popular search terms. The Desktop Web Proxy (DWP) allows for seamless authentication into the service for mobile and on-site users, and it can be automatically updated to the latest version.

Real-Time Logging and Reporting
Real-time logs display which sites and downloads users have attempted to access and whether or not they were allowed. With logs accessible for 90 days, administrators can access the historical information they need to generate key metrics. Detailed reports can be run ad-hoc or scheduled, allowing companies to accurately monitor Internet use by viewing graphs on Web traffic trends, top blocked URLs, blocked malware, bandwidth use and more. Scheduled reports can be set up to be distributed via email to a user, or a list of users, and can contain up to 100 separate charts for maximum visibility into company and user Internet use.

Support for Citrix and Terminal Services
Webroot is the only Web Security Service that provides support for Citrix and Terminal Services. This convenient feature further enhances usability and management. All Citrix or Terminal Services users are individually authenticated. Unique policies can be applied to separate users on a single Citrix or Terminal Services server with user activity logged individually.

Fast Deployment and Guaranteed Service Availability
Customer deployment can typically be complete in less than one week and there are no costly hardware, software, or equipment maintenance fees. Webroot also guarantees 99.99% service availability to ensure that customers have consistent, reliable access to a secure web communications environment.

Threat Protection
Antivirus, Antispyware and Antiphishing
Webroot Web Security Service scans all HTTP and FTP over HTTP requests for malware in the cloud, blocking threats before they ever reach a company’s network. Best-of-breed antivirus protection guarantees defence against 100% of known virus threats, and multiple zero-hour heuristic filters protect against new and unknown virus variants. Antispyware protection is powered by the industry’s leading antispyware engine, Webroot Spy Sweeper, which protects over 10 million desktops worldwide. Antiphishing detection uses advanced heuristics to identify phishing sites in real-time, ensuring sensitive personal and corporate data remains secure. For complete security, downloaded JavaScript and shellcode is inspected for malicious content/actions in real-time, preventing end-users from becoming infected.

NEW! Vulnerability Scanning and Spyware Detection
Reduce risk by identifying holes in your security before attackers do. Exclusively offered by Webroot Web Security Service, this powerful feature eliminates the need to purchase and manage a separate vulnerability scanner. You can scan endpoints directly from Webroot’s Desktop Web Proxy (DWP) to identify known system vulnerabilities including operating systems, browser versions, and other installed software, as well as spyware infections. View results within the Management Portal to facilitate remediation.

Proactive Safe Searching Capabilities
Webroot provides a unique “Scan Ahead” technology that examines all search engine queries and returns color-coded search page results based on the requestor’s Internet access policy. This feature not only helps enforce Internet use policy, but it also proactively mitigates Internet threats and harmful content. In addition to Scan Ahead, inappropriate thumbnail images are blocked from search engine results by enforcing the Safe Search feature in search engines, protecting users from exposure to inappropriate content.

Fast Browsing with Minimal Latency
Maintain a fast browsing experience and ensure a seamless Internet experience for your users. Webroot’s distributed architecture minimizes latency by maintaining multi-tenant, fully redundant datacenters around the globe. Global Server Load Balancing (GSLB) automatically routes Web traffic through the nearest datacenter, ensuring rapid response time. Unique Web content download acceleration and proprietary high-performance proxies further improve performance and ensure immediate policy compliance.
Internet Policy Enforcement
URL and Web Content Filtering
Web content filtering enables companies to enforce Internet use policies, mitigate data loss, protect users from inappropriate content and improve productivity. Webroot filters Web content based on site URL, Web application, attachment type, MIME type, file type and file size. Millions of URLs are categorized into 12 main categories and 96 subcategories. This database is continuously updated to ensure accurate and advanced control. Content filtering also includes the ability to block advertisements.

Internet Access Control
Internet access policies can be set according to group or individual user level and applied by time and location. Administrators can also set Web site access to be “Allowed,” “Blocked” or “Coached” in order to help inform users and manage Internet use. For even greater filtering control, Webroot provides the ability to create customized URL “Allow” and “Deny” lists. Anonymizing proxy detection enforces company Internet use policies even when users attempt to access blocked pages through common or custom anonymizing proxy sites.

Quota Policy Support
Administrators can easily support and enforce Internet use policies by placing limits on bandwidth consumption, time spent online and number of sites accessed. To help monitor and track Internet use, logs and reports are available to track factors such as daily bandwidth consumed by user and time spent surfing.

Roaming User Protection
As an integrated component of the service, Webroot Web Security Service provides seamless enforcement of company Internet use policies regardless of where an employee is working — whether it’s at home, the airport, a hotel or an Internet café. Mobile laptop users can be easily configured to receive automatic and uninterrupted protection even while they are outside their organization’s network. Because the Webroot service sits in the cloud, these laptop users can authenticate directly with the service rather than establishing a VPN connection to the corporate network. This roaming user protection helps to improve employee productivity, enhance network security and reduce costs.

Why Webroot?
Webroot is a global company with a history of delivering innovative security solutions to millions of businesses and consumers. Our best-of-breed technology has won numerous awards and our SaaS solutions protect over three million users worldwide. As one of the largest privately held companies in the Security SaaS market, Webroot has multiple data centres and support offices across the US, Europe, Japan and Australia. To guarantee the highest level of service, all Webroot Security Services are backed by local technical support teams and Service Level Agreements (SLAs) that are among the best in the business.

See the benefits for yourself!
To schedule a free trial or demo, call 866.915.3208, or visit www.webroot.com/business.