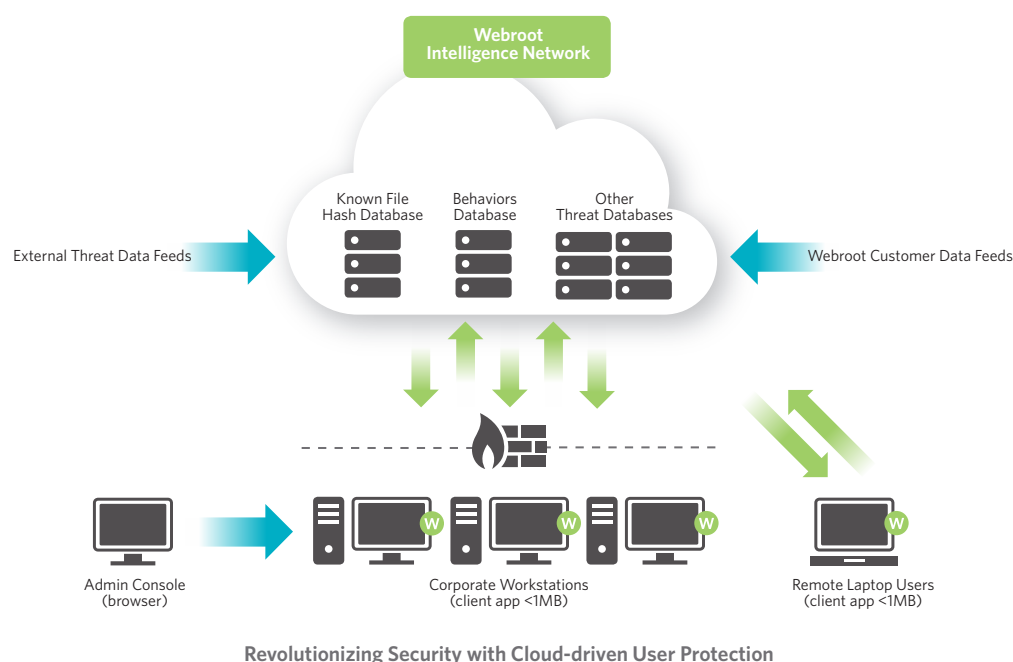# Webroot® SecureAnywhere™—Endpoint Protection

Revolutionary Security. Ultimate Performance. Minimal Management.

OVERVIEW

Webroot® SecureAnywhere™—Endpoint Protection offers a revolutionary approach to endpoint malware protection. It brings together Webroot's innovative file pattern and behavior recognition technology with the power of cloud computing to stop known threats and prevent unknown zero-day attacks more effectively than anyone else.

Using the world's lightest and fastest endpoint security client, scans are unbelievably fast—normally less than two minutes*—and they don't slow down your end-users. And because the technology is truly real-time, your security is always up-to-date, providing protection against all the latest threats and attacks without the hassle of managing signature file updates.

Webroot Intelligence Network

Known File Hash Database Behaviors Database Other Threat Databases

External Threat Data Feeds Webroot Customer Data Feeds

Admin Console (browser) Corporate Workstations (client app <1MB) Remote Laptop Users (client app <1MB)

Revolutionizing Security with Cloud-driven User Protection

FAST FACTS

Best protection against known and unknown malware

- Revolutionary file pattern and behavior recognition technology
- Recognizes if PC activity is benign or malicious
- Virtually eliminates the window of vulnerability for new threats

Extremely fast and easy to deploy

- World's smallest endpoint security client/agent (<1MB)
- Typically takes <6 seconds to install*
- Works alongside other security or software applications

Doesn't slow down PCs or hinder user productivity

- Initial scan takes <2 minutes, subsequent scans <1 minute*
- Minimal CPU usage during scans
- Sophisticated remediation eliminates system reimaging

Always up-to-date and protected

- No large daily update files stealing network bandwidth
- Off-network users remain protected and never need updates
- All users are instantly protected against any new threats

Easy to manage

- Centralized management of all endpoints
- Highly automated security management and reporting
- No on-premise management of server hardware and software

Online and offline protection

- Separate user policy controls for offline endpoint usage management
- Ability to lock down ports and devices such as USB, CD and DVD drives

*PassMark Software, "Webroot SecureAnywhere vs. Traditional Anti-virus, September 2011"

KEY BENEFITS

Revolutionary Security

Webroot's revolutionary cloud security removes the window of vulnerability that exists with other endpoint security solutions to deliver true real-time protection against all types of malicious threats.

- Virtually eliminates the vulnerability exposure time between when an exploit is released to when it's detected and ready to be removed.
- Unique file pattern and behavior recognition technology understands if PC activity is benign or malicious.
- Almost instantly checks files against the Webroot® Intelligence Network, a cloud database containing hundreds of millions of file and execution behaviors, to track and understand executable intent.
- Advanced threat intelligence determines known threats versus those that have never been seen before, protecting PCs against all known, new, and zero-day threats.
- Offline protection secures endpoints, that are not connected to the Internet. Offers powerful file heuristics and the ability to lock down ports and devices such as USB, CD and DVD drives.
- The Webroot Intelligence Network constantly collects information on new and potentially malicious files from across the Internet and Webroot customers, sharing it instantly to ensure up-to-the-minute protection.

Ultimate Performance

Webroot SecureAnywhere sets new standards in deployment, scan speeds, system resource usage, and endpoint footprint, ultimately saving you more time and money.

- Ultra-light client—the world's smallest at less than 1MB.
- Downloads, deploys, and installs in six seconds.
- Operates using minimal CPU usage to prevent slowing down end-users.
- Minimal disk space required—no local threat database is needed.
- Lightning-fast scans take under two minutes*, compared to hours for many other security solutions.
- Improved PC performance with minimal system requirements.
- Can coexist with other security products, eliminating the need to uninstall existing solutions prior to migration.
- Maximizes security and productivity by not getting in the way.

*After the initial PC scan, full system scans will typically take two minutes or less.

Minimal Management

A web-based management console lets you easily manage end-user policies via an intuitive interface. The console provides full management of all your endpoints, including the ability to centrally create and administer endpoint security policies, view detailed service reports and logs, and manage whitelists, blacklists, and file overrides. Other advantages include:

- No management server hardware or software to purchase, install, or maintain.
- Pre-configured and default policy templates.
- Easily configurable administrator alerts and notifications.
- Both online, ad-hoc, and scheduled reporting using real-time logs.
- Automatic threat definition and software updates occurring in the cloud.
- Automatic client software updates with no bandwidth or performance impacts.

KEY FEATURES

Powerful Malware Detection Provides the most advanced real-time endpoint protection against both known and unknown malware to virtually eliminate the vulnerability window between when threats emerge and when they're detected.

Offline Protection Stops attacks when an endpoint is offline with separate file execution policies applicable to local disk, USB, CD, and DVD drives. Also includes ability to lock down devices and ports.

Powerful Heuristics Heuristic settings can be adjusted based on risk tolerance for file execution. Heuristic settings include:

- *Advanced*—Analyzes new programs for suspicious actions that are typical of malware.
- *Age*—Analyzes new programs based on the time a similar file has existed within the Webroot community.
- *Popularity*—Analyzes new programs based on how often file is used or changed within the Webroot community.

Malware Remediation Comprehensive detection and removal engine identifies known and unknown threats, including dangerous rootkits and other pieces of malicious software, and removes these files from users' systems.

Remediation Rollback A fail-safe rollback feature provides the ability to restore any program, as well as roll back cleanup processes to a previous state.

Webroot® Intelligence Network Real-time threat detection and analysis via the world's largest cloud database of unique extractable objects, consisting of over 250 million files and associated file behavioral characteristics.

Instant Deployment Deploys via a packaged MSI installation file, custom deployment tool, or link to download the executable.

Software Compatibility Compatible with other software applications, including other endpoint security solutions, making deployment alongside existing applications very easy.

Integration with Webroot® SecureAnywhere™— Web Security For layered protection against web threats, seamlessly add Webroot SecureAnywhere—Web Security. The service lets you transparently route all user web traffic to easily set and enforce acceptable Internet usage and security policies. Covers on-premise workstations as well as roaming laptop users and leverages the same Webroot account management portal.

Endpoint Firewall Supplements the native Windows firewall for inbound and outbound protection to protect against "phone-home" connections from infected endpoints as well as potential botnet traffic.

System Monitoring/Application Control Advanced system-monitoring tools provide the ability to view active endpoint processes, active process durations, as well as ability to whitelist or blacklist applications.

SafeStart Sandbox Unknown files may be designated to only open within a protected sandbox for evaluation of behaviors. This ensures unwanted applications and files never infect users' systems.

Server and Virtual Server Support In addition to supporting physical Windows PC environments, Webroot SecureAnywhere can also support Windows server and virtual server environments.

Resilient Distributed Cloud Architecture Consists of multiple global datacenters to support local offices and roaming users through their nearest datacenter and provide excellent resilience and redundancy.

SYSTEM REQUIREMENTS

Management Portal Access:
- Internet Explorer® version 7, 8, and 9
- Mozilla® Firefox® version 3.6, and 4.0
- Chrome 11 and 12
- Safari 5
- Opera 11

Supported PC Platforms:
- Windows® XP Service Pack 2 and 3, 32-and 64-bit
- Windows Vista®, 32- and 64-bit
- Windows 7, 32- and 64-bit

Supported Server Platforms:
- Windows Server 2003 Standard, Enterprise, 32and 64-bit
- Windows Server 2008 R2 Foundation, Standard, Enterprise
- Windows Small Business Server 2008 and 2011

Supported Virtual Server Platforms:
- VMware vSphere 4 (ESX/ESXi3.0, 3.5, 4.0, 4.1, Workstation 6.5, 7.0, Server 1.0, 2.0
- Citrix XenDesktop 5 and XenServer 5.0, 5.5

About Webroot

Webroot is committed to taking the misery out of Internet security for businesses and consumers. Founded in 1997, privately held Webroot is headquartered in Colorado and employs approximately 450 people globally in operations across North America, Europe and the Asia Pacific region. For more information visit www.webroot.com.

Webroot Headquarters

385 Interlocken Crescent, Suite 800
Broomfield, Colorado 80021 USA
800 772 9383

Next steps:
Talk to an enterprise product expert by calling 866 254 5914