Webroot® Business Endpoint Protection

Intuitive, automated cybersecurity that helps businesses become more resilient

Overview

Today, businesses of all sizes are under constant attack. While some attacks are opportunistic, automated, and indiscriminate in nature, many are highly targeted, invasive, and precise. With the variety, volume, and velocity of attacks, it's never been more critical to use an effective, broad-spectrum endpoint security that works in conjunction with other defenses to stop malware, ransomware, phishing, cryptomining and the other damaging attacks aimed at your users and systems.

The security challenges businesses of all sizes face are the same: reduce complexity, integrate solutions into existing tools, help solve the problem of the highly variable security skills administrators have at their disposal, and ultimately become more resilient in the face of cyberattacks.

Webroot® Business Endpoint Protection solves these problems and more by delivering an award-winning[1] intuitive management console, over 40 third party integrations, a RESTful API, plus fully automated endpoint detection, prevention, protection, and remediation for a comprehensive cyber resilience strategy. It uniquely harnesses the power of cloud computing and real-time machine learning to continuously monitor and adapt each individual system's endpoint defenses to the unique threats that system and user faces.

By taking a patented proactive, predictive, and multi-layered approach to security, Webroot Business Endpoint Protection offers highly effective defenses against today's cyber threats.

Webroot's Unique Approach

Webroot® Business Endpoint Protection is diametrically different from other endpoint security solutions. As a software-as-a-service (SaaS), cloud-driven endpoint security solution, it offers a variety of benefits, including:

Hassle-free deployment

The small (<5MB) agent takes an average of 3 seconds to install[2] and is designed not to conflict with other security software. This compatibility makes deploying Webroot and replacing legacy security software much faster and easier than with other solutions, as admins no longer need to worry about impacting user productivity to roll out effective endpoint security.

Fully remote endpoint management and control

Our cloud-based management console gives you visibility and control over any device with the Webroot agent installed. You can manage multiple sites and locations and leverage powerful remote agent commands. There is no on-premises server management and the console also lets you easily trial, deploy, and manage other Webroot solutions like Webroot® DNS Protection and Webroot® Security Awareness Training, should you so wish.

Highly automated, low-cost operation

Webroot® Business Endpoint Protection was built from the ground up to be easy to deploy, manage, and maintain. You can take advantage of granular pre-configured policy templates or, easily modify them to create your own. There are never any signatures or definitions to update as threat prevention occurs in real time from the cloud. Webroot agent updates are automated, typically taking 3 seconds[2] while being completely transparent to the user. Infection alerting and remediation are automated, while regular reporting is scheduled for content, timing, and circulation. These qualities result ensure very low operational cost.

Protection online and off

Webroot uses propriety technology to monitor, journal, and contain infections even when an endpoint is offline. System and user data is protected offline too. Rather than using Windows® Volume Shadow Copy, which may be compromised by malware, Webroot protection uses a patented approach to preserving device data and protect the local host drive from being compromised or needing reimaging.

Independently benchmarked low system overheads

A key benefit of our cloud-driven approach is that the intense processing of malware discovery and analysis is performed in the cloud. Independent testing by PassMark Software shows Webroot protection has the lightest overall system resource usage among leading competitor products.[2] Full scheduled scans are transparent to users and system CPU and RAM usage are lightweight and don't hog resources.

Innovative detection technology

Unlike traditional approaches, which only have one opportunity to detect and stop a threat, next-generation Webroot protection works in multiple stages. First, it looks to predictively prevent malware from infiltrating the system. Then, it works to prevent malware and unknown files from executing if they display malicious behavior. Then, if a previously-unknown file (i.e. potential infection) does execute, Webroot protection monitors and journals the file's activity until it can classify it appropriately. If the file is deemed a threat, any changes it made to local drives are automatically rolled back to their pre-infected state. Not only is this multi-stage strategy more effective against modern threats, but it also reduces the chance of false positives.

Powered by world-class real-time threat intelligence

All Webroot solutions are backed by the Webroot® Platform, which integrates the same global Webroot BrightCloud® Threat Intelligence trusted by more than 100 network, security, and technology vendors to enhance the security of their products and services. Our 6th-generation machine learning architecture processes over half a trillion threat objects per day from a variety of vetted sources, as well as tens of millions of real-world customer endpoints, allowing us to generate around 1,000 new or revised machine learning models per day to help customers and partners all over the world achieve cyber resilience.

Webroot® Business Endpoint Protection at a Glance

» **Secure and resilient distributed cloud architecture** – Uses multiple secure data centers globally to support customers and roaming users with full-service resilience and redundancy.

» **Layered user and device defenses** – Stops attacks that take advantage of poor user awareness, not just those that target device vulnerabilities.

» **Malware detection and prevention** – Blocks viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, script-based, and fileless attacks, and a wide range of other threats.

» **Multi-shield protection** – Webroot's multi-shield protection includes Real-Time, Behavior, Core System, Web Threat, Identity, Phishing, Evasion, and Offline shields for detection, prevention and protection from complex attacks.

» **Malicious script protection** – Patented Webroot® Evasion Shield technology detects, blocks, and remediates (quarantines) evasive script attacks, whether they are file-based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing in PowerShell, JavaScript, and VBScript.

» **User identity and privacy protection** – The Identity Shield (browser and application isolation) is trusted by the world's leading banks to stop attacks like DNS poisoning, keylogging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software.

» **White and blacklisting** – Offers direct control over application execution.

» **Intelligent firewall** – The system-monitoring and application-aware outbound firewall augments the built-in Windows® firewall to protect users both on and off corporate networks.

» **Infrared dynamic risk prevention** – Analyzes individual user behavior to dynamically tailor malware prevention heuristics.

» **Powerful heuristics** – Lets admins adjust heuristic detection based on risk tolerance for file execution.

» **Full offline protection** – Stops attacks even when offline and enables admins to create separate file execution policies for local disk, USB, CD, and DVD drives.

» **Multi OS, virtualization, terminal server, and Citrix support** – Supports MacOS® devices, Windows® computers and servers, virtualization, terminal server, and Citrix environments.

» **Multi-language support** – The installed agent supports 13 languages.

» **Free, award-winning telephone support** – Our in-house support team is standing by to resolve issues with a 95% customer satisfaction rate.

» **Transparent usage and billing** –Webroot My Usage and My Billing portals within the management console make tracking and payment transparent.

What Results to Expect

Webroot® Business Endpoint Protection helps businesses achieve cyber resilience by delivering advanced protection against the ever-increasing and evolving onslaught of modern attacks. Its highly automated and effective endpoint security means you no longer need dedicated IT security resources or experts on hand to ensure the digital fitness of your business. And, with fewer infections and security-related incidents—not to mention fewer remediation cases and productivity losses—admins can focus on what matters most: being successful.

Trial and Next Steps

For more information, contact your Webroot Account Manager or our sales department. Visit webroot.com to initiate a FREE 30-day trial. Existing Webroot customers can also start trials directly via the Webroot management console.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and 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

[1] G2.com. "Usability Index for Endpoint Protection Suites" (Fall 2019)

[2] PassMark Software. "Webroot SecureAnywhere® Business Endpoint Protection vs. Eight Competitors." (March 2019)