WEBROOT
an opentext company

Webroot Business Endpoint Protection

Advanced Detection and Protection Against Malware, Ransomware, Phishing, and More

Overview

According to a cyber-readiness survey[1] published by Hiscox, small businesses with under 50 employees face almost the same rates of attack as a 20,000-employee enterprise. Today, businesses of all sizes are under constant attack from cybercriminals and others using multiple attack vectors to steal credentials, bypass defenses, and infect devices, servers, and more.

While some threats are opportunistic, automated, and indiscriminate in nature, many are now highly targeted, invasive, and precise. With the variety, volume, and velocity of attacks, it's never been more critical to use effective, broad-spectrum endpoint security that can stop today's malware, ransomware, phishing, cryptomining and other damaging attacks by protecting both users and their devices.

Webroot® Business Endpoint Protection is a next-generation, cloud-based, endpoint security solution that harnesses the power of real-time machine learning to continuously monitor and adapt each endpoint's threat detection, protection, and prevention. It defends both physical and virtual devices and their users against modern, multi-vector threats. And, by taking a real-time proactive, predictive, and multi-layered approach to protection and prevention, it offers a significantly more effective method than more reactive endpoint security solutions.

The Webroot Approach

Webroot® Business Endpoint Protection is very different from other endpoint security solutions. It is truly a software-as-a-service (SaaS), cloud-driven endpoint security solution that offers many unique operational benefits, including:

Hassle-free deployment

The small but powerful software agent needs only an average of 3 seconds to install[2] and won't conflict with existing security software. This means trials, new deployments, and replacing legacy security software is now faster and easier. Now, you don't have to worry about impacting user productivity to roll out effective endpoint security.

Remote endpoint management

A single integrated management console gives administrators full security visibility and control over any device with the Webroot agent installed. Admins can manage multiple sites and locations, allocate different access permissions and admin rights, and leverage powerful remote agent commands—all from their online console. There's no on-premises management hardware or software to manage, and the console also lets admins trial, deploy, and manage Webroot® DNS Protection and Webroot® Security Awareness Training.

Automated operation

Webroot® Business Endpoint Protection was built from the ground up to be easy to deploy, manage, and maintain. Take advantage of granular, pre-configured policy templates or create your own. There are never any signatures or definitions to manage, as collective threat prediction, prevention, and protection occurs in real time from the cloud. Admins may also automate all Webroot agent updates, which typically take 3[2] seconds and are completely transparent to the user. Infection alerting and remediation are automated, while regular reporting is easy to schedule for content, timing, and circulation.

On- and offline protection and auto-remediation

Webroot uses propriety technology to monitor, journal, and contain potential infections even when an endpoint is offline. So, as soon as an endpoint reconnects to the internet, any threats are easily remediated. Data is protected too. Rather than using Windows Volume Shadow Copy, which may be compromised by malware, Webroot uses a patented approach to preserving device data and monitoring system changes. This ensures that, if an endpoint's local host drive is compromised, it can be automatically restored to its uninfected state without reimaging.

User transparency and low system overheads

A key advantage of a cloud-driven, real-time security approach is that the heavy processing associated with machine learning and malware discovery is performed in the cloud, not on the user's device. That means full scheduled scans, agent updates, user impact, and resource usage (CPU and RAM) are extremely low. Except for block notifications when users attempt to navigate to a malicious or suspicious site, most users will not know Webroot Endpoint Protection is running.

Innovative technology

Unlike traditional antivirus, which only have one opportunity to detect and stop a threat, Webroot protection works in multiple stages. First, it attempts to prevent malware from infiltrating the system. If malware does get through, Webroot protection works to stop it before it can execute. Should it execute (this might happen in cases of brand-new, never-before-seen malware), Webroot protection will journal the file's activities and undo its changes to local host drives once it's determined to be malware.

Powered by world-class threat intelligence

Webroot's threat intelligence platform and BrightCloud services back all our solutions, and our threat intelligence is trusted by over 100 network and security vendors worldwide to enhance their own solutions. Webroot has used machine learning to classify and categorize threats since 2007. Our advanced, 6th-generation machine learning architecture processes threat data from a variety of vetted sources as well as millions of real-world customers and users of our technology partners' solutions.

Webroot® Business Endpoint Protection at a Glance

- **Secure and resilient distributed cloud architecture** – We use multiple secure global data centers to support customers and roaming users globally with full-service resilience and redundancy.
- **Layered user and device defenses** – Stop attacks that take advantage of poor user awareness, not just those that target device vulnerabilities.
- **Malware detection, prevention, and protection** – Prevent viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, and wide range of other endpoint threat vectors.
- **Multi-shield protection** – Endpoint Protection includes the following shields for predictive protection against zero-day threats: Real-Time, Behavior, Core System, Web Threat, Identity, Phishing, and Offline.
- **User Identity and Privacy** – The Identity Shield component of our endpoint protection is trusted by the world's leading banks to stop online banking-related attacks, including DNS poisoning, keystroke logging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software.
- **White and blacklisting** – Admins have direct control over which applications can execute.
- **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** – This feature analyzes individual user behavior to dynamically tailor malware prevention.
- **Powerful heuristics** – Admins can adjust these based on risk tolerance for file execution.
- **Full offline protection** – Stop attacks when offline or create separate file execution policies for local disk, USB, CD, and DVD drives.
- **Multi OS, virtualization, terminal server, and Citrix support** –Endpoint Protection supports MacOS® devices, Windows® computers and servers, as well as virtualization, terminal server, and Citrix environments.
- **Multi-language support** – The Webroot software agent supports over 13 languages.
- **Free telephone support** – The award-winning in-house Webroot support team is standing by.
- **Transparent Usage and Billing** – Whether for internal or external client billing, the Webroot My Usage and My Billing portals within the management console make tracking and payment transparent to all.

What Results to Expect

Webroot® Business Endpoint Protection delivers advanced prediction, detection, protection, and prevention against the ever-increasing number of attacks faced by today's businesses. With such a highly automated and effective endpoint security solution, you no longer need dedicated security resources or experts on hand to be safe. And, with fewer infections and security-related incidents (not to mention fewer remediation cases and productivity losses), you can focus on what matters most: being successful and profitable.

Trial and Next Steps

For more information, contact your Webroot Account Manager, our sales department, or request a FREE 30-day trial at webroot.com. Existing Webroot customers can also access free trials directly via their management console.

About Webroot

Webroot, a Carbonite company, harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Webroot operates globally across North America, Europe, Australia and Asia. Discover Smarter Cybersecurity® solutions at 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] Hiscox. "2019 Cyber Readiness Report."
[2] PassMark Software. "Webroot SecureAnywhere® Business Endpoint Protection vs. Eight Competitors." (March 2019)