WEBROOT
Smarter Cybersecurity™

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 100 users or fewer now face the same risk of attack as a 20,000-employee enterprise. Businesses of all sizes are under constant attack from cybercriminals, who use multiple threats to steal credentials, bypass defenses and infect network devices, servers, computers, and more. Some threats are opportunistic, automated, and indiscriminate in nature, while others are highly targeted, invasive, and precise. With the variety, volume, and velocity of attacks that businesses experience today, it's never been more critical to deploy effective, broad-spectrum endpoint security that can detect and prevent today's malware, ransomware, phishing, crypto-threats, and other modern threats.

Webroot® Business Endpoint Protection was the first next-generation, fully cloud-based endpoint security solution to harness the power of machine learning to continuously monitor and adapt endpoint threat detection, protection, and prevention. It defends many different types of physical and virtual systems and their users against modern, multi-vector threats. By taking a predictive, adaptive, multi-layered approach to stopping attacks in real time, Webroot Business Endpoint Protection offers a faster and significantly more effective alternative to traditional business antivirus solutions.

The Webroot Approach

Webroot Business Endpoint Protection is very different from the other endpoint security solutions. As a software-as-a-service (SaaS), fully cloud-based driven endpoint security solution, it offers a variety of benefits.

Hassle-free deployment

The small but powerful software agent only needs 30 seconds to install[2] and won't conflict with existing security software. That means trials, brand new deployments, and even replacing legacy software are fast and easy, so you never have to worry about impacting user productivity to roll out security.

Fully remote endpoint management

The single integrated management console gives administrators full security visibility and control over any device with the software agent installed. Admins can manage multiple sites and locations, allocate different access permissions and admin rights, and leverage 40+ powerful agent commands—all from a single online console. There's no on-premises hardware to manage, and the same console also enables admins to initiate and manage trials and subscriptions to Webroot® DNS Protection and Webroot® Security Awareness Training.

Fully automated operation

Endpoint Protection was built from the ground up to be easy to deploy, manage, and maintain. Take advantage of pre-configured policy templates or create your own. There are never any signatures or definitions to manage; all protection occurs in real-time, from the cloud, without impacting the user's or admin's experience. Admins can also automate software agent updates, which typically take 5 seconds or fewer, and are transparent to the user. Alerting is automated and reporting can be scheduled 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 a given endpoint is offline. This reduces the number of false detections to nearly negligible levels. Instead of a Volume Shadow Copy, which can be compromised by attackers, Webroot uses a patented approach to preserving data and system changes. That means a compromised endpoint's local drives may be automatically restored to its uninfected state, without reimaging.

User transparency and low system overheads

A key advantage of a cloud-driven, real-time approach is that the heavy processing associated with machine learning and malware discovery is performed in the cloud, not on the client device. That means full scheduled scans, agent updates, user impact, and

resource usage (CPU and RAM) are extremely low. With the exception of block notifications when users attempt to navigate to a malicious or suspicious site, most users will hardly notice Webroot Business Endpoint Protection running.

Innovative technology

Unlike traditional antivirus, which only has one opportunity to detect and stop a given 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 drives, once it's determined to be malware.

Powered by world-class threat intelligence

Webroot threat intelligence and BrightCloud services back all Webroot protection solutions, and are trusted by 85+ network and security vendors worldwide to enhance their own solutions. Webroot has been using machine learning to classify and categorize threats since 2007. Our advanced 6th-generation machine learning architecture processes threat data sourced from a variety of vetted sources, as well as our own real-world customers and users of our technology partners' solutions.

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 threats.

» **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 in 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 are allowed to execute.

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

» **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 14 languages.

» **Free telephone support** – The award-winning in-house Webroot support team is standing by.

What Results to Expect

Webroot Business Endpoint Protection delivers advanced detection, protection, and prevention against the ever-increasing number of attacks small- to medium-sized businesses face. Because it's a highly automated and effective solution, businesses no longer need dedicated security resources or teams of experts on hand to stay safe. And with fewer infections and security-related incidents, not to mention fewer remediation cases and productivity losses, businesses can finally focus on what matters most: growing profitably.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.