Webroot SecureAnywhere® Business Endpoint Protection

Smarter malware prevention that solves the performance, dwell time visibility, and management issues of your endpoint security

OVERVIEW

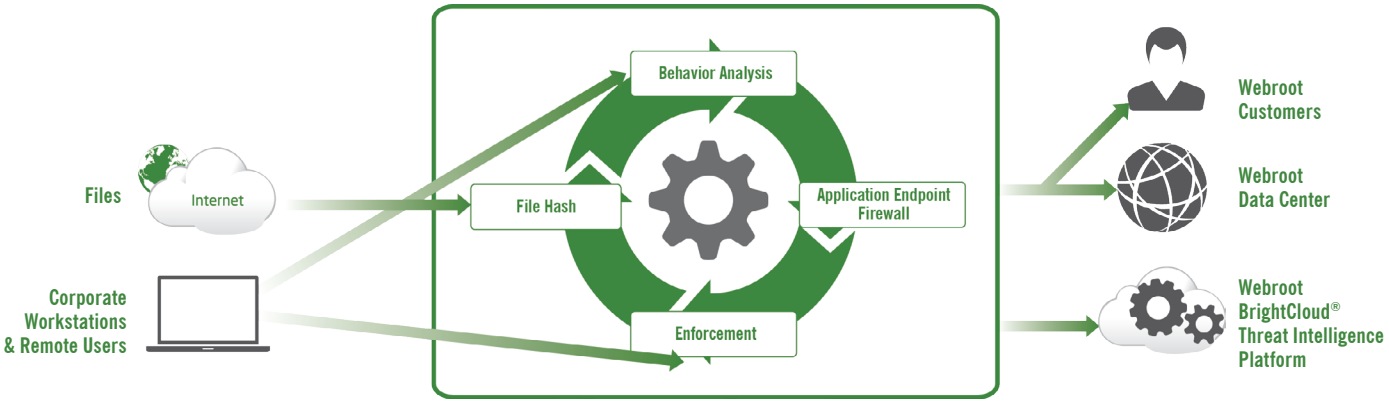
Confidence has never been so low in a key threat prevention technology: endpoint security. Conventional antivirus protection is struggling to keep up with today's threats and attacks. It slows down machines and users and is complex and resource-intensive.

Now, by combining innovative SecureAnywhere file pattern and predictive behavior recognition technology with the almost limitless processing power of cloud computing, Webroot effectively stops malware and zero-day threats at the moment of attack. The smarter, next-generation Webroot® approach to malware prevention is more effective and accountable than any conventional antivirus. You no longer need to rely on an outmoded detection model that is easily overwhelmed by today's malware—a model that yields unknown dwell times and doesn't alert on attacks until long after the infiltration has occured.

Traditional antivirus presents the hassle of ensuring every endpoint has the latest update. SecureAnywhere Business Endpoint Protection communicates with the cloud, which means there are no definition or signature updates to deploy and manage. As malware detection occurs continuously in real time, performance issues fade away. Scheduled systems scans are normally around 30 seconds[1] and never impact device performance. Virtual desktop and server environments, plus many embedded operating systems, also see improved performance.

The world's smallest and fastest endpoint security client makes deployment fast and easy. The SecureAnywhere antimalware agent happily coexists with other antivirus solutions, with no need to immediately rip and replace.

SecureAnywhere Business Endpoint Protection is a smarter way to solve malware prevention, endpoint security performance, management. It provides the protection you need without the demanding overhead of conventional antivirus.



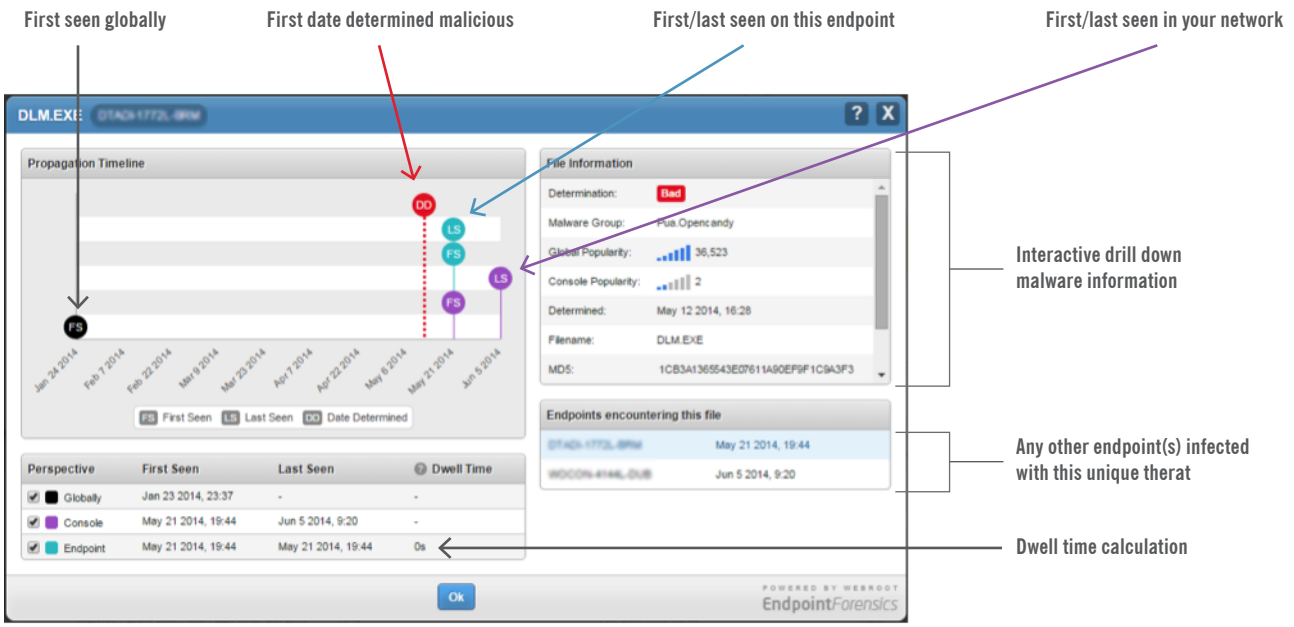
Uncovering zero-day malware

VISIBLE EFFICACY

A feature-rich endpoint protection solution amounts to nothing if it can't deliver its key feature: malware prevention. SecureAnywhere Business Endpoint Protection is the first malware prevention technology to report on its own efficacy at detecting infections and stopping malware. Dwell time reporting gives you visibility into any infection on any endpoint within your network, showing you when the infection began and how long it has taken Webroot to stop that threat.

Another factor contributing to the efficacy of SecureAnywhere Business Endpoint Protection is its continuous infection monitoring, journaling, and auto-remediation. If it cannot immediately categorize new or changed files and processes as 'known' good or 'known' bad, then the agent begins monitoring and journaling all events. If an observed process is categorized as malicious, then any system changes are reversed and the endpoint is auto-remediated to its last known good state. This extra layer ensures minimal false positives. If administrators wish to reclassify an application, they can easily do so via the cloud-based console.

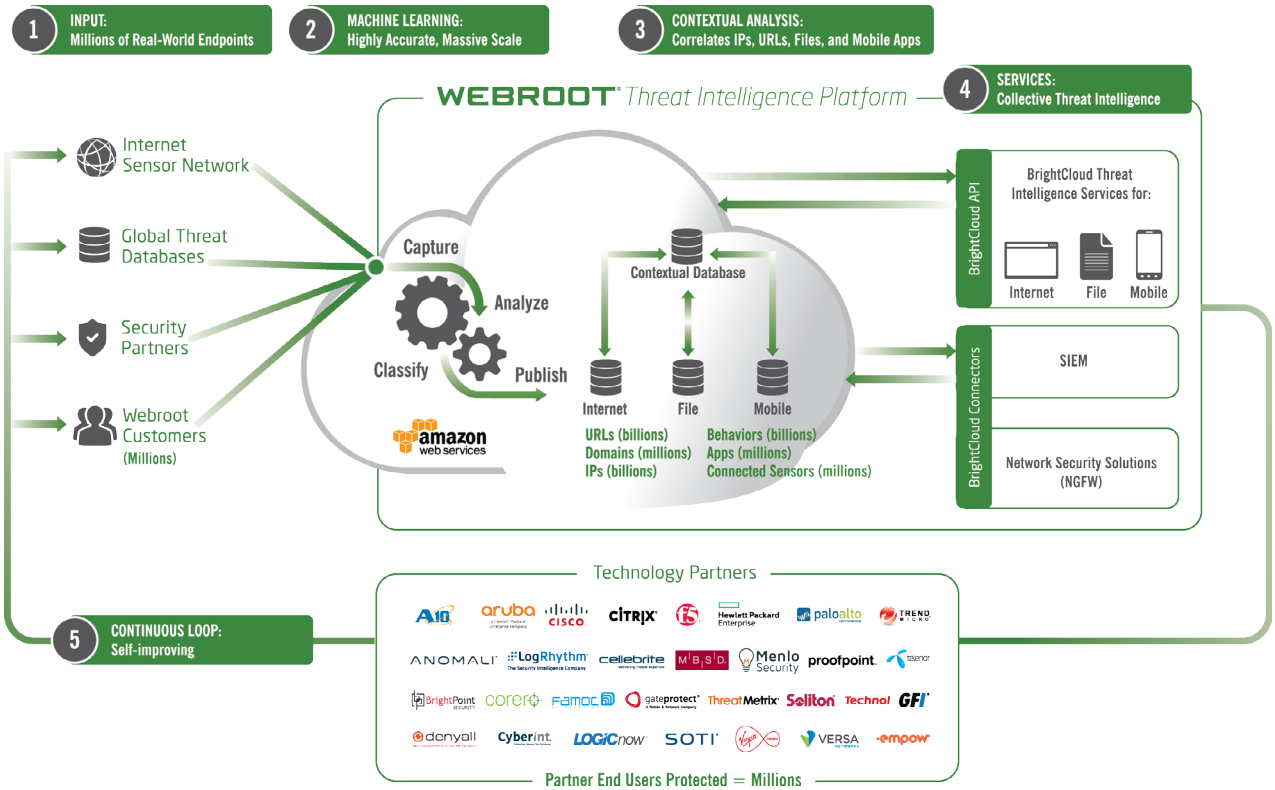
Endpoint Dwell Time Infection Visibility



FLEXIBLE CLOUD-BASED MANAGEMENT

Webroot SecureAnywhere solutions use cloud-based management, which means no on-premise hardware or software is needed and the console is always up to date. Webroot offers a standard console or our Global Site Manager console, so you can choose the management features appropriate to your organization's needs. The standard console is perfect for managing anything up to 1,000 endpoints with less complex user groupings and only a few different policy types. The Global Site Manager makes it straightforward to manage up to 100,000 endpoints, and, through its hierarchical management architecture, you can easily control multiple sites and locations. The Global Site Manager also supports policies at the global and individual site level, plus local site administration access rights and permissions that are easily managed alongside central administration of all sites.

This makes Global Site Manager ideal for global and or multi-location organizations, as well as Managed Services Providers (MSPs) administering numerous customer sites. Cloud-based management with full remote endpoint administration also makes the delivery of global management extraordinarily cost-effective compared to conventional antivirus.



The Webroot BrightCloud® Threat Intelligence Platform– the most powerful real-time threat analysis engine in the world

POWERING PREDICTIVE PREVENTION

All Webroot SecureAnywhere solutions are powered by the Webroot BrightCloud® Threat Intelligent Platform. Leveraging big data analytics and collective threat intelligence from our users and technology partners worldwide, the BrightCloud Threat Intelligent Platform identifies threats as they occur. This big data architecture continuously processes, analyzes, correlates and contextualizes vast amounts of disparate information while also applying a patented, fourth-generation machine learning and malicious code identification system to create predictive behavioral determinations on malware instantly – with incredibly high accuracy.

Big data processing allows SecureAnywhere Business Endpoint Protection to uncover malware as it attempts to infect an individual user's endpoint, while simultaneously protecting all other SecureAnywhere endpoints against the same attacks. This collective approach to threat intelligence creates a massive real-time malware detection net that has intimate knowledge of more than 300 million executables, including their runtime behavioral characteristics and interactions. This, coupled with another 200+ terabytes of threat data, ensures that Webroot customers are always protected from both existing and new threats.

KEY SECURITY FEATURES

Webroot SecureAnywhere Business Endpoint Protection focuses on delivering a high-performance endpoint malware prevention and management solution. It offers highly accurate and effective endpoint malware prevention with a range of additional security shield capabilities that keep both the user and the device safe.

Identity & Privacy Shield

These shields protect users by assuming the endpoint is already infected by some completely undetectable malware. They protect user information and transactional data that could be exposed during online transactions from specific types of threats, including phishing, DNS poisoning, keystroke logging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software mounting man-in-the-browser or man-in-the-middle attacks. The Sheilds lock down the OS and browser to protect all user information and credentials – even shared passwords. Aside from securing browser activities, the Identity Shield may be extended under user policy to cover other endpoint applications by adding them to the Identity Shield protection list, securing those applications.

Infrared

Infrared is a multi-layer defense incorporating several aspects of BrightCloud Threat Intelligence to help thwart threats early on in their lifecycle – often before a threat researcher sees a single sample. It looks at the reputation of the websites an individual visits and uses BrightCloud Threat Intelligence to determine their risk level. If the user commonly visits low-reputation websites, then the endpoint goes into a state of heightened awareness and closely interrogates any new files or processes that are introduced into their system. Infrared also interprets user behaviors and the overall safety level of the user. So, if a user is classified as "high risk", Webroot then dynamically tunes malware prevention to that user, while preventing false positives for less risky users.

Web Threat Shield

Our Web Threat Shield blocks access to known phishing sites and malicious domains by leveraging BrightCloud Threat Intelligence to access the latest security intelligence on any website.

Intelligent Outbound Firewall

In addition to its Shields, Webroot SecureAnywhere Business Endpoint Protection has its own intelligent system-monitoring and application-aware outbound firewall. This sophisticated firewall protects users both within and outside the corporate gateway, augmenting the Microsoft Windows® firewall to offer full control of outbound and inbound connections without adding an unnecessary drain on endpoint resources. It manages and monitors all outbound traffic to protect against "phone-home" threats and ensures that only policy-approved applications communicate with the network. It also automatically recognizes known good and bad programs, so users aren't pestered with pop-ups or forced to make uninformed judgments.

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 BrightCloud Threat Intelligence
- **Popularity** – Analyzes new programs based on how often a file is used or changed within BrightCloud Threat Intelligence

Offline Protection

Stops attacks when an endpoint is offline with separate file execution policies applicable to local disk, USB, CD, and DVD drives.

Virtualization, Terminal Server & Citrix Support

In addition to supporting Windows PC environments, SecureAnywhere Business Endpoint Protection also supports Windows Server, Virtualization, Terminal Server and Citrix environments.

Mobile Smartphone and Tablet Support

Webroot SecureAnywhere® Business Mobile Protection is available for Android™ and iOS® smartphones and tablets.

Resilient Distributed Cloud Architecture

Consists of multiple secure global data centers to support local offices and roaming users through their nearest data center, providing full service resilience and redundancy.