Webroot SecureAnywhere® Business Endpoint Protection

Multi-vector protection that secures endpoints and users across all stages of a cyberattack

Overview

Modern threats use multiple vectors to attack, from malicious email attachments to infected web ads to phishing sites. Criminals combine a range of threat technologies, deployed in numerous stages to infect computers and networks. This blended approach increases the likelihood of success, the speed of contagion, and the severity of damage.

Multi-vector attacks are designed to exploit the blind spots of signature-based security, allowing malware to infiltrate systems undetected. Unfortunately, even modern endpoint solutions still rely—at least in part—on signature-based detection models. This approach only protects end users once the threat is known, and after the vendor has created a signature and it has been updated on the endpoint, which is often too late.

Even newer, so-called "next-generation" endpoint solutions, which are typically more effective than their traditional competitors, are ill-equipped to fight modern attacks, as many only protect endpoints at the infection stage, and only across a single vector.

The only way to stop zero-day threats is with multi-vector endpoint protection that can secure users and their devices at every stage of an attack, across every possible attack vector.

The SecureAnywhere® Difference

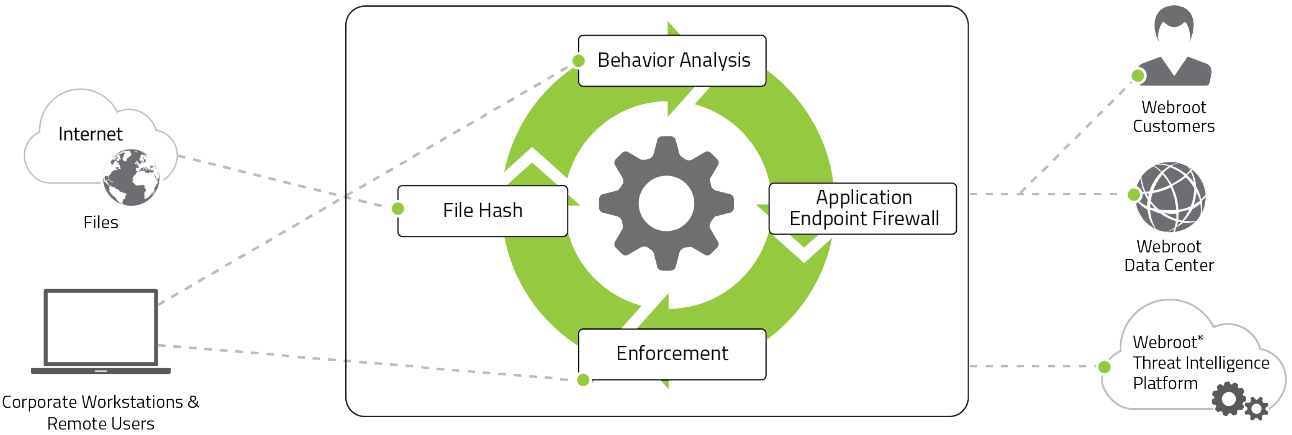
Webroot SecureAnywhere® Business Endpoint Protection offers a unique security approach that protects against threats across numerous vectors; including email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives, as well as other blended threats with the potential to deliver malicious payloads.

Powered by the industry-leading cloud-based Webroot Threat Intelligence Platform, Webroot solutions combine the latest real-time intelligence from Webroot BrightCloud® services with advanced machine learning and behavior-based heuristics. Using our always up-to-date, cloud-based technology, Webroot is able to detect, analyze, categorize, score, and highly accurately predict the threats each endpoint is experiencing in real time.

By combining SecureAnywhere file pattern and predictive behavior recognition technology with cutting edge machine learning and the processing power of cloud computing, Webroot effectively stops malware and zero-day threats at the moment of attack. The Webroot approach is more effective and accountable than single-vector competitors. 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, can't protect users until after malware has already infiltrated the system, and doesn't alert on attacks until long after the infiltration has occurred.

Because SecureAnywhere Business Endpoint Protection is fully cloud-based, there are no definitions or signatures to deploy and manage. Malware detection occurs continuously in real time, so performance issues fade away. Scheduled systems scans are normally around 18 seconds and never impact device performance, even on virtual desktop and server environments, as well as embedded operating systems. The software agent itself happily coexists with other antivirus solutions, so there's no need to rip and replace an existing solution.

The world's smallest, fastest endpoint security client offers unique protection against multi-vector threats.


Internet
Files
Corporate Workstations & Remote Users
Behavior Analysis
File Hash
Application Endpoint Firewall
Enforcement
Webroot Customers
Webroot Data Center
Webroot® Threat Intelligence Platform

Uncovering zero-day malware

Visible Efficacy

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 was contained by Webroot before being automatically remediated.

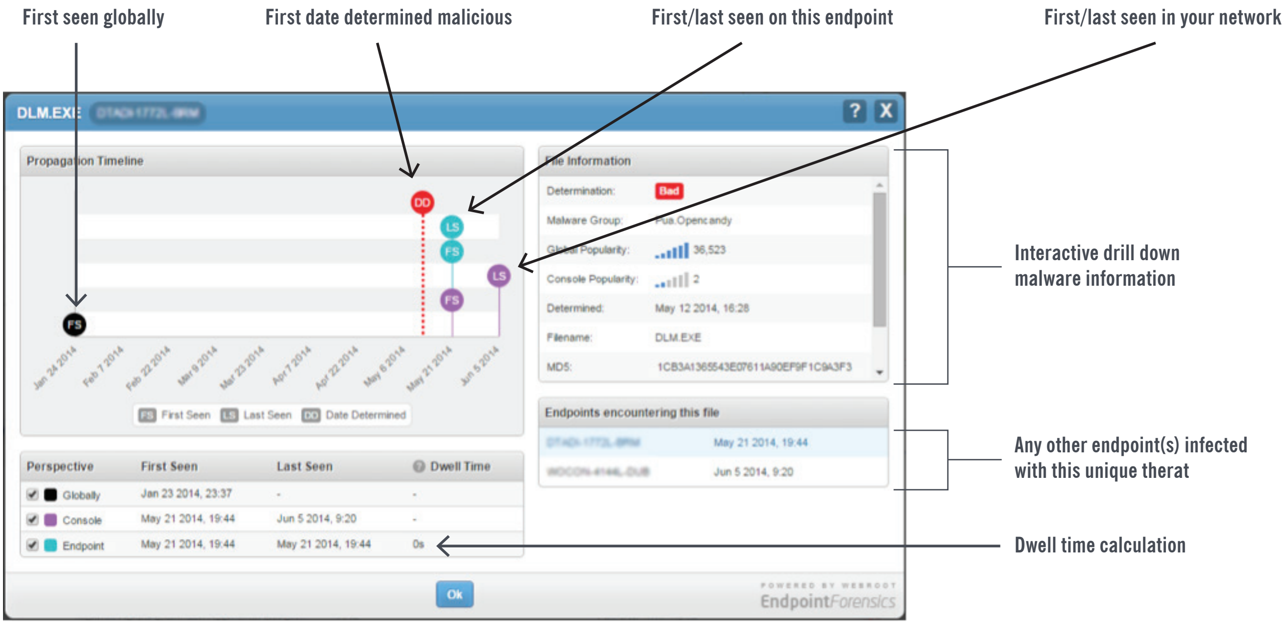
A major factor contributing to the efficacy of SecureAnywhere Business Endpoint Protection is its continuous infection monitoring, journaling, and auto-remediation. If it cannot immediately categorize new or changed files and processes as 'known' good or 'known' bad, then the agent begins monitoring 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. On the rare occasion that a false positive does occur, admins can easily white list files as needed within their management console.

Flexible Cloud-Based Management

Webroot SecureAnywhere solutions use cloud-based management, which means no on-premises hardware or software is needed and the console is always up to date. The Webroot Global Site Manager console makes it straightforward to manage up to 100,000 endpoints, and, through its hierarchical management architecture, you can easily control multiple sites and locations, as best suited to your organization's needs. 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 businesses of all sizes, including those with global 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 delivering global management extraordinarily cost-effective compared to conventional antivirus.

Infection Dwell Time: Visibility into Containment and Remediation



DLM.EXE [redacted]

File Information

Determination:	Bad
Malware Group:	Pua.Opencandy
Global Popularity:	36,523
Console Popularity:	2
Determined:	May 12 2014, 16:28
Filename:	DLM.EXE
MD5:	1CB3A1365543E07611A90EF9F1C9A3F3

Endpoints encountering this file

[redacted]	May 21 2014, 19:44
[redacted]	Jun 5 2014, 9:20

Perspective	First Seen	Last Seen	Dwell Time
☑ ■ Globally	Jan 23 2014, 23:37	-	-
☑ ■ Console	May 21 2014, 19:44	Jun 5 2014, 9:20	-
☑ ■ Endpoint	May 21 2014, 19:44	May 21 2014, 19:44	0s

Powering Predictive Prevention

All Webroot SecureAnywhere solutions and BrightCloud threat intelligence services are powered by the Webroot® Threat Intelligence Platform. Leveraging big data analytics, machine learning, and threat intelligence from customers and technology partners worldwide, the Webroot Threat Intelligence Platform identifies infections as they occur. This big data architecture continuously processes, analyzes, correlates and contextualizes vast amounts of disparate information while also applying a patented, fifth-generation machine learning and malicious code identification system to create predictive behavioral determinations on malware instantly—with impressive 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 hundreds of terabytes of threat data, ensures that Webroot customers are continuously protected from both existing and new threats.

Key Security Features

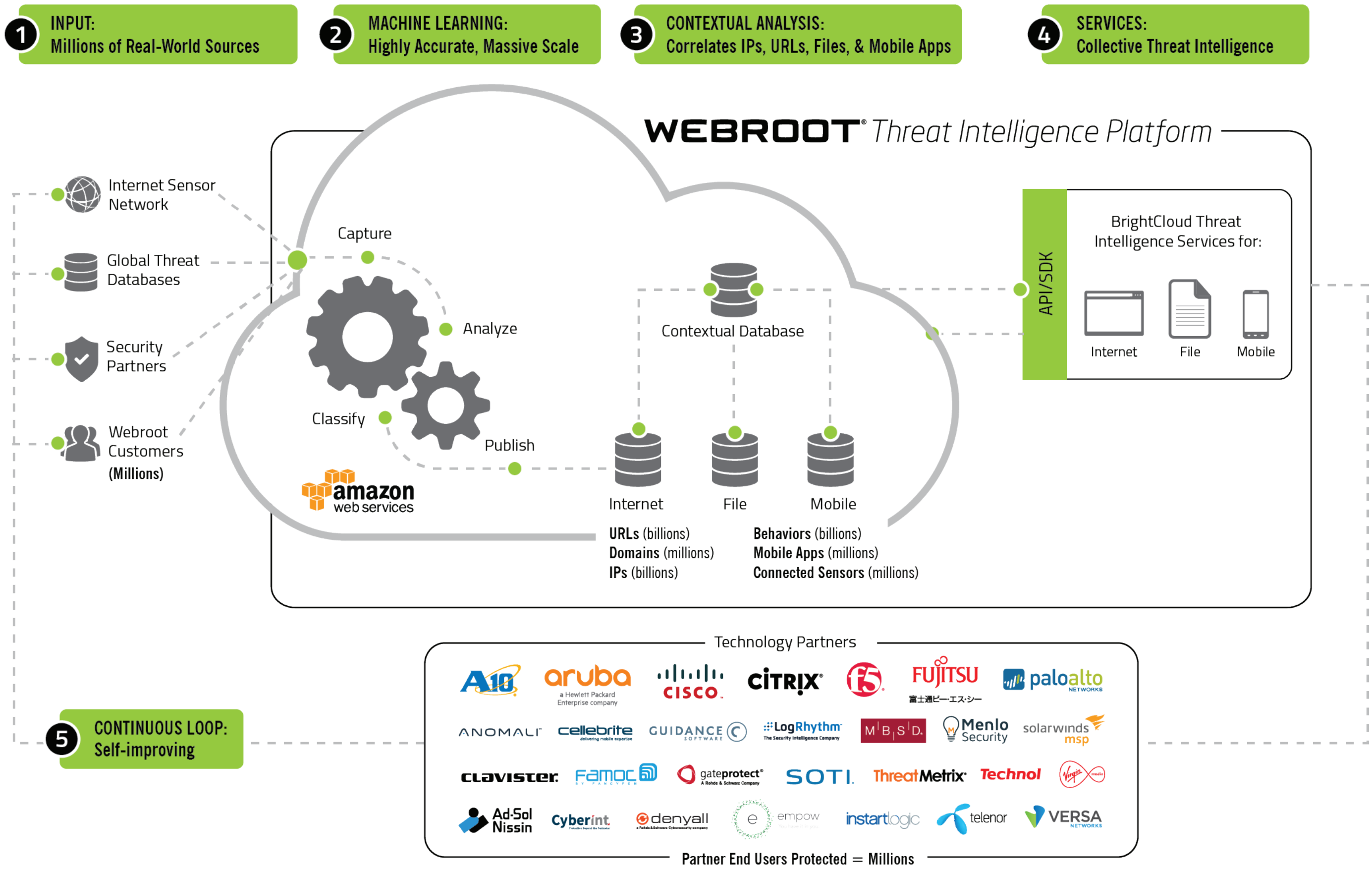
Webroot SecureAnywhere Business Endpoint Protection offers highly accurate and effective endpoint malware prevention with a range of additional security shield capabilities that keep both the user and the device safe.

Identity Shield

This shields protects users by assuming the endpoint is already infected by as-yet undetected malware. It protects user and transactional data that could be exposed during online transactions from phishing, DNS poisoning, keystroke logging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software mounting man-in-the-middle attacks. The shields 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 secure other endpoint applications as well.

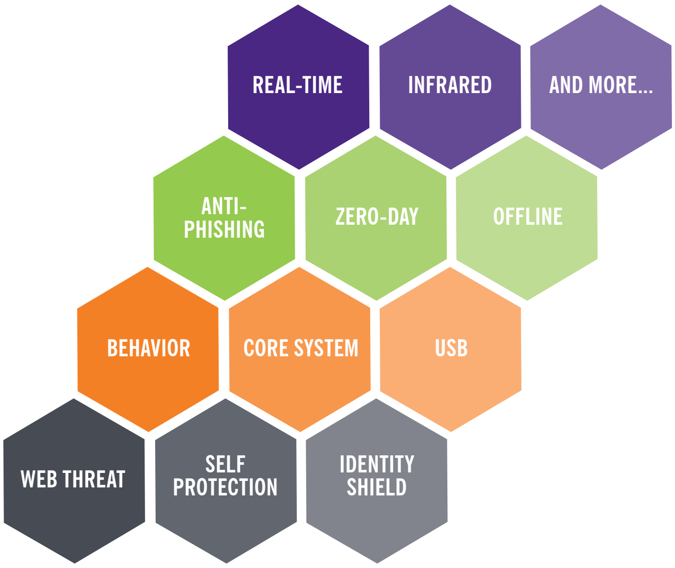
Infrared

Infrared is a multi-layer defense that incorporates several aspects of Webroot Threat Intelligence to help thwart threats early on in their lifecycle—often before a threat researcher sees a single sample. It examines the reputation of the websites an individual visits and uses Webroot Threat Intelligence to determine their risk level. If the user commonly visits low-reputation websites, the agent goes into a



1 INPUT: Millions of Real-World Sources
2 MACHINE LEARNING: Highly Accurate, Massive Scale
3 CONTEXTUAL ANALYSIS: Correlates IPs, URLs, Files, & Mobile Apps
4 SERVICES: Collective Threat Intelligence
WEBROOT® Threat Intelligence Platform
Internet Sensor Network
Global Threat Databases
Security Partners
Webroot Customers (Millions)
Capture
Analyze
Classify
Publish
amazon web services
Contextual Database
Internet
File
Mobile
URLs (billions)
Domains (millions)
IPs (billions)
Behaviors (billions)
Mobile Apps (millions)
Connected Sensors (millions)
API/SDK
BrightCloud Threat Intelligence Services for:
Internet
File
Mobile
Technology Partners
5 CONTINUOUS LOOP: Self-improving
Partner End Users Protected = Millions

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



Webroot Multi-Vector Protection

heightened state of awareness and closely interrogates any new files or processes that are introduced into the system. Infrared also interprets user behaviors and their overall safety level. If a user is classified as "high risk", Webroot then dynamically tailors malware prevention to that user, while preventing false positives for less risky users.

Web Threat Shield

The Web Threat Shield leverages Webroot anti-phishing technology to offer unique real-time protection against polymorphic phishing URLs, as well as malicious and high-risk websites and domains.

Intelligent Outbound Firewall

In addition to its shields, SecureAnywhere Business Endpoint Protection includes an intelligent system-monitoring and application-aware outbound firewall that augments the Microsoft Windows® firewall to protect users on and off the corporate network. It monitors all outbound traffic to protect against "phone-home" threats, ensures only approved applications communicate with the network, and automatically recognizes known good and bad programs. Users aren't pestered with pop-ups or forced to make uninformed judgments, and resources aren't drained.

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 Webroot Threat Intelligence

» **Popularity**
Analyzes new programs based on how often a file is used or changed within Webroot 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.