WEBROOT®

Webroot SecureAnywhere® Business Endpoint Protection

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

OVERVIEW

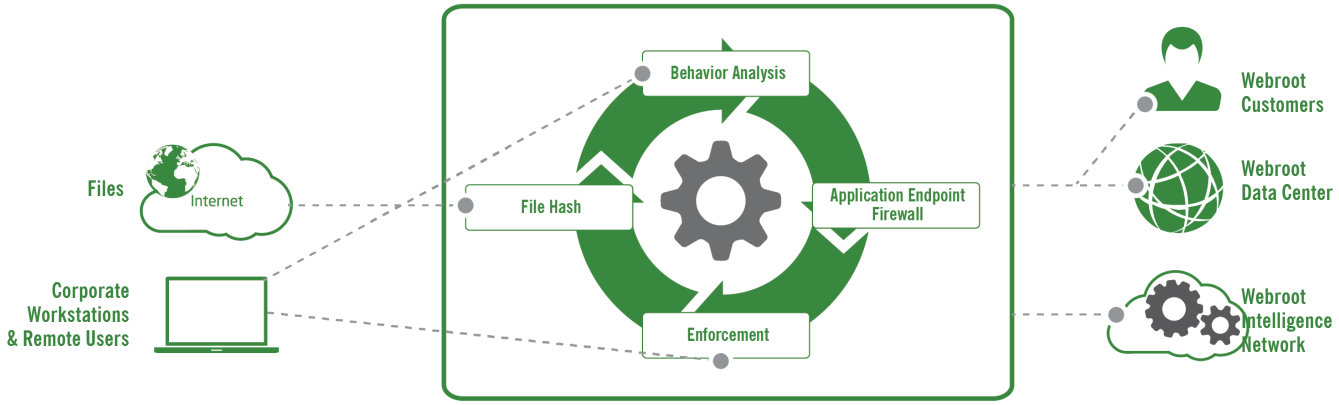
Confidence has never been so low in a key threat prevention technology: endpoint security. Conventional antivirus protection is struggling to keep up with today's threats and attacks. It slows down machines and users and is complex and resource-intensive.

Now, by unifying 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 infection. The unique, 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 results in infections only becoming visible long after the endpoint is infected.

Traditional antivirus presents the hassle of ensuring every endpoint has the latest update. Webroot 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 architecture 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 and endpoint security performance and management issues. It provides the protection you need without the demanding overhead of conventional antivirus.


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

Uncovering zero-day malware

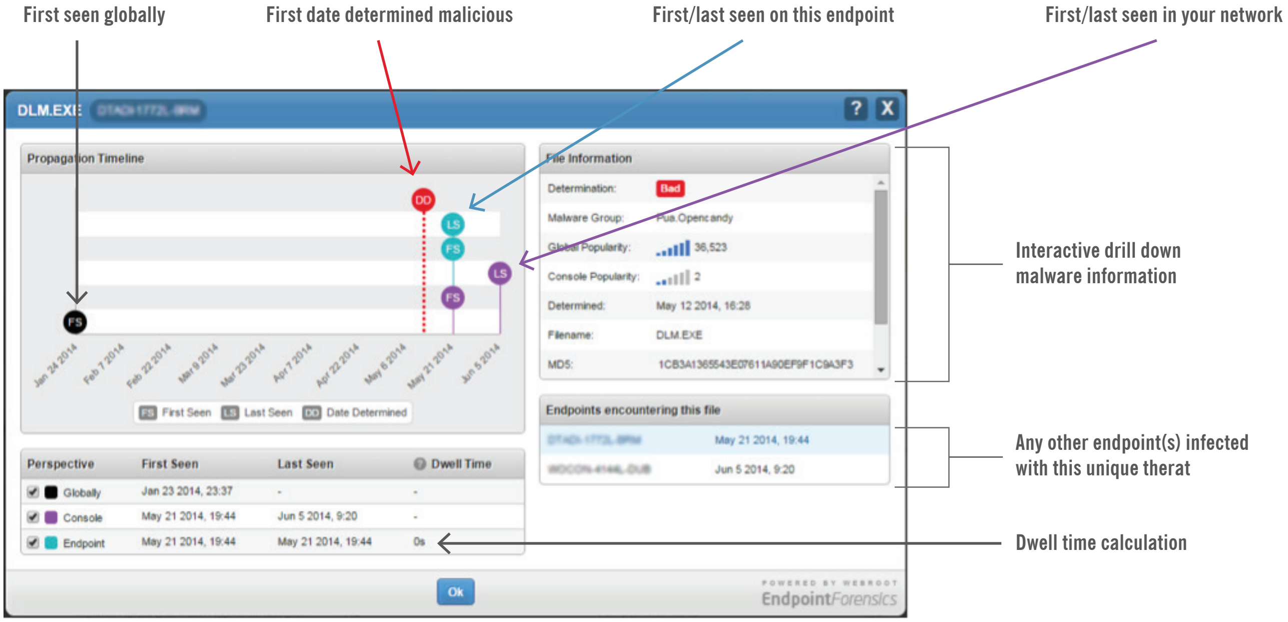
VISIBLE EFFICACY

A feature-rich endpoint protection solution amounts to nothing if it can't deliver its key feature: malware prevention. SecureAnywhere 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 is its continuous infection monitoring, journaling and auto-remediation.

If SecureAnywhere 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



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

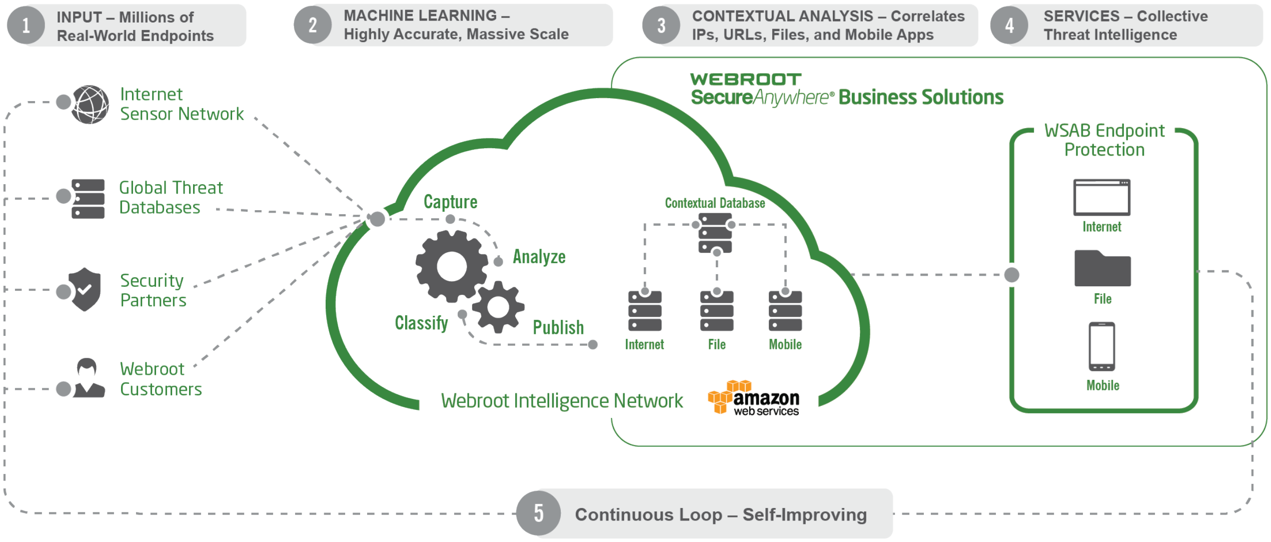
[redacted]	May 21 2014, 19:44
[redacted]	Jun 5 2014, 9:20

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

FLEXIBLE CLOUD-BASED MANAGEMENT

Webroot SecureAnywhere has 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 Site Manager console or our Global Site Manager console, so you can choose the management features appropriate to your organization's needs. The Site Manager 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, or if you are a Managed Services Provider 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.


1 INPUT – Millions of Real-World Endpoints
2 MACHINE LEARNING – Highly Accurate, Massive Scale
3 CONTEXTUAL ANALYSIS – Correlates IPs, URLs, Files, and Mobile Apps
4 SERVICES – Collective Threat Intelligence
Internet Sensor Network
Global Threat Databases
Security Partners
Webroot Customers
WEBROOT SecureAnywhere® Business Solutions
Capture
Analyze
Classify
Publish
Contextual Database
Internet
File
Mobile
Webroot Intelligence Network
amazon web services
WSAB Endpoint Protection
Internet
File
Mobile
5 Continuous Loop – Self-Improving

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

POWERING PREDICTIVE PREVENTION

At the center of stopping malware on every endpoint using SecureAnywhere is the Webroot Intelligence Network (WIN). Leveraging big data analytics and threat intelligence from our users and technology partners worldwide, WIN identifies threats as they occur. The WIN 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 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.

Endpoint Protection Fast Facts

Zero-day Malware and APT Prevention

» Predictive behavior recognition technology detects APTs and malware
» Dwell time alerting and reporting instantly reveals any endpoint infection
» Full visibility of any infection by endpoint

Always Protected and Up-to-date

» No definition or signature file updates to manage
» Every endpoint protected individually (on and offline)
» All users instantly and collectively protected against new threats

Never Slows System Performance

» Idle CPU usage of 0.10%[1] – 10.8%[1] during scans
» Initial full system scan uses <15[1] MB of RAM
» Scheduled scans take <30[1] seconds

Standard and Global Site Management Consoles

» Standard console for simple deployments up to 1,000 users
» Global Site Manager console for up to 100,000 users
» Global Site Manager ideal for multi-site, multi-location and multi-administered deployments

Powerful Endpoint Management Tools

» Multiple powerful Agent Commands to remotely control and instruct endpoint(s)
» Overrides to apply both white- and black-list application policies down to individual user level
» Identity and Privacy Shields to secure sensitive data at the browser and application level

Fast and Easy to Deploy

» World's smallest endpoint security agent (<750KB[1])
» Takes under five seconds1 to be fully operational
» No-conflict design so the agent can run alongside other security software

Easy to manage

» No on-premise hardware or software to manage
» Fully remote management of all endpoints with granular administrator access rights
» Choice of Standard or Global management consoles to suit operational requirements

Low Operational Costs

» Highly automated management and customizable reporting
» Endpoint infection rollback and auto-remediation
» Integration with Autotask, Continuum, Kaseya, LabTech and Spiceworks

Fully Integrated Support

» Fully inclusive web-based and telephone support
» Auto user logging, instant ticketing and escalation from console
» One-call—10-minute average—ticket resolution

[1] PassMark Software Webroot SecureAnywhere Business Endpoint Protection vs. Seven Competitors (February 2014)

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 endpoint 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 the WIN 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 WIN 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 WIN to access the latest security intelligence on any web site.

Smart Outbound Firewall

In addition to its Shields, Webroot SecureAnywhere has its own "smart" 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 WIN

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

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 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 datacenters to support local offices and roaming users through their nearest datacenter, providing full service resilience and redundancy.

System Requirements

Management Portal Access:

» Internet Explorer® version 7 and newer
» Mozilla® Firefox® version 3.6 and newer
» Chrome 11 and newer
» Safari 5 and newer
» Opera 11 and newer

Supported PC Platforms:

» Windows 8, 8.1, 32 and 64-bit
» Windows 7, 32 and 64-bit
» Windows Vista®, 32 and 64-bit
» Windows® XP Service Pack 2 and 3, 32 and 64-bit
» Windows XP Embedded
» Mac OS X v.10.9 "Mavericks"
» Mac OS X v.10.8 "Mountain Lion"
» Mac OS® X v.10.7 "Lion"

Supported Server Platforms:

» Windows Server 2012 Standard, R2
» Windows Server 2008 R2 Foundation, Standard, Enterprise
» Windows Server 2003 Standard, Enterprise, 32 and 64-bit
» Windows Small Business Server 2008, 2011, 2012
» Windows Server Core 2003, 2008, 2012
» Windows Server 2003 R2 for Embedded Systems
» Windows Embedded Standard 2009 SP2
» Windows XP Embedded SP1, Embedded Standard 2009 SP3
» Windows Embedded for POS Version 1.0

Supported Virtual Server Platforms:

» VMware vSphere 5.5 and older (ESX/ESXi 5.5 and older), Workstation 9.0 and older, Server 2.0 and older
» Citrix XenDesktop 5; XenServer 5.6 and older; XenApp 6.5 and older
» Microsoft Hyper-V Server 2008, 2008 R2
» Virtual Box

About Webroot

Webroot provides intelligent cybersecurity that harnesses collective threat intelligence to protect the Internet of Everything. We protect consumers, businesses and technology providers from malware and other cyber-attacks using a cloud-based threat intelligence network. Computers, tablets, smartphones and the Internet of Things can be secured by our award-winning suite of SecureAnywhere® and BrightCloud® products. Webroot protects over 30 million devices and is trusted by market-leading technology companies, including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, and RSA. Webroot is headquartered in Colorado and operates globally across North America, Europe and the Asia Pacific region. Discover smarter cybersecurity at www.webroot.com and www.brightcloud.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