

WEBROOT[®]
Smarter Cybersecurity™



Fighting Endpoint Threats with the Power of BrightCloud® Threat Intelligence

Cyber-attacks are now so frequent that endpoint defenses without access to broad, instant, and actionable malware security intelligence simply aren't good enough. Without intelligent next-generation endpoint defenses in place, organizations will get infected more and more regularly, and may not become aware of breaches until it's too late. In this threat landscape, effective endpoint malware prevention requires continuous monitoring of every individual endpoint and an immediate response to anything new or unexpected occurring on any device. Infection dwell times of days, weeks, or months are unacceptable, as are forensics and audits that can detail the kill chain but are unable to break it.

The goal of all endpoint security is to mitigate attacks. However, understanding one set of attack vectors will no longer let you stop the next attack; threats and attacks are too variable, polymorphic, and unpredictable. Proactive mitigation, real-time visibility, and an immediate response are the only real defenses.

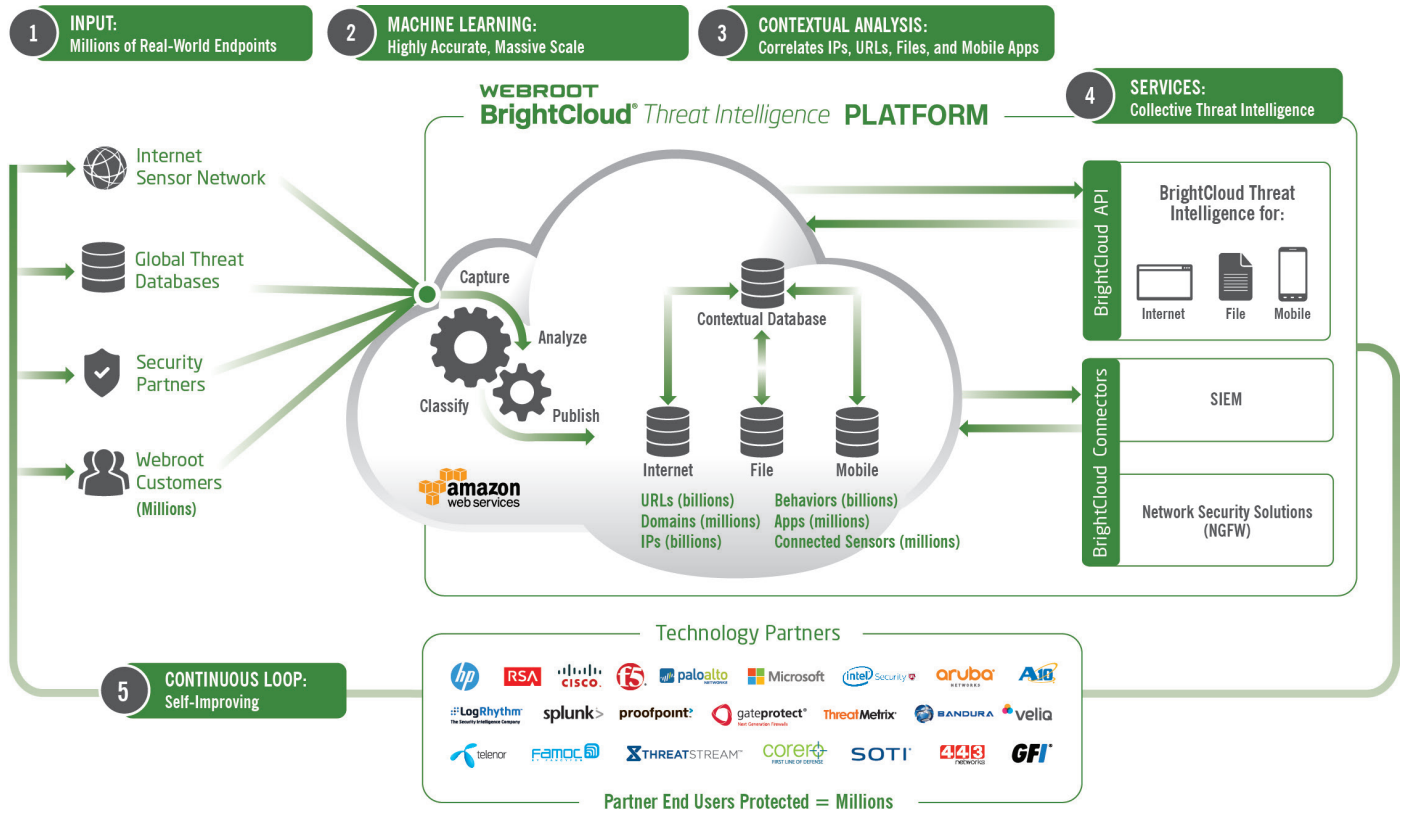
Webroot® Smarter Cybersecurity™ solutions and threat intelligence services are all powered by the Webroot BrightCloud® Threat Intelligence Platform, which was purpose-built to deliver robust, next-generation threat prevention. BrightCloud Threat Intelligence Services integrate billions of pieces of information from millions of sensors to create the world's largest malware detection net, providing proactive protection against both known and never-before-seen attacks.

COLLECTIVE AND PREDICTIVE

The BrightCloud Threat Intelligence Platform encounters tens of millions of instances of malware and potentially unwanted applications and monitors billions of IP addresses and URLs. It analyzes millions of new and updated mobile apps for malicious behavior and studies major malware trends based on data from millions of endpoints. All of this and more continuously enriches BrightCloud Threat Intelligence and allows us to accurately and effectively protect organizations from sophisticated attacks.

Continuous Analysis and Correlation

- 1 Monitor**
Accurately monitor the entire IPv4 space and in-use IPv6 addresses and continuously update a dynamic list of approximately 12 million malicious IP addresses
- 2 Classify**
Classify and score over 95% of the internet on a daily basis and detect phishing sites in real time
- 3 Categorize**
Categorize millions of files that are seen across millions of Webroot customer endpoints
- 4 Assess**
Assess the risk of millions of mobile apps (over 7 million new and updated in 2014)



Webroot BrightCloud® Threat Intelligence

We believe it is essential for IT departments, users, and others to have access to up-to-date intelligence on threats to their systems and endpoints of all types. Threats are constantly changing, so security controls must adapt accordingly. These security controls include being aware of the latest malicious IPs, the types of websites that are most often impersonated in phishing attacks, and the categories of apps that are most likely to be malicious.

Real-time, contextual, and predictive threat intelligence that spans the spectrum of attack vectors is the critical component in implementing a defense-in-depth strategy. It's the only way to fight back against today's cybercriminals and give companies an edge. It's what makes our threat intelligence not simply a cloud-based data repository but the most powerful, real-time threat analysis engine of its kind.

Massive data processing capacity, coupled with our proprietary implementation of the most advanced machine learning technology available, and a powerful contextual analysis engine, has enabled Webroot to accurately classify and score unsurpassed numbers of URLs, IPs, malware files, and mobile apps to help keep our customers ahead of the exponential proliferation of threats they face.







MACHINE LEARNING

A key differentiator is our unique approach to machine learning. In web threat analysis, most security vendors use Bayesian networks or support vector machine (SVM) models to populate their work queues for human analysis. This approach isn't scalable, or even particularly accurate. Webroot, on the other hand, uses maximum entropy discrimination (MED) and other techniques to generate highly accurate and scalable web threat analysis. Here is a brief outline of the differences between the three machine learning technologies used, as well as the levels of accuracy associated with each.

1. Bayesian networks analyze site features to make predictive determinations and provide a simplistic, two-dimensional model to split known good from bad sites across a flat feature space.
2. SVM analyzes data, feature, and content patterns to make predictions on sites at a higher degree of accuracy than Bayesian networks, but still requires human analysis to achieve an acceptable confidence level.
3. MED uses advanced algorithms to weave a flexible fabric through the three-dimensional feature space and make highly definitive determinations on the vast majority of websites – offering speed, scale, and accuracy.

Advanced Machine Learning

Through MED, BrightCloud Threat Intelligence currently classifies well over 2,500+ URLs per second at an error rate of less than 2% (versus an average human error rate of 5-15%). Webroot utilizes global teams of multilingual web analysts to analyze the relatively small number of websites where machine learning technology doesn't achieve a sufficient degree of determination confidence. Human analysts evaluate these cases and then feed each of them back into the machine learning model, continuously improving our accuracy.

 27+ Billion URLs	 9+ Billion File Behavior Records
 600+ Million Domains	 17+ Million Mobile Apps
 4+ Billion IP Addresses	 37+ Million Connected Sensors

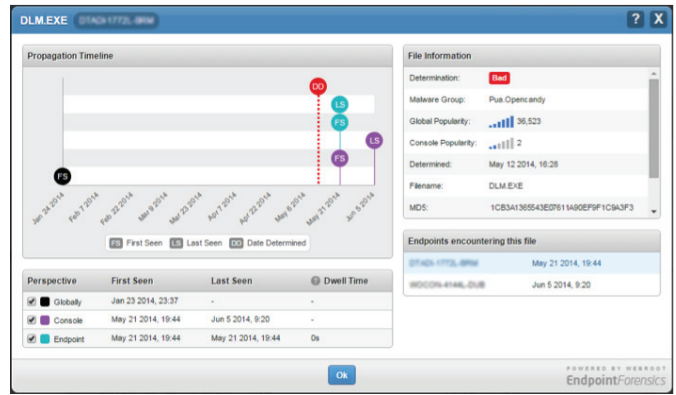
DATA CORRELATION

BrightCloud Threat Intelligence also leverages a powerful contextual analysis engine that takes previously disparate data and correlates it to create a deeper insight of the interconnected landscape of URLs, IPs, files, and mobile apps. Mapping the relationships between these different data points enables Webroot to provide highly accurate and dynamic intelligence that is always up to date, with virtually no false positives. For example, a seemingly benign IP may not show up as a risk on other IP reputation lists. Because that IP has been tied to other known malicious URLs, IPs, files, or mobile apps by the BrightCloud® contextual analysis engine, its reputation score is reduced via this correlated intelligence, keeping customers safe from what could be a never-before-seen attack.

REAL-TIME VISIBILITY

Webroot BrightCloud® Threat Intelligence doesn't rely on stagnant signature files. Our smarter approach to malware prevention:

- » Identifies the point and time of infection and alerts admins accordingly
- » Minimizes the dwell time and vulnerability window between the launch and detection of an attack
- » As soon as a threat is recognized on an individual endpoint, the entire network of endpoints is simultaneously protected in real time
- » Few system resources are needed, freeing up CPU, disk space, and memory, keeping end user impact to a minimum



Endpoint Dwell Time Reporting

SMARTER ENDPOINT PROTECTION

Although other endpoint protection vendors have invested in threat intelligence as well, they only use it to supplement their traditional, signature-based offerings. None of them deliver the breadth of real-time monitoring or security intelligence available from Webroot BrightCloud Threat Intelligence.

Because Webroot SecureAnywhere Business Endpoint Protection leverages the power of cloud-based, collective threat intelligence, it leaves only the tiniest of device footprints (2MB).^{*} In contrast, independent performance testing by PassMark Software determined that the average device footprint across seven competitor solutions was over 1,140MB.^{*}

- » **Quick Installation and Full Compatibility:** The Webroot SecureAnywhere agent is fully installed and operational in just 5* seconds. Its no-conflict design means it can run alongside existing security solutions, so you can either augment your protection or replace it without risking a vulnerability window.
- » **Fast Scans Reduce System and User Impact:** Scheduled scans with Webroot SecureAnywhere Business Endpoint Protection take 91* seconds, while the competitor solutions tested required an average of 30 minutes.*
- » **Minimal Resource Usage:** Even when scanning, the program uses less than 10%* of CPU resources. Hogging system resources and degrading performance is a major concern with traditional endpoint security, that can use up to 24%* of the CPU. With Webroot SecureAnywhere Business Endpoint Protection, the heavy lifting is done in the cloud, not on the endpoint.
- » **Low Bandwidth Consumption:** Network traffic to and from the Endpoint Protection agent averages only a few hundred kilobytes per day, while other solutions require megabytes' worth of daily updates.

^{*} Source: PassMark Software Performance Benchmark August 2015

INFORMATION

For more information, including white papers, case studies, customer testimonials, and the complete PassMark Software Benchmark Performance report, visit our website or contact one of our Webroot Channel Partners.

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 10, 32 and 64-bit
- » 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.10.10 "Yosemite"
- » 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 Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. Discover Smarter Cybersecurity solutions at www.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