WEBROOT
Smarter Cybersecurity™

BrightCloud® Streaming Malware Detection

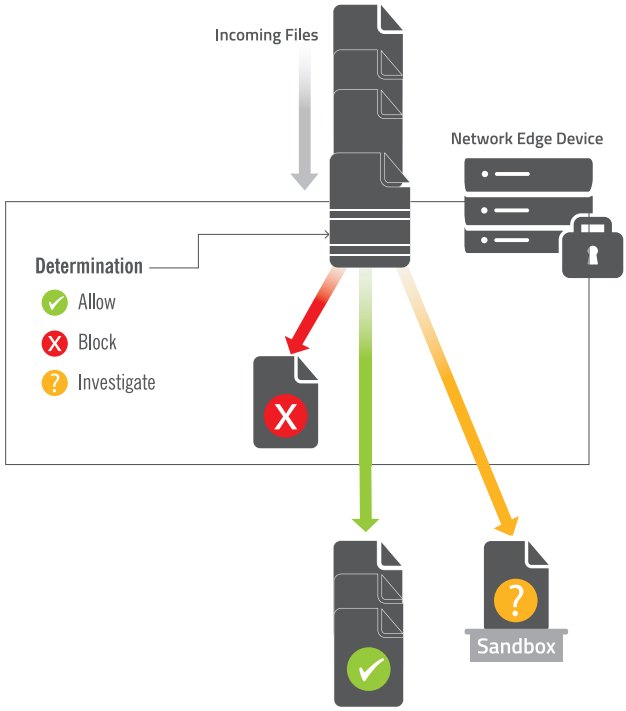
Catch malicious files in transit before they infiltrate your customers' networks

- The vast majority of malware is polymorphic and designed to evade detection
- Traditional and network-based security approaches are too slow and ineffective
- Analyzing files as they enter the network catches malware before it can spread

Polymorphic malware hides from traditional detection technologies by changing its code each time it runs. In fact, 92% of malware caught by Webroot in 2016 was seen on just one endpoint, and 99% of samples were seen on less than ten.[1] In addition, these variants tend to be extremely short-lived, and organizations that rely on traditional security are unlikely to catch them before they infiltrate and spread across networks and systems.

Webroot BrightCloud Streaming Malware Detection was specifically designed to combat the challenges of polymorphic malware and targeted malware in general. This innovative technology provides a risk score for files as they stream through the network perimeter, without requiring the entire file to be downloaded. The contents of a file are parsed as the file streams through a network appliance and scored at a rate of over 5,000 per minute to avoid posing any undue network latency. Users then set policies for the threshold at which files are allowed, blocked/dropped, or routed for further investigation and analysis.

This solution can be used as an additional layer of security in front of other slower, heuristic- or signature-based technologies such as sandboxes or antivirus. This frees up network bandwidth by dropping malware at the perimeter and eliminates the need to re-inspect benign files. It is also ideal for integration with backup solutions and storage management devices to ensure clean backup copies, and can be used for upfront network filtering by internet service providers or content delivery networks to filter out malicious files before they reach customers.



Detect Malware in Transit

*92% of malware caught by Webroot in 2016 was seen on just one endpoint.**

*Webroot 2017 Threat Report

Partner Benefits

» **Differentiate yourself from your competition**
Innovative technology catches malicious files in transit before they penetrate your customers' networks

» **Rely on trusted performance**
Leverage the massive scale of advanced machine learning for reliable, real-time protection

» **No impact on network throughput**
Files are scanned as they stream through the appliance, over 500 times faster than traditional sandboxing

» **Easy to integrate and use**
Simple integration into your solution via a pre-compiled SDK

Webroot BrightCloud Streaming Malware Detection in Action

Integrating Webroot BrightCloud Streaming Malware Detection provides effective network-based malware detection that can be tuned to suit risk tolerance and preferences, without imposing network latency.

» Catches malicious files in transit before they are able to penetrate and spread throughout the network

» Assesses files byte by byte with no need for the entire file to be present

» Makes determinations in milliseconds – over 500 times faster than a typical network sandbox environment

» Improves network performance and reduces latency because it works upstream from slower sandboxing and signature-based technology

Easy Integration

The Webroot BrightCloud Streaming Malware Detection SDK integrates seamlessly into perimeter security devices used by enterprises, small to mid-sized businesses, or consumers, including next-generation firewalls, firewall routers, network intrusion detection systems, intrusion prevention systems, email and web gateways, unified threat management devices, and even home routers.

System Requirements

» CentOS 6.5+

» Red Hat Enterprise 7.1+

» Ubuntu 14+

» Windows 7+

» Compiler of GCC 4.4.7+

» Minimum 328MB memory

» 120MB of disk space

About Webroot

Webroot delivers next-generation network and endpoint security and threat intelligence services to protect businesses and individuals around the globe. Our smarter approach harnesses the power of cloud-based collective threat intelligence derived from millions of real-world devices to stop threats in real time and help secure the connected world. Our award-winning SecureAnywhere® endpoint solutions and BrightCloud® Threat Intelligence Services protect millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, Citrix, F5 Networks, Aruba, Palo Alto Networks, A10 Networks, and more, Webroot is headquartered in Colorado and operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity™ solutions at 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