CARBONITE an opentext company | WEBROOT an opentext company

# BrightCloud® Streaming Malware Detection

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

### Overview

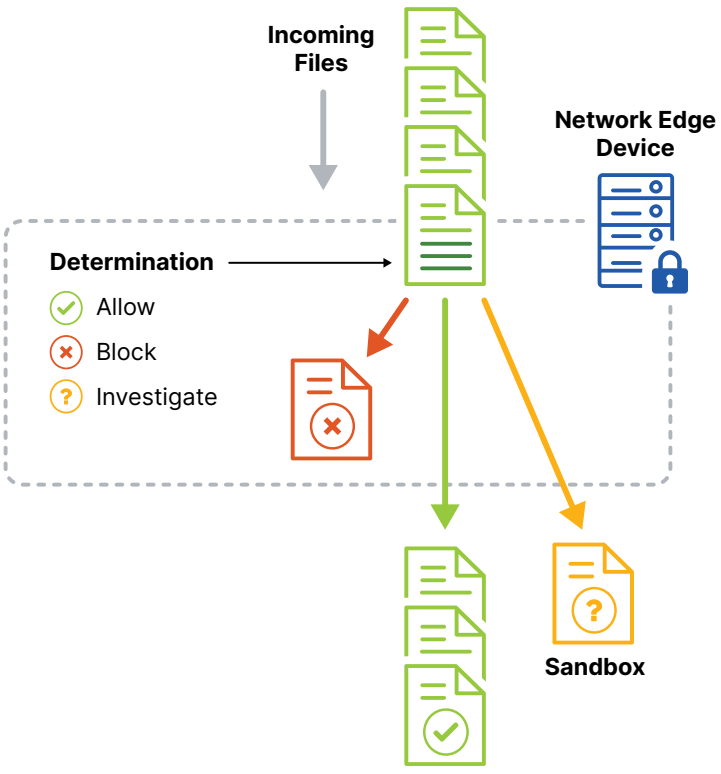
- The vast majority of malware is polymorphic and designed to evade detection
- Traditional and network-based security approaches are too slow and ineffective
- Analyzing files as they enter the network catches malware before it can spread

Polymorphic malware hides from traditional detection technologies by changing its code each time it runs. In 2019, 93.6% of malware seen was polymorphic.[1] 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 combats the challenges of polymorphic malware. This innovative technology provides a determination for files as they stream through the network perimeter, often 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 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.

*93.6% of malware detected by Webroot in 2019 was polymorphic.[1]*




Detect Malware in Transit at the Network Edge

[1] Webroot Inc. "2020 Webroot Threat Report." (February 2020)

## Partner Benefits

- **Differentiate yourself from your competition**
  Innovative technology enables end users to maximize investments in more expensive (and cumbersome) solutions, such as sandboxes, by ensuring only unknown or bad files are sent for in-depth analysis.
- **Rely on trusted performance**
  Leverage the massive scale of advanced machine learning for reliable, real-time protection.
- **No impact on network throughput**
  Improve network performance with a solution that works upstream from slower sandboxing and signature-based technology.
- **Easy to integrate and use**
  Integrate Streaming Malware Detection into your solution via a precompiled SDK.

## Additional Enhancements with File Reputation

Streaming Malware Detection can be coupled with BrightCloud File Reputation to provide an even stronger layer of defense. Combining file intelligence with cutting edge polymorphic detection ensures superior coverage of both known and never-before-seen files.

The BrightCloud® File Reputation service provides up-to-the minute file intelligence derived from millions of real-world sensors. Each file is analyzed by the latest machine learning techniques and vetted through years of threat expertise. This real-time lookup service of known malicious and allowed file identifiers helps to effectively stop the distribution of threats through networks. This verification significantly reduces the amount of 'noise' by enabling policies to automatically determine which files to allow, block, or investigate further, allowing security administrators to focus on unknown potential threats.

## 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 Server 2012+
- Compiler of GCC 4.4.7+
- Minimum 350MB memory
- 260MB of disk space

**Contact us to learn more – Webroot US**

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383

**About Carbonite and Webroot**

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.