DATASHEET

BrightCloud® Threat Intelligence

BrightCloud® Streaming Malware Detection

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

86% of malware is unique to a single PC.[1]

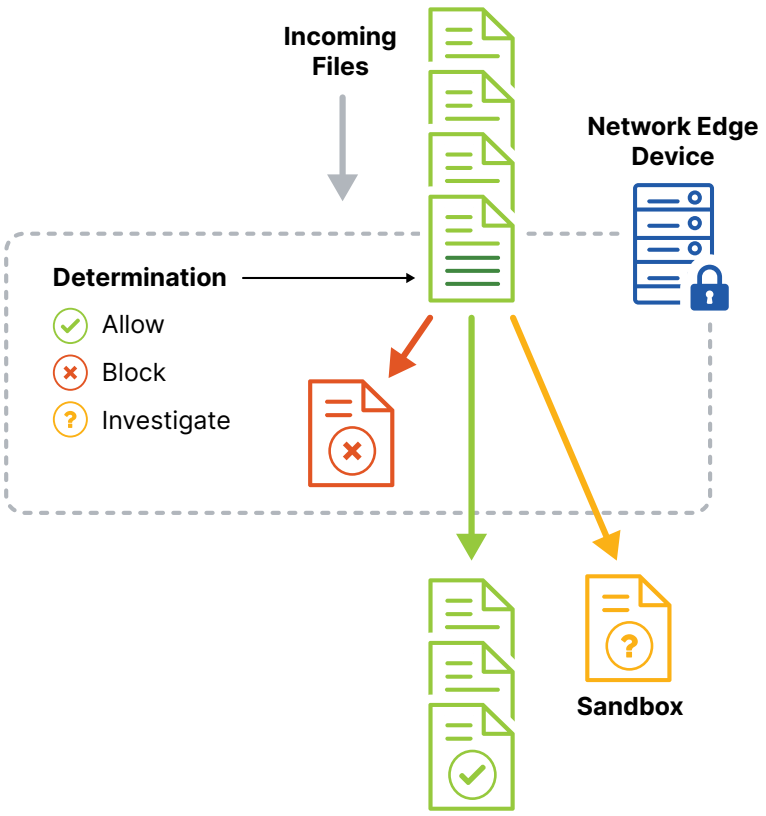
Overview

- 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. These variants tend to be extremely short-lived. Organizations that rely on traditional security are unlikely to catch them before they infiltrate and spread across networks and systems.

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. It 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 at the Network Edge

Partner Benefits

1. **Block/address** the malware at the network edge preventing the lateral spread
2. **Faster (policy-based) response** to potential malware without network bandwidth or user experience impact
3. **Enhanced protection** with AI-based intelligence combining historical insights and real-time insights

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 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 and management devices.

System Requirements

- CentOS 6.5+
- Red Hat Enterprise 7.1+
- Ubuntu 14+
- Windows Server 2012+
- Compiler of GCC 4.4.7+
- Minimum 350MB memory
- 400MB of disk space

[1]2021 Webroot BrightCloud® Threat Report

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.