WEBROOT
Smarter Cybersecurity™

BrightCloud® Threat Investigator

Empower customers to make better informed security decisions for proactive protection

Overview

» Single-vector intelligence isn't sufficient for threat investigation or proactive protection

» Contextual intelligence spanning threats from URLs, IPs, files and mobile apps provides insight into relationships surrounding a specific object

» Partners can supplement existing services with additional intelligence to help their customers make informed decisions and take proactive protective measures

The use of threat intelligence has become a critical component of network and endpoint defenses for companies worldwide, whether integrated directly or embedded in security appliances, such as next-generation firewalls or gateways. However, data can be stale, prone to false positives, or lacking in sufficient breadth and depth to be actionable.

BrightCloud® Threat Intelligence Services provide real-time, highly accurate, and actionable threat intelligence across the internet threat spectrum. This includes coverage of over 95% of the internet, monitoring of the entire IPv4 space, classification of billions of file behavior records, and scoring of millions of mobile applications. As the most dangerous threats often span multiple threat vectors, connections between URLs, IPs, files, and mobile apps are analyzed in order to provide greater accuracy and predictive risk scores based on a guilt-by-association model.

While each BrightCloud Threat Intelligence Service offers correlated intelligence on its specific threat vector, it can be useful to explore the primary connections surrounding a specific URL, IP, file, or mobile app to better understand why a score was given and to proactively protect against other potential threats.

The BrightCloud Threat Investigator API is available to complement any BrightCloud Threat Intelligence Service. Through an API, Webroot technology partners can now access additional contextual intelligence on all primary connections (regardless of object type) to a central object seen within their existing service. This can be used to gain additional contextual knowledge around an object under investigation to potentially take action or automatically block more malicious actors.

In addition, the BrightCloud Threat Investigator is a web-based tool that enables partners to visually demonstrate the contextual relationships between IPs, URLs, files and mobile apps. This can be used by Webroot partners to showcase the power of correlating data across the internet threat landscape. More than showing relationships between various threat actors, the additional intelligence available through the API can be demonstrated as well, including threat status, threat history, geo-location, certificate, WHOIS, and additional contextual information.

Partner Benefits

» Leverage the full power of the Webroot® Threat Intelligence Platform

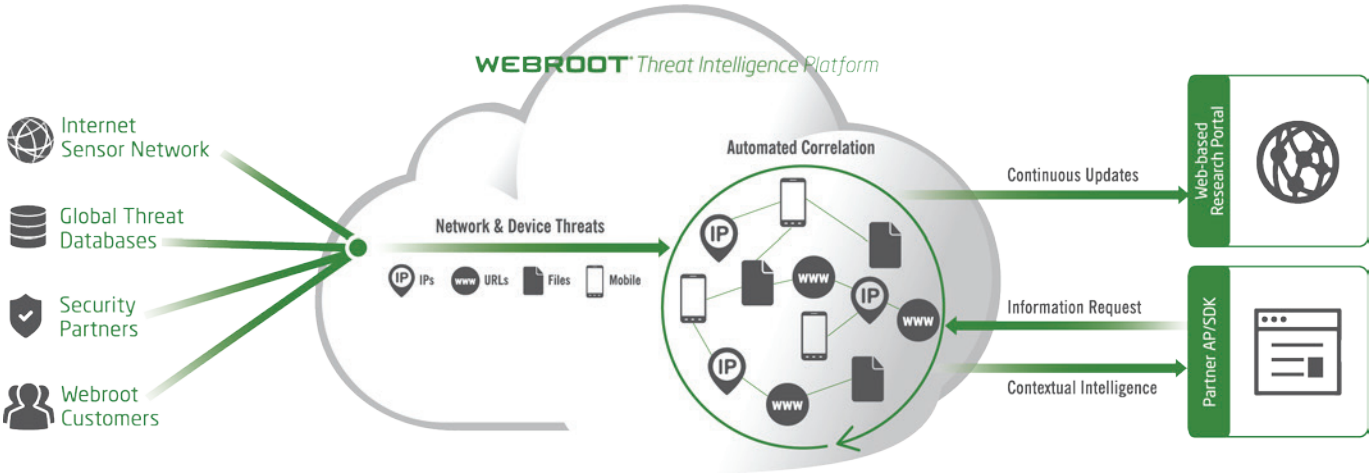
» Understand why a specific IP, URL, file, or mobile application received its reputation score, including threat status, history, geolocation and other contextual data points

» Use the BrightCloud Threat Investigator as a demonstration tool to tout the benefits of the threat intelligence used by your security solution

» Differentiate yourself from your competition

» Leverage the ability to offer more in-depth insight and investigative information to your customers in order to proactively protect their networks and endpoints

The BrightCloud Threat Investigator provides contextual intelligence around a URL, IP, file, or mobile app under investigation.



BrightCloud® Threat Investigator

BrightCloud Threat Investigator in Action

» Provides customers a compelling way to investigate and understand why a risk score was provided via rich metadata around the primary connections and influences surrounding a specific IP, URL, file, or mobile application

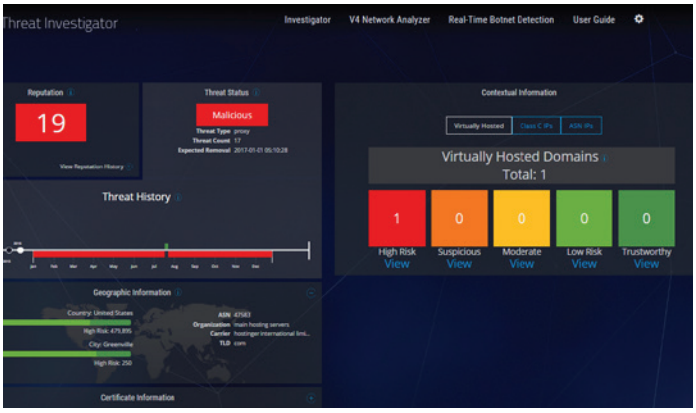
» Empowers customers to take proactive protective measures by blocking other malicious IPs, URLs, files, or mobile applications related to a particular threat actor under investigation

» Demonstrates why a specific IP, URL, file, or mobile application received its reputation score, including threat history and other contextual data points

Easy Integration

Using our intuitive software development kit (SDK), REST services, and API, partners can easily integrate the BrightCloud Threat Intelligence Services into their own solutions. The BrightCloud Threat Investigator is available for Webroot technology partners using the BrightCloud SDK V5.20 and above as well as via BrightCloud REST APIs. This intelligence can be incorporated within the network device interface for the end customers' use.

BrightCloud® Threat Investigator provides contextual intelligence on the relationships between IPs, URLs, files and mobile apps



Additional intelligence is made available for each threat actor

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