BrightCloud® Threat Investigator

BrightCloud Threat Intelligence Research and Investigation Tool

The BrightCloud® Threat Investigator is a web-based graphical user interface that allows threat response teams and threat researchers to see and understand the detailed contextual intelligence the Webroot® Threat Intelligence platform holds on individual internet objects including IPs, URLs, files, and applications. This additional contextual knowledge of an internet object under investigation helps threat teams better understand why a risk score was given, and enables them to implement proactive measures or automatically block known or potential threats.

As an example, a threat response team can now delve deeply into the relationships surrounding an IP address that was the source of a malicious file to determine exactly what type of threat it poses to their organization, how long it has been an active threat, its geographic point of origin, how it is related to other internet elements, and other insights into why it was classified as malicious. This information can be instrumental when determining the appropriate response to a malicious object that has infiltrated their organization.

BENEFITS OF THE BRIGHTCLOUD THREAT INVESTIGATOR:

» **Leverage the Webroot Threat Intelligence Platform**
Understand why a specific IP or URL received its reputation score, including threat status, history, threat types, geographic point of origin, and other contextual data points

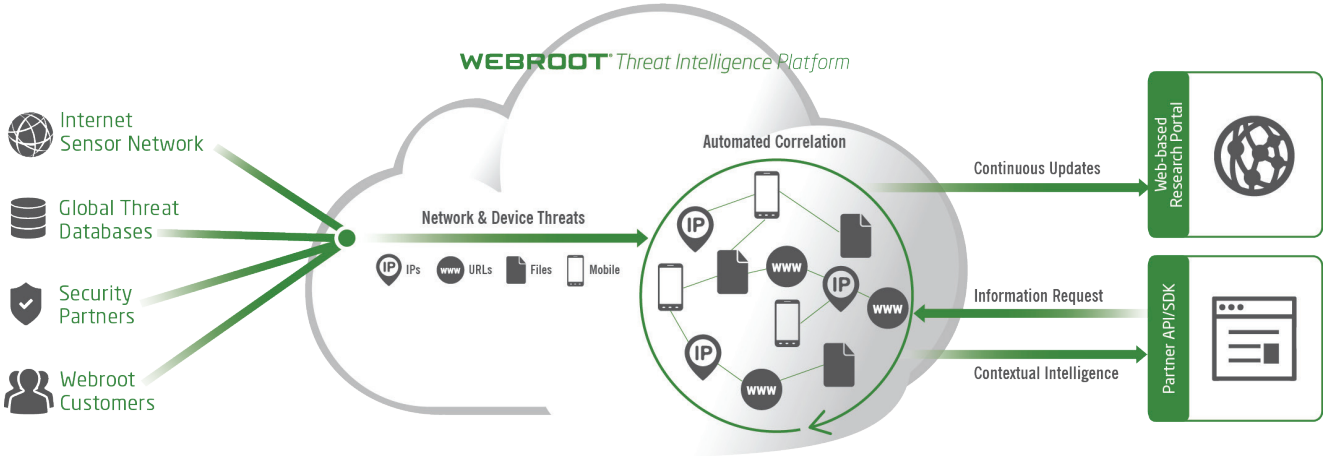
» **Add rich contextual knowledge on threats and related internet objects**
Take advantage of a compelling investigative platform to discern the primary connections and influences around a specific IP, URL, file, or mobile application

» **Gain insight in order to take proactive protection measures**
Get detailed insight and rich metadata to proactively protect your networks and endpoints from additional malicious IPs, URLs, files, and mobile applications related to threats and objects under investigation

» **Integrate intelligence into day-to-day operations**
Enable first responders and security research teams to access intelligence via an intuitive web-based graphical user interface directly from their desktops

The Threat Investigator is a new member of the Webroot BrightCloud Threat Intelligence Services for next-generation firewall (NGFW) and security information and event management (SIEM) family. These products leverage the Webroot Threat Intelligence Platform to provide organizations with an additional layer of real-time protection. BrightCloud for NGFW enables the proactive blocking of malicious IPs at an organization's perimeter, while BrightCloud for SIEM enables the correlation of an organization's inbound network traffic with real-time Webroot threat intelligence to first determine malicious activity, and then to prioritize the most critical events for immediate investigation and remediation. By blocking additional threats, and making efficient and effective use of security resources to save precious investigation and prioritization time, these solutions help limit potential IP and monetary loss, as well as damage to the organization's reputation.

The Webroot Threat Intelligence Platform is an advanced cloud-based security platform that is enhanced by a contextual database which identifies and evaluates relationships between internet object types. BrightCloud provides predictive and actionable information on both current and emerging threats across the entire 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.

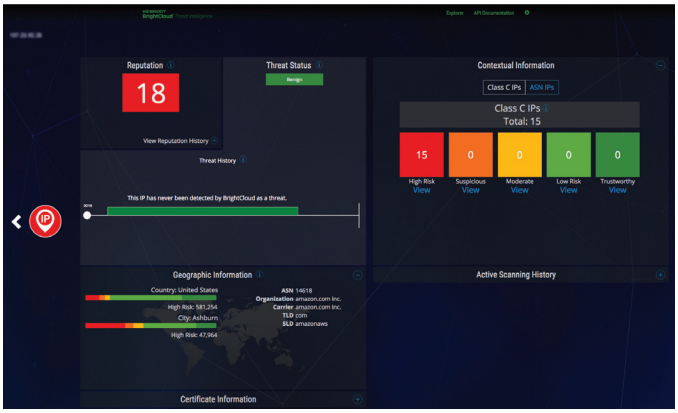


OVERVIEW

- Multi-vector intelligence is necessary for threat investigation and proactive protection
- Contextual intelligence spanning threats from URLs, IPs, files and mobile apps provides insight into the relationships surrounding a specific object
- The BrightCloud Threat Investigator offers additional contextual threat intelligence and metadata on individual internet objects to help organizations make informed decisions on threats and take proactive protective measures

In addition to the visualization of relationships across the threat landscape, a wealth of meta-data is also available on individual objects. This includes reputation score, reputation history over time, and factors influencing reputation, such as age, popularity, and number of infections, current threat status, origin geolocation including ASN, organization and carrier, the date the threat was first identified by Webroot, types of activities the object has been engaged in, as well as the number of virtually hosted domains for a given IP address.

BrightCloud Threat Intelligence Services classify and identify malicious files, apps, URLs, and IPs in milliseconds. Enterprise security teams can



benefit from these services by integrating next-generation predictive Webroot threat intelligence into their network security solutions, such as next-generation firewalls or SIEM to improve their efficacy and efficiency in recognizing, investigating, and stopping known and unknown threats and attacks.

The BrightCloud Threat Investigator is available as a complementary service to subscribers of BrightCloud Threat Intelligence Services for NGFW and SIEM.

About Webroot

Webroot delivers next-generation 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 tens of millions of devices across businesses, home users, and the Internet of Things. Trusted and integrated by market-leading companies, including Cisco, 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