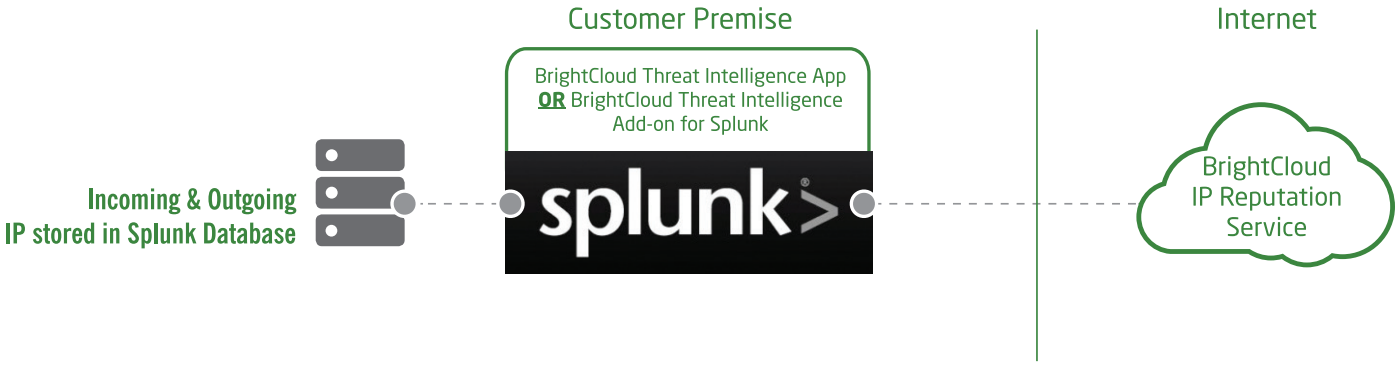
BrightCloud® *Threat Intelligence* for Splunk®



Today, cybercriminals have an immense number of exploits and attack vectors available to them, and they use numerous techniques to hide their identities and activities, such as encrypted communications, DNS cache poisoning, URL redirection, hyperlink obfuscation, and more. However, every packet on the internet has a source and destination IP address, so disabling inbound and outbound communications to and from IPs known to be malicious is highly effective. But how does one know which IPs to block? How can administrators differentiate between an employee chatting online with an associate in Eastern Europe from an attack on the corporate network? They need threat intelligence with global context and real-time updates to enhance their SIEM's detection of these threats.

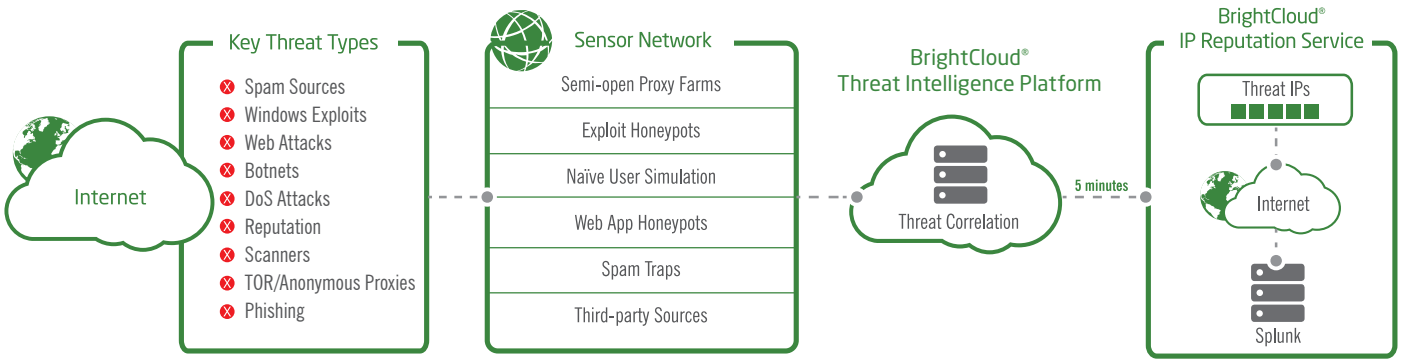
The BrightCloud Threat Intelligence App for Splunk and BrightCloud Threat Intelligence Add-on for Splunk enable enterprises to easily integrate BrightCloud IP threat intelligence into their Splunk environment with a continuously updated feed of malicious IP addresses. This allows Splunk Enterprise and Splunk Enterprise Security (ES) users to correlate malicious IP addresses with other data coming into Splunk, detect IP threats, and alert the security team before those threats lead to incidents, breaches, and data loss.

GLOBAL SENSORS AND CLOUD-BASED ANALYTICS

The BrightCloud Threat Intelligence App and Add-on are powered by the Webroot® BrightCloud Threat Intelligence Platform (BCTI). Unlike other single vector threat intelligence services, BrightCloud collects and correlates threat intelligence across multiple vectors – IP, URL, file and application – from a massive network of nearly 35 million users protected by Webroot® endpoint security solutions. BCTI also receives data from technology partners such as Palo Alto Networks, Cisco, F5, RSA, Aruba Networks, and Microsoft. BCTI is a cloud-based, big data analytics platform with 3rd generation machine learning that can analyze and correlate threat intelligence across these four vectors to six degrees of separation to provide the most comprehensive, accurate, and actionable IP threat intelligence available today, including up-to-the minute intelligence on IPs of emerging threats.

CONTEXTUAL AWARENESS

Brand new and unknown threats aren't on blacklists. They exist anonymously in the grey area between highly trusted IPs and known threats. Unlike static, rapidly out-of-date public blacklists, the BrightCloud Threat Intelligence Platform continuously monitors over 4.3 billion IPs across the world and updates the list of 12 million IPs that have been identified as malicious. BCTI identifies threats across nine threat types, such as botnets, exploits, scanners, spam sources, and more. BCTI tracks the relationships between the different threat vectors – URL, IP, file and application – and correlates that data to provide a more accurate threat score than single-vector blacklists. For example, a seemingly benign new IP, which other blacklists may classify as safe, may be tied to an URL with a history of phishing attacks, which automatically affects its IP reputation score. BCTI uses its correlation engine to proactively protect enterprises against threats that static blacklists can't detect. It can also help track known phishing proxies, allowing enterprises to block malicious requests from phishing sites, such as man-in-the-middle attacks.



BrightCloud® IP Reputation Service

INNOVATIVE PROSECUTION METHODOLOGY

To keep the list of 12 million malicious IPs updated and accurate, the BrightCloud Threat Intelligence Platform uses a prosecution methodology:

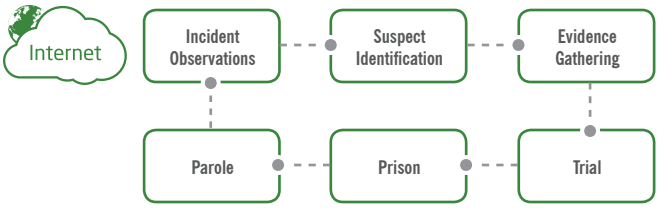
- Deploy an automated algorithm to identify suspicious IPs
- Examine the IP's activities and associations and correlate them
- Apply machine learning and automated classification algorithm
- Judge and sentence the IP as malicious for a term
- Re-evaluate IP after serving sentence
- Resentence or release IP on parole with heavy monitoring

BCTI uses this prosecution model to update the 12 million malicious IPs list every 5 minutes, accounting for changes, such as new malicious traits on previously benign IPs, or when formerly malicious IPs turn benign. Because this IP reputation data is dynamic, it has a higher efficacy and lower number of false positives than traditional, static blacklists.

EASY INTEGRATION

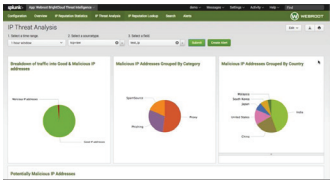
Customers can use the Webroot BrightCloud Threat Intelligence App for Splunk and the BrightCloud Threat Intelligence Add-on for Splunk to pull IP reputation data directly into Splunk Enterprise and Splunk Enterprise Security respectively to make the data available for correlation, analysis, and detection of malicious IP activities within their Splunk environments.

PROSECUTION PROCESS

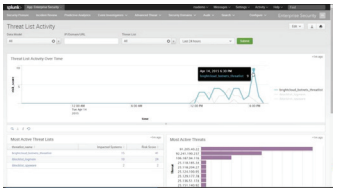


LEARN MORE

With thousands of new threats created every day and targeted specifically at stealing your data, real-time threat intelligence is more important than ever. With the BrightCloud Threat Intelligence App for Splunk and BrightCloud Threat Intelligence Add-on for Splunk, enterprises can easily integrate the most comprehensive and actionable IP threat intelligence into their Splunk Enterprise and Splunk Enterprise Security environments to detect IP-related threats. Contact a Webroot Threat Intelligence expert today to discuss how the BrightCloud Threat Intelligence Platform can protect your business against malicious IPs.



The BrightCloud Threat Intelligence App for Splunk provides out-of-the-box dashboards to correlate & detect malicious IP activities.



The BrightCloud Threat Intelligence Add-on for Splunk integrates with Splunk App for Enterprise Security dashboards to correlate & detect malicious IP activities.

About Webroot

Webroot provides Smarter Cybersecurity™ solutions. We provide intelligent endpoint protection and threat intelligence services to secure the Internet of Everything. By leveraging our cloud-based collective threat intelligence platform, computers, tablets, smartphones, and more are protected from malware and other cyberattacks. Our award-winning SecureAnywhere™ intelligent endpoint protection and BrightCloud® threat intelligence services protect tens of millions of consumer, business, and enterprise devices. Webroot technology is trusted and integrated into market-leading companies including Cisco, F5 Networks, HP, Microsoft, Palo Alto Networks, RSA, Aruba and many more. Webroot is headquartered in Colorado and operates globally across North America, Europe, and the Asia Pacific region. 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