AIRLOCK®
SECURE ACCESS HUB

WEBROOT®
Smarter Cybersecurity™

Airlock® Threat Intelligence

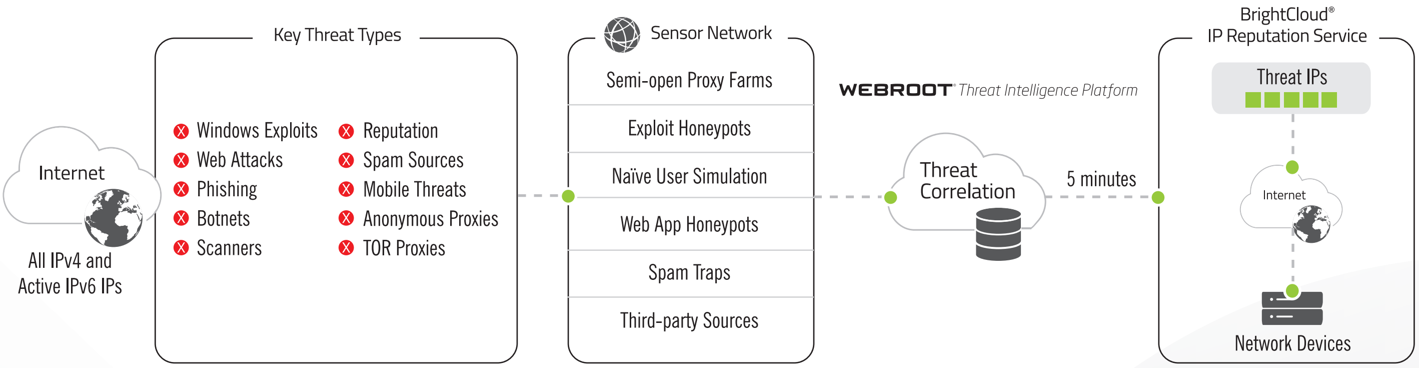
Targeted attacks against IT services are often global and coordinated. Many of the computers used for this purpose, such as botnet zombies, are not new to the game and have likely been causing trouble elsewhere before. Therefore, Airlock® integrates Webroot's® BrightCloud® Threat Intelligence Service to identify malicious clients in real time and block them before they do harm. The new IP address management features complement the threat Intelligence feeds perfectly, enabling the implementation of comprehensive IP-based access rules.

Threat Intelligence powered by Webroot®

Webroot's® BrightCloud® Threat Intelligence Service delivers high-quality, global threat intelligence feeds in real-time. IP addresses that perform attacks, belong to botnets, are infected with malware, send spam, are involved in phishing, or access via TOR and other proxies, are immediately blacklisted. Airlock® integrates Webroot's Threat Intelligence Service as a module and updates IP reputation data continuously. At the push of a button, malicious IP addresses can be blocked and prevented from accessing protected services.

Effective Security

Airlock seamlessly integrates Webroot's® Threat Intelligence Service. Based on the categories and trust levels provided, this automatically blocks dangerous clients and further increases application protection against misuse. Webroot® BrightCloud® Threat Intelligence Services is a proactive, automated security solution that provides effective, real-time policy enforcement against the latest threats.
The service is fully integrated including automatic data updates. There is no more need for time-consuming integration of the services into your own application landscape.



The benefits of the combination

The close integration into Airlock® provides many benefits for you: Threat information can be used in Airlock® for maximum security. On one hand they are used on the Web Application Firewall for blocking and labelling. In addition, the information can also be forwarded to back-ends, which can themselves build logic around it, such as selective transaction signing or fraud detection. Airlock® also seamlessly uses the data in the area of risk-based authentication. In addition, the threat categories are integrated in Airlock® Reporting and extend existing attack dashboards with valuable insights.

The Webroot® Plattform

The Webroot® platform uses machine learning, to discover, analyze, and classify 500 billion data objects every day, including 37,000 malicious URLs, 15,000 phishing sites, and 100,000 malicious IP addresses.

Brightcloud® IP Reputation

The BrightCloud® IP reputation service publishes dynamic information about high-risk IP addresses and provides insight into inbound communication with a dynamic blacklist of ~6 million malicious IP addresses and updates every 5 minutes. IPs are divided into 10 categories, including Windows exploits, phishing, botnets and spam sources.

Webroot® Threat Intelligence Features:

- Predictive intelligence enabled by our contextual database, combined with an unmatched historical database for additional threat insights
- Intelligence based on comprehensive global presence and rich, real-world data
- Continuously updated data in near-real time with reputation scoring and active threat status
- Advanced cloud-based, machine-learning with massive computing power and patented mathematical models coupled with human feedback, threat research, and threat reverse engineering.

Webroot Threat Categories

Spam Sources: IP addresses involved in tunneling spam messages through proxy, anomalous SMTP activities, and forum spam activities.

Windows Exploits: IP addresses participating in the distribution of malware, shell code, rootkits, worms, or viruses for Windows platforms.

Web Attacks: IP addresses using cross-site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force attacks to target vulnerabilities on a web server.

Botnets: IP addresses acting as botnet command and control (C&C) centers, and infected zombie machines controlled by the C&C servers.

Denial of Service: The denial of service category includes DoS, DDoS, anomalous sync flood, and anomalous traffic detection.

Scanners: IP addresses involved in unauthorized reconnaissance activities such as probing, host scanning, port scanning and brute force login attempts.

Phishing: IP addresses hosting phishing sites and sites related to other kinds of fraudulent activities.

TOR Proxy: IP addresses acting as exit nodes for the TOR Network. Exit nodes are the last point along the proxy chain and make a direct connection to the originator's intended destination.

Proxy: IP addresses providing proxy services, including both VPN and open web proxy services.

Mobile Threats: Denial of service, packet sniffing, address impersonation, and session hijacking