BrightCloud® Threat Intelligence for IoT Gateways

OVERVIEW

- Preventing threats from crossing the IT/OT threshold is a major concern for IoT centric organizations and device designers
- Disabling communication to and from malicious IPs and websites is a proven solution
- Webroot enables manufacturers of IoT Gateways to better protect their customers with up-to-the-minute threat intelligence

IoT gateways are emerging as a preferred network element to securely connect legacy and next-generation devices to the Internet of Things (IoT). They integrate technologies and protocols for networking, embedded control, storage, analytics, security, and manageability. However, many IoT gateways are built without sufficient security or intelligence to properly protect critical infrastructure.

BrightCloud® Threat Intelligence for IoT Gateways offers the most effective way to help Information Technology (IT) and Operational Technology (OT) security administrators secure their critical infrastructure and devices against network based threats. This high volume, high availability cloud service delivers real-time threat intelligence on malicious IPs and websites to IoT Gateways for added security. This includes the broadest, most up-to-date and accurate website content and reputation intelligence, and robust threat identification of 10 categories of IP-borne attacks such as botnets and command and control services.

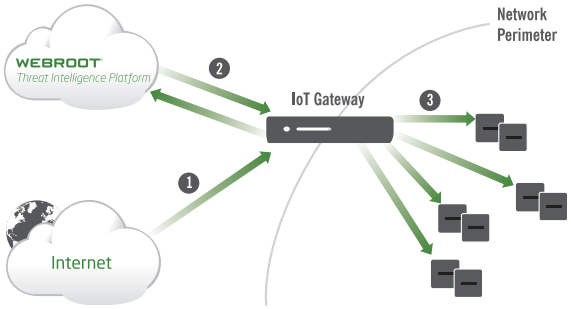
With this service, IoT gateway manufacturers can address customers' key concerns, including device integrity, IT, OT and bandwidth resources, as well as legal liabilities around network usage and compliance. Leveraging Webroot threat intelligence, IoT device and platform developers will significantly improve the effectiveness of blocking unwanted inbound traffic and also ensure that outbound communications are not being used for malicious purposes.

4+ Billion IPv4 and IPv6 addresses monitored, with a continuously updated list of ~ **12 million malicious IPs** at any given time

27+ billion URLs tied to **600+ million domains**, classified and scored, across 45+ languages

INBOUND PROTECTION

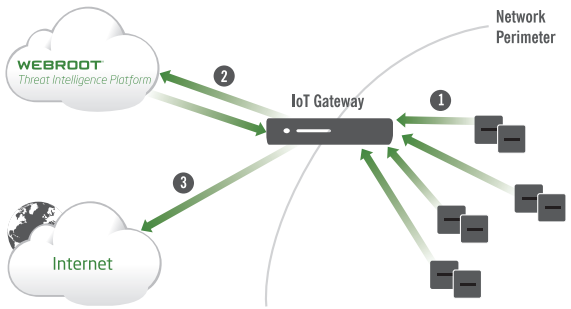
Webroot continuously monitors the entire IPv4 and active IPv6 space, conducting extensive analysis for many server born attacks. Everything from remote triggered threats—such as Windows exploits, web attacks, botnet and command and control servers—to passive attacks from spam sources and phishing sites are all categorized, tested, and re-tested daily, providing the most extensive and accurate list of malicious addresses for inbound blocking at the network edge.



Step 1: Internet address makes inbound request
Step 2: IP address looked up and validated in the Webroot Threat Intelligence Platform
Step 3: Non-malicious address allowed to communicate with network devices

OUTBOUND PROTECTION

To date, Webroot has scored and classified over 95% of the internet (over 27 billion URLs), generating the largest URL database of its type. This includes intelligence on malicious web categories relating to botnet, command and control servers, phishing URLs, known malware sites, and many URLs related to data exfiltration and hacking. With this data, policies can be created to allow security administrators to control where their IoT devices and gateways can connect, ensuring proper communication to approved data centers and remote sites.



Step 1: Device makes call to internet
Step 2: URL/IP address looked up and validated in the Webroot Threat Intelligence Platform
Step 3: Valid network requests allowed access to the internet

PARTNER BENEFITS

» **Differentiate yourself from your competition**
Offer industry-leading protection against malicious IP addresses and websites to finely tune security settings within IoT Gateways

» **Leverage Webroot® Threat Intelligence**
Harness the world's most powerful cloud-based security analysis platform

» **Flexible integration options**
Simple, flexible integration options let you use the latest web and IP reputation intelligence to suit your needs

» **No impact on device performance**
Devices are protected from malicious sites via real-time intelligence that won't impact network traffic

» **Low Risk**
Webroot has proven this technology with leading next-generation security appliances providers for over 10 years

BRIGHTCLOUD THREAT INTELLIGENCE FOR IOT GATEWAYS IN ACTION

Integrating Webroot Threat Intelligence into IoT gateways :

» Provides an additional layer of IP and web filtering protection from sites that host malware or spyware

» Enhances IoT gateways to increase real-time protection against known malicious threats, unauthorized network access and Denial of Service (DoS) attacks

» Enables IoT-centric enterprises to allow devices to communicate with reputable servers on the internet, while preventing access to low reputation or threat-based locations that may host malicious software or other threat types

PARTNER INTEGRATION OPTIONS

Using our intuitive software development kit (SDK), REST services, and an API, partners can easily integrate BrightCloud Threat Intelligence Services into their own solutions. The service integrates with existing security solutions through the same SDK as other BrightCloud services, making integration of multiple services easy. Depending on the business need, BrightCloud Threat Intelligence Services may be integrated in different modes, enabling partners to select the integration and deployment type best suited to their needs. The options are:

» **Hosted.** All IP and URL queries are sent over the internet to the Webroot Threat Intelligence Platform

» **Local Database.** A database is downloaded to the endpoint, no queries are sent to the Webroot Threat Intelligence Platform and the database is updated once daily

» **Hybrid Model.** All queries are first examined against a locally cached database. If the IP or URL category and reputation score are not stored there, then the query is forwarded to Webroot Threat Intelligence Platform for classification and scoring

Strategic partners across the globe have had tremendous success integrating BrightCloud services into their network solutions, from next-generation firewalls to network load balancers. Because BrightCloud services provide an uncomplicated integration, these solutions can be easily implemented.

Platform Compatibility

The Webroot Software Development Kit includes source code, and is compliant with the following platforms:

» **Operating Systems:**
- Linux®
- Microsoft® Windows™ Embedded
- Microsoft Windows 10 IoT Core

» **CPU Compatibility:**
- Intel, ARM, MIPS

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/IoT.

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