WEBROOT
an opentext company

The BrightCloud® Threat Intelligence SDK

Realize optimum value from BrightCloud services through our SDK

Overview

» Fully realize the value of real-time intelligence

» Expedite implementation of services

» Achieve higher efficiency and ensure consistent and accurate results across hundreds of thousands of daily updates

For partners who consume Webroot BrightCloud® threat intelligence, we highly recommend implementing the BrightCloud Threat Intelligence SDK to help leverage the full value of the services and ensure the best lookup performance, reliability, and efficacy possible. The SDK contains purpose-built functions that allow partners to expedite the implementation of BrightCloud threat intelligence.

Some partners who currently consume plain text threat intelligence feeds may hesitate to commit additional engineering resources to consume BrightCloud data via the SDK. However, based on our extensive experience, partners will find the upfront effort associated with SDK integration a worthwhile investment as they receive the best value from these services.

The Value of Real-time Intelligence

The BrightCloud SDK was developed in collaboration with Webroot's extensive partner network and represents a set of best practices for integrating the data into third party solutions that achieves the utmost performance. The Webroot® Platform's collection network is made up of over 95 million real-world sensors, representing the classification of more than 842 million domains, 37 billion URLs, 4 billion IP addresses, 36 billion file behavior records, and more than 31 million mobile apps to date. The SDK provides access to all of this data in real-time, requiring minimal memory, CPU, or disk resources. Having all of this data in the cloud allows access to the most up-to-date intelligence at the precise time of need.

The SDK allows users to automatically and seamlessly apply hundreds of thousands of real-time updates to the URLs and IPs published every day. In addition to the real-time benefit, the code implemented in the SDK is time-tested with proven reliability in tens of millions of hardware appliances for more than 10 years. The runtime performance of the code in the C++ object library provided by the SDK exceeds the performance of other delivery options due to the extensive, real-world testing specific to web filtering and the overall efficiency of the C++ language.

Clear text lists can never be as comprehensive nor updated as optimally as Webroot's cloud database, which is best accessed through the SDK.

The Value of Performance

The SDK allows users to leverage the full categorization capacities of the BrightCloud Web Classification and Reputation services, while also optimizing resources. Logic built into the SDK lookup routines around Longest Common Prefix (LCP) and All One Category (a1cat) make the volume of URLs the SDK can categorize significantly greater than the number of URLs physically held in memory.

In addition, the SDK leverages a fixed-length MD5 hash lookup algorithm that provides significantly better performance than a clear text URL list lookup in memory. The SDK automatically validates and standardizes URL lookups, then converts them to MD5 hashes for faster lookup against an ordered MD5 database. Because of the standardized and sortable properties of MD5

Overall, the stability within the SDK strengthens both the threat intelligence and security posture of a partner's products.

hashes, partners using the SDK benefit from the efficiency of a hashed lookup versus a clear text lookup. URL lookups via the SDK also resolve a greater number of URLs than exact-match variable length text lookups in traditional memory maps.

Finally, the 3-tier caching mechanism in the SDK ensures continuous real-time synchronization between data in memory caches and our cloud databases. This is a critical component for implementing real-time threat intelligence, as it works to eliminate the data synchronization issues that accompany the ingestion of static lists. The patented SmartCache algorithm implemented within the SDK leverages different Time to Live values (TTLs) for cache entries based on categorization and reputation to optimize cache performance for filtering policy enforcement.

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.

The Value of User Experience

The SDK employs a modular design, so partners can choose which modules to use or not, depending on their specific needs. Similarly, the modules share the same logic, allowing for ease of use between them. We have refined the SDK's programming interface to three simple functions: Initialize, Lookup, and Shutdown. While these three functions satisfy most users' query and process management needs, the SDK is customizable for more specialized control, if desired.

The SDK also includes more complex tools, such as in-memory cache management, data synchronization, connection pooling, cloud communications, and retry logic, all of which are handled automatically.

Partner Benefits

» **Achieve higher efficiency**
In-memory cache management ensures the most efficient use of storage space by saving only the data needed, while connection pooling offers higher program efficiency.

» **Ensure better accuracy**
With data synchronization, partners benefit from more accurate categorizations, especially across updates to the data.

» **Enhance security through better responsiveness**
Cloud communications and retry logic ensure the BrightCloud services are responsive.

» **Take advantage of time-tested technology**
All of the tools within the SDK have been tested and honed over time to offer users greater efficacy and value.

Next Steps

Whether BrightCloud services are your first foray into threat intelligence or an enhancement of your solution, integrating through the BrightCloud SDK is the best way to offer you improved value in terms of real-time intelligence, performance, and user experience.

To discuss implementing the SDK within your environment, contact your Webroot sales representative or visit 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