CARBONITE an opentext company | WEBROOT an opentext company

BrightCloud® Threat Intelligence Cloud Service Intelligence

Enabling partners to identify and manage interactions with cloud services and associated applications

Organizations are increasingly turning to Cloud Access Security Broker (CASB) providers and other network and security technology vendors to address cloud service risks, enforce security policies and evaluate compliance with regulations, even when cloud services are beyond their perimeter and out of their direct control. CASB providers are expected to maintain a central location for policy and governance concurrently across multiple cloud services — for users and devices — and granular visibility into and control over user activities and sensitive data.

Cloud Service Intelligence addresses evolving security needs

Since many companies now rely on these cloud services to maintain a significant amount of data and infrastructure, the need for intelligence and visibility has increased. Webroot® BrightCloud® Cloud Service Intelligence enables technology and security vendors to enforce data-centric security policies to mitigate the risk of interactions with cloud services and associated applications. Using three components – Cloud Application Classification, Cloud Application Function and Cloud Application Reputation – partners can identify shadow IT, assess risks to information and data within a cloud service, and manage and monitor access to cloud services.

Users of BrightCloud® Cloud Service Intelligence information can identify cloud applications that pose security or compliance risks within these applications.

Three unique components with features to meet specific use cases

Webroot® BrightCloud® Cloud Service Intelligence has three components – Cloud Application Classification, Cloud Application Function and Cloud Application Reputation. These components can be embedded into a partner's solution to enforce data-centric security and compliance policies around cloud services and applications. Using BrightCloud® Cloud Service Intelligence, partners can:

- Identify traffic associated with cloud applications and distinguish between use of sanctioned and unsanctioned applications
- Classify and control access to cloud applications by their main purpose
- Track and govern specific actions being performed on cloud applications to identify and prevent data and information loss
- Assess the risk to information security from use of the application based on governance, compliance and security metrics.

Key Benefits

- Better address cloud application risks, and set up and enforce policies that pertain to usage of cloud applications
- Provides a more complete reputation score to better manage risk, including incorporation of the patent-pending Domain Safety Score that uncovers malicious content hiding on encrypted, benign domains
- Additional intelligence regarding cloud application use and reputation assists in data loss prevention and data discovery efforts, a critical element of cloud application deployment and use
- Assists in the ability to monitor data use and movement throughout an organization
- Saves time and resources of building a similar data set in-house, speeding up time to market and reducing development costs

Cloud Application Classification:
Each cloud application will be categorized based on its main purpose for businesses.

Cloud Application Function:
Each URL accessed in the operation of specific function within a cloud application will be categorized by that function.

Cloud Application Reputation:
Each organization governing a cloud application will be assigned a heuristic-based score. The score represents the reputation of the organization and the relative safety of data and information within the organization. The score can consider criteria such as application and data security, corporate governance, industry compliance and certifications, and historical security breaches. The score also incorporates BrightCloud's Domain Safety Score, a patent-pending technology that assesses the cybersecurity risk to users and networks from visiting a domain. This score is a unique capability that helps address the issue stemming from HTTPS protocols that have led to limited visibility at the webpage level. It allows organizations to better categorize malicious content that could be hiding on benign domains, whether encrypted through HTTPS or not.

Examples of use cases include:

- Cloud Application Classification to monitor network bandwidth directed toward different cloud applications
- Cloud Application Classification to enforce policies pertaining to access of specific applications based on sanctioned vs. unsanctioned activities
- Cloud Application Reputation to assess unsanctioned applications and determine new access policies
- Cloud Application Function to enforce policies pertaining to the movement of data across and within cloud applications
- Cloud Application Function to track abnormal activity related to cloud applications (e.g. excessive downloads)

Harnessing the power of BrightCloud® Threat Intelligence

BrightCloud® Cloud Service Intelligence is the latest offering within the BrightCloud® Threat Intelligence (BCTI) suite and is delivered via the BCTI API core service. The API uses many of the same access conventions as other BrightCloud APIs, including a unified authentication method, to streamline adoption for existing customers.

When combined with Web Classification and Reputation, BrightCloud® Cloud Service Intelligence offers a complete filtering solution that considers both the security and compliance concerns for online businesses and users.

Function classifications

- Login
- Search
- Upload
- Download
- Edit
- Share
- Create
- Delete
- Like
- Post

Category classifications

- Cloud file sharing
- Social networking
- Webmail
- Instant messaging
- Office document and productivity
- Streaming media
- Web meetings
- IT services and hosting
- Sales and CRM
- Payment
- Consumer
- Human resources

Contact us to learn more – Webroot US
Email: wr-enterprise@opentext.com
Phone: +1 800 772 9383

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.

© 2020 Open Text. All rights reserved. OpenText, Carbonite, and Webroot are each trademarks of Open Text or its subsidiaries. All other trademarks are the properties of their respective owners. DS_091120