

OpenText Threat Intelligence Cloud Service Intelligence

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

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 within encrypted and 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

Organizations are increasingly turning to Cloud Access Security Broker (CASB), Security Service Edge (SSE), Secure Access Service Edge (SASE) 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.

Connecting information with business processes is at the heart of OpenText™ Extended ECM. Extended ECM integrates into the widest range of enterprise applications and systems to eliminate content silos and ensure information is visible and available to all people, processes, and systems that need it. Behind the scenes, automated governance protects and secures content throughout its lifecycle. Information is current, quickly found, and easy to act upon.

Cloud Service Intelligence addresses evolving security needs

Since many companies now rely on cloud services to maintain a significant amount of data and infrastructure, the need for intelligence and visibility has increased. OpenText Threat Intelligence (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 OpenText Threat Intelligence (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

OpenText Threat Intelligence (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 OpenText Threat Intelligence (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 linked to the use of the application based on governance, compliance and security metrics

Cloud Application Classification:

Each cloud application will be categorized based on its main purpose for businesses.

Cloud Application Function:

Identify important actions undertaken by users within supported applications, such as data uploads and downloads. This gives our partners more granular control of what actions a user can perform within individual apps.

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 OpenText Threat Intelligence (BrightCloud) 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 within 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

Services

Consulting services

- Cloud file sharing
- Social networking
- Webmail
- Instant messaging
- Office document and productivity
- Streaming media
- Web meetings
- IT services and hosting
- Sales and CRM
- Human Capital Management
- E-Commerce and Accounting
- Identity and Access Management
- Website Builder

- 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 OpenText Threat Intelligence

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

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