OpenText Threat Intelligence Web Classification and Web Reputation Services

Real-time web threat intelligence accurately assesses URL and domain risk and helps enforce web policies

OpenText Threat Intelligence Classification Stats

- 1 billion domains and 43+ billion URLs classified
- 86 site categories, including high-risk categories
- 45+ languages

Overview

- Web threat intelligence enables security solution providers and enterprises to give internet users access to reputable websites while blocking access to malicious and inappropriate sites
- Website classification and reputation analysis protect users from malware, phishing, ransomware, and advanced attacks, while helping enforce compliant internet usage policies that reduce legal liabilities, improve employee productivity and protect children
- OpenText™ Threat Intelligence (BrightCloud) Web Classification and Web Reputation Services track more than 1 billion domains and 43 billion URLs, organize them into 86 categories, and assign them reputation scores based on multiple contextual and behavioral factors
- OpenText Threat Intelligence (BrightCloud) Threat Intelligence provides accurate and up-to-date intelligence by collecting data on more than 87 billion unique URL visits per year, analyzing data with sixth-generation machine learning models, and using innovative technologies to counter threat actor tactics such as encrypting web traffic, dynamically generating web content, and hiding malicious activities on legitimate websites and behind proxy servers

Goal #1: Protect Employees, Corporate Guests, and Consumers

Employees and guests on company networks routinely visit URLs that expose them to phishing attacks, keyloggers, botnets, ransomware and spyware, drive-by malware, and other threats. But identifying dangerous URLs isn't easy. Threat actors evade detection by rapidly cycling through new domains and URLs, dynamically generating malicious content on web pages that were previously safe, compromising legitimate websites, by creating sites that shift rapidly between malicious and benign. They also encrypt traffic (in 2022, about half of phishing sites used HTTPS) and hide behind proxy and geolocation services (70% of malicious URLs did so in 2022). Traditional, static, list-based internet protection services simply cannot keep up.

Goal #2: Reduce Legal Risk and Productivity Losses

Enterprises create internet usage policies in part to avoid legal liability when employees abuse web access to create a hostile work environment for their peers or violate compliance regulations. They also seek to control inappropriate web activities that affect productivity or waste corporate computing resources and network bandwidth. Enforcing these policies – without interfering with legitimate work or offending employees – requires granular, accurate, up-todate URL categorization and risk analysis.

OpenText Threat Intelligence (BrightCloud) Web Classification Service

By providing the most up-to-date and accurate website intelligence, the OpenText Threat Intelligence (BrightCloud) Web Classification Service significantly improves visibility into all internet usage and helps organizations mitigate online threats. Additionally, with the superior coverage and visibility offered by this service, security solution providers and their customers can address goals related to reducing legal liabilities around web usage and compliance, improving employee productivity, and reduce inappropriate use of enterprise computing resources.

With its 86 website categories, the OpenText Threat Intelligence (BrightCloud) Web Classification Service provides the granular insight customers require. Security solution providers can use these to help their customers accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as botnets and websites that attempt to bypass URL filtering with proxy servers and anonymizers.

Enterprises can also enforce internet access policies related to productivity (e.g., websites for online games, shopping, entertainment, news, sports, and hobbies), to IT resources (e.g., streaming media, peer-to-peer, personal data storage), to sensitive and controversial topics (e.g., drugs, pornography, gambling, weapons, illegal activities), and more.

OpenText Threat Intelligence (BrightCloud) Web Reputation Service

The OpenText Threat Intelligence (BrightCloud) Web Reputation Service delivers up-to-date risk scores for websites as users visit them. This enables security solution partners to add a dynamic layer of protection to their customers' web defenses by accurately assessing the risk posed when opening a URL, independent of its site category.

The Web Reputation Service complements the Web Classification Service by offering an additional lens, through which a site can be evaluated as a potential threat. In addition to category, it uses site history, age, rank, location, networks, links, real-time performance, and other contextual and behavioral trend data to determine a site's Web Reputation Index (WRI). WRI scores range from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious and High Risk.

The service also provides domain-level reputation scores based on the domain's threat history, age, popularity, underlying URLs, and other factors. These reputation tiers enable enterprises to finely tune their security settings based on their risk tolerance and to proactively prevent attacks by limiting the risk of end user exposure to inappropriate or malicious web content.

Domain Safety Score

The Domain Safety Score is available as an add-on to the Web Classification and Web Reputation Services. It can help address the issue HTTPS protocols may present, in which categorization at the domain level may not reflect the content of individual web pages within the domain. Domain safety scores help network and gateway devices that cannot decrypt SSL/TLS traffic or DNS solutions which only see FQDNs make better security filtering decisions in situations with minimal page-level visibility.

OpenText Threat Intelligence (BrightCloud) Platform

The OpenText Threat Intelligence (BrightCloud) Web Classification and Web Reputation Services are powered by the OpenText Threat Intelligence (BrightCloud) Platform. Data on new and known sites is continuously created and refreshed, every 5 minutes ensuring that site categorizations and reputation scores are always as current as possible.

Whenever a user visits an uncategorized site, it is dynamically crawled, classified and scored. Each website's score and classification are checked and adjusted over time.

The OpenText Threat Intelligence (BrightCloud) Platform is enhanced by threat hunting techniques, enabling accurate detection and classification of malicious URLs. OpenText Threat Intelligence (BrightCloud) uses a proprietary and fully automated deep crawling infrastructure for threat hunting, which is combined with contextual data to accurately categorize thousands of URLs per second. The proactive and methodical parsing of massive quantities of network data enables the OpenText Threat Intelligence (BrightCloud) Platform to uncover significantly more malware URLs and to determine that, on average, 91% of the new malicious URLs discovered each day are zero-day sites. With its highly sophisticated combination of global threat sensors, sixth-generation machine learning models, and multilingual human oversight, the OpenText Threat Intelligence (BrightCloud) Platform continuously maintains and expands its knowledge of threats and other website classifications, delivering maximum value for our partners.

OpenText Threat Intelligence (BrightCloud) Web Classification and Web Reputation Services in Action

Integrating OpenText Threat Intelligence (BrightCloud) Web Classification and Web Reputation Services into security solutions not only provides an additional layer of web filtering protection from sites that host malware or spyware, but it also enables security solution providers to offer far more granular security management. The services enhance our partners' solutions by increasing real-time protection against known malicious threats.

In addition, Web Classification and Web Reputation Services can help:

- Improve network speed by blocking unwanted and malicious content on integration partner gateways
- Power parental URL classification within a consumer internet security solution to help parents protect children against harmful and unwanted content
- Enhance or power URL filtering on secure web gateways, SSE/SASE services, next-generation firewalls and IPS systems, offering greater visibility and improved control over web browsing

Partner Benefits

Differentiate yourself from your competition

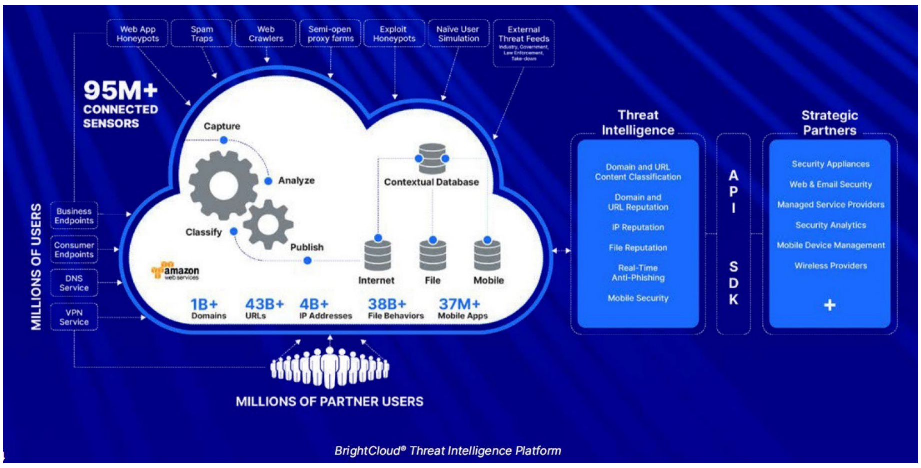
1. Enable compliance without impacting user experience
2. Protect with real-time and contextual intelligence visibility based on the foundation of AI and historical threat insights
3. Minimize customer risk by responding to evolving threats with faster speed and contextual accuracy

Resources

Contact us to learn more ›

OpenText Threat Intelligence (BrightCloud) ›

Phone: +1 800 870 8102



Leverage OpenText Threat Intelligence (BrightCloud) Threat Intelligence

- Take advantage of the visibility provided through more than 95 million real-world sensors via the world's most powerful cloud-based security analysis platform

No impact on user experience

- Protect end users from malicious sites using real-time intelligence in a way that won't impact their online experience
- Enforce internet use polices with greater accuracy
- Improve network performance with granular classification categories

Flexible Partner Integration Options

Web Classification and Web Reputation Services integrate seamlessly with existing security solutions through the intuitive OpenText Threat Intelligence (BrightCloud) software development kit (SDK), REST services, and an API. Multiple OpenText Threat Intelligence (BrightCloud) services can be integrated via the same SDK. Three hosting models are available, allowing partners to select the integration and deployment type best suited to customer needs:

Hosted:

- All URL queries not already cached are sent over the internet to the OpenText Threat Intelligence (BrightCloud) Platform for classification and scoring.

Local Database:

- A database is downloaded locally and fully updated once per day, with regular incremental updates providing the latest intelligence between full updates.

Hybrid Model:

- URL queries are first examined in a locally cached database and forwarded to the OpenText Threat Intelligence (BrightCloud) Platform only if the URL category and WRI are not stored there.