BrightCloud® Threat Intelligence Services Overview

Empowering defenders with comprehensive, real-time threat intelligence

Challenge

The ever-increasing volume, speed, and sophistication of cyberattacks requires a response beyond traditional security. Cybercriminals are continuously launching dynamic, stealthy threats designed to infiltrate network defenses through multiple attack vectors. Companies need solutions that are as dynamic as the attacks they defend against, to stay ahead in the ever-evolving threat landscape. Security solution vendors depend on comprehensive, reliable, real-time, actionable cyber threat intelligence to realize the full potential of their products and services in detecting and mitigating threats.

BrightCloud® Threat Intelligence Services provide unmatched visibility and insights into threats across URLs, IP addresses, file hashes, cloud applications and more. Our platform leverages sixth-generation machine learning models to deliver up-to-date, actionable intelligence. It offers the breadth and depth of data our technology partners need to keep customers and their assets safe. Our services are trusted by global network and security industry leaders and innovators, who use BrightCloud's predictive intelligence to keep their solutions and customers ahead of the ever-evolving modern threats.

Comprehensive, powerful, predictive, and proven

BrightCloud Threat Intelligence provides operational threat intelligence that is comprehensive, powerful, predictive, and proven. It features:

- Threat intelligence services covering multiple critical threat vectors
- A network of more than 95 million connected sensors
- A cloud-based platform that collects, analyzes, correlates, and disseminates threat data with remarkable accuracy and speed
- Predictive risk scores generated by analyzing and correlating multiple forms of threat data with sixth-generation machine learning models
- Integration with the world's leading technology and security providers

BrightCloud Threat Intelligence features a cloud-based platform that collects, analyzes, correlates, and disseminates multiple types of threat data with remarkable accuracy and speed and generates predictive risk scores using sixthgeneration machine learning models.

BrightCloud[®] Threat Intelligence Services provide technology vendors with comprehensive operational threat intelligence that is always up-to-date, highly accurate, contextualized, and actionable. BrightCloud does this through robust security offerings that cover web, file, and IP-based threats. These services are all powered by the BrightCloud Platform.

Web Classification and Web Reputation Services

BrightCloud's Web Classification Service and Web Reputation Service keep end users from visiting unwanted and unsafe sites by providing content classification and independent reputation scores for more than one billion domains and over 43 billion URLs. With 86 website categories, the Web Classification service enables partners to accurately identify websites that propagate malware, spam, spyware, adware, and phishing attacks, as well as websites with illegal or sensitive content, such as adult materials, drugs, and gambling. The Web Reputation Service delivers valuable contextual and behavioral information about websites, including the threat history of each domain, site popularity metrics, geo-locations, and networks associated with the websites. It also features a Web Reputation Index (WRI) with reputation scores that organizations can use to fine tune security settings. Using BrightCloud's categories, contextual information, and reputation scores, organizations can make their networks more secure, adhere to HR and compliance policies, and enforce effective web policies that protect users against web threats and prohibited content.

IP Reputation Service

The IP Reputation Service offers intelligence on more than four billion IPv4 and IPv6 addresses. It uncovers more than 600,000 new malicious IP addresses daily, as well as providing metadata and insights on each IP address that can be used to improve incident response and security analytics. The IP service is updated continuously, to thwart threat actors who rapidly cycle through new addresses. The service enables security solutions vendors and their customers to quickly detect web-based attacks, block traffic from malicious internet hosts, identify botnets and threat actor command and control systems, whilst finetuning security settings based on risk tolerance.

Real-Time Anti-Phishing Service

The Real-Time Anti-Phishing Service determines whether a website is being used for phishing at the precise moment a user encounters it. This provides live protection against zero hour phishing attacks, including those utilizing disguised redirection and recently hijacked websites. The service evaluates URLs and page content using hundreds of site attributes and contextual information, including the reputation of embedded links, the history of threats from the domain, and the length of time the site has existed. Advanced machine learning models ensure that results are useful and accurate with low false positive rates. The Real-Time Anti-Phishing Service allows organizations to improve the effectiveness of web, email, and network security solutions and defend against ransomware campaigns, spear phishing attacks, and fraud from newly observed phishing links.

Streaming Malware Detection

BrightCloud's Streaming Malware Detection technology detects malicious files containing both recognized and polymorphic malware. Thousands of files a minute can be parsed as they pass through a gateway, often without requiring complete files to be downloaded, avoiding undue network latency. Files can be blocked, allowed, or routed for additional investigation based on partner requirements. Streaming Malware Detection helps to prevent cyberattacks that involve malware, and it can also improve the performance of other security solutions by pre-filtering malicious files.

File Reputation Service

The File Reputation Service checks executable files against a cloud-hosted database of billions of known good and bad file behavior records so that integration partners can efficiently block or allow files or flag them for analysis. Files are collected from millions of real-world sensors and evaluated continuously using advanced machine learning techniques. Files are identified through a unique fingerprint, including those that are encrypted or password protected. The service also provides contextual information about files such as the date when they were first detected, how many times they have been detected by BrightCloud sensors, and the type of malware they contain. The File Reputation Service not only helps security solution vendors and their customers block malicious executables, it also helps cloud applications and service providers ensure that files already stored are free of malware.



The BrightCloud Platform

Cloud Service Intelligence

Cloud Service Intelligence enables security solution vendors and their customers to identify and manage interactions with both authorized and "shadow IT" cloud services and applications. As users interact with cloud resources, the service identifies and classifies services and applications, allows identification of unsanctioned "shadow IT" services, allowing partner solutions to track and control these interactions based on policies, while assessing the risk of the applications based on governance, compliance, and security metrics. Cloud Service Intelligence helps organizations enforce web access policies, control shadow IT, flag abnormal interactions, and reduce the risk of attacks through unknown and insecure web service providers.

A cloud-based platform designed for volume, accuracy, and speed

Threat actors are everywhere and move fast. Defenders need comprehensive intelligence and visibility so they can move faster. The BrightCloud cloud-based threat intelligence platform features limitless scale, lightning-fast data processing, and globally distributed service delivery for high performance and resilience. This infrastructure enables the platform to absorb data from more than 95 million global sensors and real-world endpoints while analyzing, correlating, and disseminating critical intelligence in real time.

Data correlation for contextual, predictive threat intelligence

BrightCloud® Threat Intelligence Services use a powerful contextual analysis engine and advanced artificial intelligence to map the relationships between billions of interconnected internet objects and services. Uncovering associations between an object and other URLs, IPs, files, cloud services and applications, and mobile apps allows the BrightCloud platform to accurately predict how likely it is that the object is malicious.

For example, an IP address that other services classify as safe might be tied to URLs and files with histories of dangerous behavior. BrightCloud's advanced analysis would provide a predictive reputation score in the "Suspicious" or "High Risk" range for this IP address, enabling security teams to examine or block communication with it and defend their organization against attacks from that source.

Trusted and proven Intelligence

Security solution vendors want threat intelligence that is current, actionable, and accurate. They want broad coverage of the threat landscape and context that explains why objects and behaviors are security or compliance risks. That's exactly what BrightCloud® Threat Intelligence Services provide, which is why they are trusted by the world's leading technology and security providers.

Partner benefits with BrightCloud[®] Threat Intelligence Services

• Effective cybersecurity

BrightCloud® Threat Intelligence Services enable our partners to provide proactive, automated cybersecurity solutions to their customers, solutions that deliver unobtrusive and effective security and policy enforcement to meet today's most pervasive threats.

Deep knowledge for superior protection

BrightCloud® Threat Intelligence Services leverage contextual intelligence and behavior analysis to overcome the accelerating pace of threat innovation. They power the mitigation of threats the moment they appear on any network or device connected to the BrightCloud Platform.

• Flexible integration options

BrightCloud® Threat Intelligence Services integrate with existing security solutions through the BrightCloud software development kit (SDK) and an easy-to-use REST API. Depending on the service, it may be integrated in any of three modes (hosted, local database, or hybrid), allowing partners to select the integration and deployment type best suited to their needs. Additional integration option information is available on each service's datasheet.

Learn More

Power your security solutions with the speed and accuracy required to protect your customers from new waves of sophisticated online threats. With BrightCloud® Threat Intelligence Services, you can overcome the next generation of internet-borne threats, protect your customers from malicious actors in real time, and stay at the forefront of cybersecurity technology.

Visit www.brightcloud.com to learn more.

Phone: +1 800 870 8102

opentext[™] | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_011924