BrightCloud Threat Intelligence

BrightCloud® Threat Intelligence Services

Empowering protectors with predictive, real-time threat intelligence

The ever-increasing volume, speed and sophistication of cyberattacks requires a move beyond traditional security. Today's cybercriminals are launching dynamic, stealth threats that are targeted and designed to infiltrate defenses through multiple entry points of a network. Technology and security vendors can't risk losing their customers' trust. They also can't afford to diminish the potential value of their own products and services as a result of unreliable real-time intelligence. Companies need solutions that are as dynamic as the attacks they defend against, so they can stay ahead of the ever-evolving threat landscape.

BrightCloud® Threat Intelligence Services provide unmatched visibility and knowledge across URLs, IP addresses, files and mobile threats. Our sixth generation, machine learning-based platform powers intelligence that is always up-to-date, highly accurate and offers the breadth and depth of data our technology partners need to keep their customers safe online. Our services are trusted by global leaders and innovators in the network and security spaces, who use our predictive intelligence to keep their solutions and customers ahead of modern threats.

Powerful. Predictive. Proven.

A three-dimensional approach is needed to provide threat intelligence that is powerful, predictive and proven. BrightCloud Threat Intelligence does this by having:

- Breadth of services to cover all critical threat vectors

- Cloud-based approach for volume, scale, depth and speed

- Greater accuracy and predictive risk scoring by correlating previously disparate data derived from real-world endpoints

- Integration with the world's leading technology and security providers

Cybercriminals are launching dynamic, stealth threats that are targeted and designed to infiltrate defenses through multiple network entry points.

Breadth of Services

BrightCloud® Threat Intelligence Services provide technology vendors with collective threat intelligence that is always up-to-date, highly accurate, contextual and actionable. BrightCloud does this through robust security offerings that cover web, file and mobile threats. These services are all powered by the BrightCloud Platform. Read more at www.brightcloud.com.

Web Classification and Web Reputation Services

These services provide content classification and independent reputation scores for billions of web pages to keep end users from visiting unwanted and unsafe sites. With 82 website categories, partners can accurately identify websites that propagate malware, spam, spyware, adware and phishing attacks, as well as websites with sensitive content, such as adult, drugs and gambling. Using these categories and reputation scores, organizations can achieve a more secure network, adhere to HR and compliance policies and implement and enforce effective web policies that protect users against web threats and prohibited content.

IP Reputation Service

The IP Reputation Service includes intelligence on millions of threat-related IP addresses and provides IP threat insights using a broad range of data to maintain a relevant and accurate dataset of scored threat IPs. Our dynamic database is continuously updated, meaning the information is used to finely tune security settings based on risk tolerance, proactively prevent attacks by reducing risk of end user exposure to malicious IP addresses and to enrich our partners' security data and products.

Real-Time Anti-Phishing Service

The Real-Time Anti-Phishing Service provides effective, live protection against zero-hour phishing attacks, with a focus on low false positives. It determines whether the site poses a phishing risk at the precise moment it is encountered, meaning the analysis and determinations are never stale.

Streaming Malware Detection

Designed to combat polymorphic malware, this innovative technology allows our partners' devices to make determinations at the network level to enable users to quickly allow, block or flag files for investigation.

File Reputation Service

This service provides dynamic file reputation intelligence on known malicious and allowed files to stop malware distribution and enable security teams to focus on actual or potential threats.

Mobile Security SDK

For enhanced mobile security, this SDK provides industry-leading protection against mobile threats with antivirus, antimalware, application scanning, quarantine management, device root detection and device risk scoring, offering significantly better protection than a simple, static block list approach.
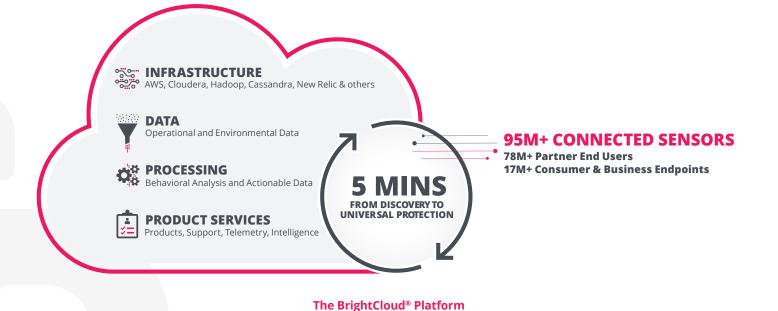
Cloud-based Approach for Volume, Scale, Accuracy and Speed

Most modern malware is created with a specific purpose and once its mission is complete, the threat disappears. Traditional, reactive, list-based security that works by recognizing known threats is ineffective against sophisticated attacks. That's why BrightCloud® Threat Intelligence Services use a proactive approach.

Through the BrightCloud Platform, data is fed into the cloud from millions of global sensors and real-world endpoints, where it is analyzed and correlated with other data points, to provide a comprehensive view of the online threat landscape.

That intelligence is then available to the rest of the network in real-time, including BrightCloud partners through BrightCloud® Threat Intelligence Services. The BrightCloud Platform features limitless scale, lightning-fast data processing and a globally distributed database cluster for high performance and resilience.

Data Correlation for Contextual, Predictive Threat Intelligence

BrightCloud® Threat Intelligence Services use a powerful contextual analysis engine that takes disparate data from BrightCloud Platform feeds and correlates it for deep insight into the landscape of interconnected URLs, IPs, files and mobile apps. Mapping the relationships between these different data points enables BrightCloud to provide partners with highly accurate, up-to-date and actionable intelligence. This also allows BrightCloud to accurately predict how likely an internet object is to be malicious in the future by its associations with other URLs, IPs, files and mobile apps. For example, a seemingly benign IP, which other services may classify as safe, may be tied to other URLs, IPs, files or mobile apps with histories of dangerous behavior. Our advanced analysis provides a predictive reputation score which enables users to proactively protect themselves through self-defined policies based on their risk tolerance. Each of the BrightCloud® Threat Intelligence Services benefits from this correlation engine to proactively protect users against threats that traditional technologies can't detect.

INFRASTRUCTURE
AWS, Cloudera, Hadoop, Cassandra, New Relic & others

DATA
Operational and Environmental Data

PROCESSING
Behavioral Analysis and Actionable Data

PRODUCT SERVICES
Products, Support, Telemetry, Intelligence

5 MINS
FROM DISCOVERY TO
UNIVERSAL PROTECTION

95M+ CONNECTED SENSORS
78M+ Partner End Users
17M+ Consumer & Business Endpoints

The BrightCloud® Platform

Trusted and Proven Intelligence

Security and technology vendors want to integrate threat intelligence that is current, actionable and accurate. Vendors want broad coverage of the threat landscape and context as to why objects or behaviors are a security or compliance risk. 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 Security**
  BrightCloud® Threat Intelligence Services enable our partners to provide a proactive, automated security solution to their customers, delivering unobtrusive and effective security and policy enforcement against today's most pervasive threats.

- **Deep Knowledge Equals Superior Protection**
  BrightCloud® Threat Intelligence Services leverage contextual intelligence and behavior analysis to overcome the pace of malware innovation, rendering the next generation of threats obsolete the moment a cyberattack appears 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 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 clients from a new breed of sophisticated online threats. With BrightCloud® Threat Intelligence Services, you can overcome the pace of malware creation and render the next generation of web-based threats obsolete; identify and protect your customers from malicious actors in real time; and secure an expanding corporate network perimeter with web, file and mobile security solutions.

Visit www.brightcloud.com to learn more.

[1] 2021 Webroot BrightCloud® Threat Report

Contact us to learn more
BrightCloud.com
Phone: +1 800 870 8102

About BrightCloud

BrightCloud was the first threat intelligence platform to harness the cloud and artificial intelligence to stop zero-day threats in real-time. The platform is used to secure businesses and their products worldwide with threat intelligence and protection for endpoints and networks. With more than 10 years of experience in building and analyzing the industry's most robust internet threat database, BrightCloud has the strongest coverage model, fewest uncategorized objects and the most historical records which others cannot replicate.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. As a whole, we are a market leader in cyber resilience, offering total endpoint protection and disaster recovery for businesses of any size.