WHITE PAPER

BrightCloud®
Threat Intelligence

Key considerations when selecting a web classification vendor

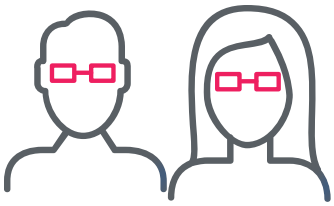
Intro

Since launching our web classification service in 2006, we've seen tremendous interest in our threat and web classification services, along with an evolution of the types and sizes of cybersecurity vendors and service providers looking to integrate this type of curated data into their product or service. Over the years, we've had the good fortune to work with partners of all sizes, from global networking and security vendors to innovative and dynamic start-ups across the world.

Your use case: how well does it align with the vendor?

Each use case is unique. Every vendor or service provider brings its own benefit to market and has its own idea about how their service or solution adds value for customers, clients or prospects. That's why our adaptive business model focuses on consulting with partners on technical implementation options, spending the time to understand each business and how it may benefit from a well-architected integration of classification and/or intelligence services.

It's essential, when looking for a threat intelligence partner, that businesses work with an experienced solutions architect to ensure their use case aligns with the data the vendor can provide, and to avoid any design or implementation pitfalls that may cause trouble for the business or its customers later on.

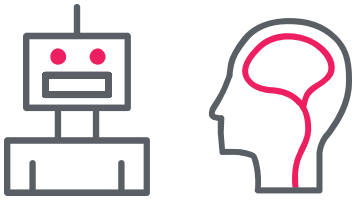


BrightCloud's team of senior solutions architects have experience guiding businesses through initial evaluations and proof-of-concepts through to implementation and operations of the integrated solution. When evaluating a vendor, it's important to consider all of the technical resources being provided to you, including the human talent involved.

Longevity and track record

A key factor influencing the constant change on the internet is innovation – every service provider is continuously enhancing and improving its services to keep pace with changes in the threat landscape, and with general changes to the internet itself. As well as keeping up with this change, it's important that a vendor brings a historical perspective to the partnership. This experience will come in handy in many ways. Scalability, reliability and overall business resilience should be expected from a well-established vendor.

At BrightCloud, we use our years of threat and classification data to ensure we have the most highly trained and accurate machine learning models in the industry. It's how we maintain our leadership in this space. From our beginnings with patented techniques to accelerate maximum entropy discrimination (MED) technology back in 2006, to today's use of multiple layers of machine learning and AI across our services portfolio, it's only through hard-won experience and continued innovation that we are able to bring maximum detection and prediction of threats to bare, and to ensure the accuracy of classifications for our partners.

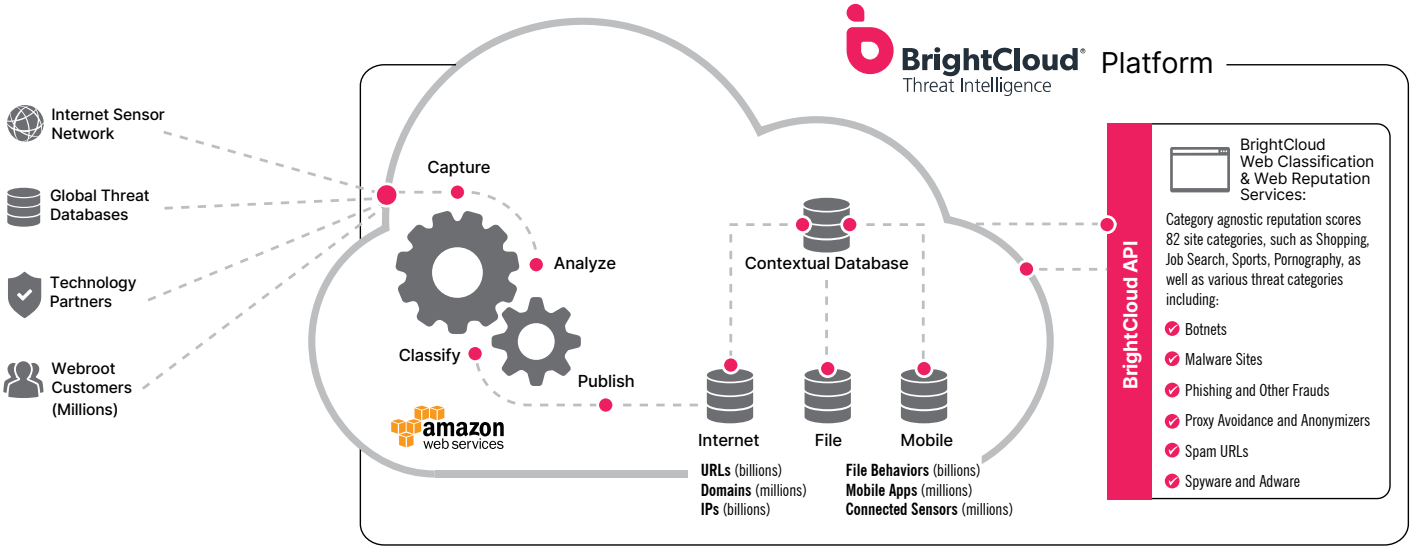


Industry Recognition

Fair comparative evaluations of web classification and threat intelligence providers are difficult to achieve. We can offer guidance to prospective partners here, but it's often more reassuring to simply see the strong partner relationships we have today. Many of these we've worked with for well over a decade. When evaluating a vendor, we recommend looking closely at current partners and imagining the investments each have made in their integrated solutions. This speaks volumes about integration performance and the quality of the partnership.

Here are some of the partners BrightCloud is proud to work with:

A10 Networks, Aerohive Networks, Airlock Secure Access Hub, Akamai, Anomali, Alcatel-Lucent Enterprise, Array Networks, Aruba a Hewlett Packard Enterprise company, Asian Link, Attivo Networks, Awake, Blancco, Cisco, Citrix, Centripetal, Circle with Disney, Clavister, Clearedin, Colortokens, CujoAI, Cyberinc, Cyberint, Cybersponse Adaptive Security, digital shadows_, DuoCircle, empow, f5, family zone, Fluency, Fujitsu 富士通ビー・エス・シー, GFI, GreatHorn, Hitachi Inspire the Next Hitachi Solutions, iboss, lastline, Light Point Security Browsing the web has never been safer, LogicHub, LogRhythm The Security Intelligence Company, MIBSID, ManageEngine, MCS 株式会社 MCセキュリティ, Menlo Security, NetMotion, Netography, nyansa, OPSWAT, ordr take control, Rohde&Schwarz Cybersecurity, Ruckus an ARRIS company, Securonix Security Analytics. Delivered., SaferNet Creating A Safer Internet, solarwinds msp, Technol, telenor, Threat Blockr, untangle, Varonis, Versa Networks, WebScale, Zerum Integrating Simplified, Zyxel Networks



Technology platform

A classification or threat dataset is only as good its sources and the analytics used to parse it. Many companies offer classification and/or threat intelligence data, but the quality of that data varies significantly.

Weakness in an implementation dramatically increase the error rate in the classifications or threat identifications made in the vendor platform, so we recommend vendors take time to understand how a classification provider gathers their data and the processes they use to analyze it. Poorly processed data will result in false positives, false negatives or other misclassifications, ultimately resulting in a product or service that's disappointing to customers.

BrightCloud has been evolving and integrating its platforms for 10+ years and our architecture today is second-to-none. We pioneered the use of the cloud for threat analysis and web classification and reputation, and we were the first to offer fully scalable classification of the entire web using machine learning. We were also the first with a fully cloud-managed endpoint security product that shares its findings and classifications to the cloud. This means we see and identify new real-world threats early across the risk spectrum and often allows us to be the first to classify new threats and dangerous URLs.

Threat Intelligence Capabilities

For our partners that require threat intelligence, it's critical they understand where their threat data comes from. There are now a great many sources of threat data, but again these are far from equal. Worse still, comparing source is often no simple task.

Any start-up can gather threat data; filtering, processing and republishing it for a profit. The true value of threat intelligence, however, comes from combining many sources of threat data with real user experience data to both add key detection and classification capabilities and to gain a contextual perspective for scoring external threats.

At BrightCloud, we are fortunate to have a unique combination of key advantages in this area:

First, due to the real-time, cloud-backed threat detection and remediation capabilities of our endpoint and network security products, we see first-hand new attack types when they hit "patient zero." This includes each of the multi-layered defenses built into our platform, including:

- DNS filtering
- Web filtering
- Real-time phishing detection
- Behavior-based intent determination

With this direct experience of new threats, we can determine the malware distribution URL, malware family, malicious behaviors and command-and-control (C2) URLs and IPs. These data points are then fed straight to our cloud platform for analysis and contextualization.

Second, we benefit from being the first to harness machine learning-based classification and malware detection for the entire internet. Our highly evolved machine learning models, some which are generated daily via supercomputer, provide visibility over the latest threats as we deep crawl across the web, analyzing potential attacks seen by users and partners through millions of endpoints around the globe.

Finally, a decade of pioneering threat research and classification in the cloud has given us the most highly evolved and massively scaled big data threat analytics solution in the industry. Using the BrightCloud® Platform, we can detect the latest threats and predict the next wave of new ones, helping our customers limit their exposure to risk and allowing our partners to deliver superior detection and classification capabilities to their users.

Ease of integration

As mentioned, every use case is unique. So are the platforms into which web classification, malware detection and threat intelligence services are integrated. It's therefore crucial that any vendor provide flexible integration options that can accommodate any pioneering partner, service provider or systems integrator. Simply providing data via an API is useful, but will it always deliver the performance required for real-time applications? Delivering a local database of threats or classifications may help with performance, but what about new threats? Achieving a balance of flexible delivery, performance and security is crucial, so take time to discuss with potential vendors how they plan to deliver.

BrightCloud's sixth generation threat intelligence SDK seamlessly delivers classification and threat intelligence services to our partners. This refined implementation tool makes it easy for partners to get maximum value from our services without sacrificing performance or classification accuracy. Use of the SDK is not mandatory, however. Vendors may choose to call our cloud API directly, or to run our daemon locally within the implementation environment to benefit from the multiple layers of intelligence caching and query optimization it provides.

Phishing Detection

Phishing sites are some of the most dynamic and short-lived attack platforms on the web, so intelligence sources must be capable of detecting and tracking them in real-time. Most phishing intelligence sources depend on manual submissions of phishing sites by end users. This is far from ideal. Users are prone to error, and for every 10,000 users who click on a phishing site only one will report it to an authority or tracking service, leading to massive under-reporting of this threat vector.

Today, 95% of all attack campaigns begin with a phishing email. Many of these lead the user a lure page in order to capture their credentials or deliver an exploit or malware payload. How does a potential vendor detect and block these threats?

BrightCloud has been developing phishing detection machine learning models for more than a decade. Our dynamic, rapidly evolving platform harnesses the power of the San Diego Supercomputer Center plus our global endpoint data sources to track developing threats. We continuously evaluate and tune our performance to stay ahead of both these threats and the competition.

Category coverage: beware category overload

There are various approaches to classifying the web and different vendors specialize in different areas. In many cases, this is determined by the data sources they have access to or the markets in which they operate. Again it's important to evaluate the partners to whom the vendor is delivering services and to consider how the vendor may or may not add value to the partnership.

When looking at the available categories, quantity does not always equal quality. We often see vendors spreading themselves too thinly or being too keen to add new categories to their services in order to fulfil a perceived need.

Our partners depend on the consistent performance of our services, but also the consistent delivery mechanisms of our services.

For us, this includes the selection of categories we include in our web classification service. More than 100 partners have integrated our classification and/or other threat intelligence services, and we ensure that once they have completed their integration they are not burdened with constant requests to update or change their implementation. This allows them to focus on developing their own products or services without distraction from us as a vendor.

Efficacy and performance

Efficacy is fundamental to web classification or threat detection capabilities, so it should be a core criterion when evaluating a vendor. Depending on the use case, false positives or false negatives may be the primary concern when making determinations. Potential vendors should be evaluated for performance in these areas and asked how they approach continuous improvement.

Outright performance is actually relatively easy to test. Discuss with vendors the performance metrics they share and consider what performance testing to undertake during a proof-of-concept exercise. Consider how local caching solutions or data delivery mechanisms may affect both efficacy and performance of the solution. These often play against each other, so it's crucial the vendor strikes the right balance.

BrightCloud was first to the cloud for delivery of these solutions, and our architecture is highly evolved, mature and stable. We have a long track record of satisfied partners to help vouch for the quality, efficacy and consistency of our services. Still we continue to innovate to stay ahead of an evolving threat landscape.

Reliability

Building any third-party service or solution into a product, platform or service entails risk. There's always the chance the new dependency negatively affects the performance or user experience of a service. So it's importance to ensure a vendor can reliably deliver consistent performance. Examine each's track record and customers base, along with the use cases they've previously implemented. Do the vendor's claims match the available evidence? Can current customers be contacted about their experiences with the vendor?

On top of delivering intelligence and classification services to partners, BrightCloud also operates globally delivered cloud services that power our own products and protect millions of users in real-time. Any reliability issues quickly become apparent to us as a service provider. We're also uniquely situated to understand the scalability and reliability of our platform compared to competitors that serve only integration partners, rather than end users directly. We see this as a unique asset and validation of our approach.

Scalability

In assessing vendors, it can be difficult to determine the level of scalability possible with their platform. It helps to ask questions about how they build and operate their services, and looking for examples where they've responded to unexpected growth events that can help demonstrate the scaling capabilities of their platform. Be wary of smaller or upstart vendors as they may have difficulty when their platform is heavily loaded or when called upon to grow faster than their existing implementation allows.

At BrightCloud, our experience of massive scale deployments using the latest cloud-native delivery mechanisms is unrivaled. We deliver not only to our partners, but also to millions of end-users across the consumers, small and medium-sized businesses and large enterprises.

In 2019, BrightCloud was acquired by OpenText, a global leader in Enterprise Information Management. OpenText helps organizations tackle the most complex digital transformation programs with confidence. With the world's most complete and integrated Information Management platform, we empower our customers to organize, integrate and protect data and content as it flows through business processes inside and outside their organization.

Our innovative OpenText Security and Protection Cloud solutions enable organizations of all sizes and consumers to be cyber resilient by detecting, investigating, preventing, and protecting against the ever-increasing attack surface. Integrating our award winning on-premises, hybrid and cloud-based products, we offer the industry's most comprehensive data security and data management solutions to help our customers be secure, productive and compliant with regulatory requirements.

Operating at scale is now our mission, as we enter an unprecedented stage of growth and innovation, allowing us to deliver to existing markets while expanding into new ones.

Flexibility

Some solutions may look technically sound, easily accessible and well-documented while a mutually agreeable business model remains elusive. Conversely, an agreeable business model may not be backed by the efficacy or quality of service that desired from a chosen vendor.

BrightCloud has over a decade of experience of working with a wide range of partners, from global enterprises to start-ups, government organizations and beyond. We understand the business and operational challenges facing businesses of all sizes, and we take time to take find workable billing and pricing structures for partners. Successful partnerships are the priority. This approach has helped us build relationships that withstand the test of time.

Feedback loops: making the best better

We're often approached by contacts asking us for a "feed" of some kind. It may be a feed of threat data, malware information or classifications. In fact, many of our competitors simply push data for customers or partners to consume as their "product." But this approach has inherent weaknesses.

The nature of the internet and its threats means that staying ahead is a monumental challenge. Without a self-correcting feedback mechanism and the ability to uncover zero-day threats, vendors can't possibly deliver the efficacy needed to make a difference with an integrated solution.

BrightCloud provides a dynamic service, not a feed. This involves delivering threat and classification data that's not stale. Instead it ensures new threats are detected and remediated quickly. Without this feedback mechanism, any solution is doomed to failure. Delivering it without sacrificing performance or flexibility is another unique BrightCloud strength.

When automated feedback or oversight is not enough, our global team of expert threat analysts steers our automation. With their help, we respond quickly to meet customer expectations. An elite team of technical post-sales support experts is also on-hand to help with queries about evolving your implementation. In evaluating providers, be sure to understand who's really there to help when needed.

Partnership: not just a customer relationship

As mentioned, we seek to build strong partnerships with mutual long-term benefit. Look for this approach when considering a vendor, knowing you'll likely be working with them for a long time and fewer changes to your vendor lineup mean more time optimizing your products and services. Ask yourself: Who will we be working with? Do we trust them? How easy are they to get ahold of? These are critical considerations when selecting a vendor for your business.

Finding ways to benefit client relationships is key for BrightCloud. Whether in terms of marketing, technical resources, product innovation or thought leadership, we believe our partners' successes are our success.

Summary

We hope to have provided some food for thought when it comes to selecting an integration partner. We're always standing by to discuss prospective clients' needs and to provide any possible guidance regarding our services. We're here to help you craft the best possible solutions and services. Please contact us to take the next step towards an even more successful future.

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.