WEBROOT
Smarter Cybersecurity™

Multi-vector Internet Threat Intelligence for the Anti-Fraud Market

Protect your network and your customers

Introduction

As fraud tactics become increasingly advanced, and as criminals become more aware of the tools that could detect and prevent their activities, the security industry must continue harnessing new techniques to enhance the levels of defense we can provide. That's why Webroot is bringing the benefit of real-time threat intelligence across multiple vectors of attack to the anti-fraud market.

Partnering with leaders in the anti-fraud space, Webroot empowers service and solution providers to add even greater value to their products and services through accurate and timely threat intelligence services. This document describes how Webroot is uniquely well-placed to service this market, and provides an introduction to the various services available.

Webroot® Threat Intelligence

For over 20 years, Webroot has maintained a proven track record for delivering industry-leading threat intelligence, award-winning endpoint security services, and market-leading support. As the first security service provider to move its protection and intelligence engines into the cloud, and as pioneers in the use of advanced machine learning and classification techniques, Webroot has a unique and unrivaled perspective on active threats.

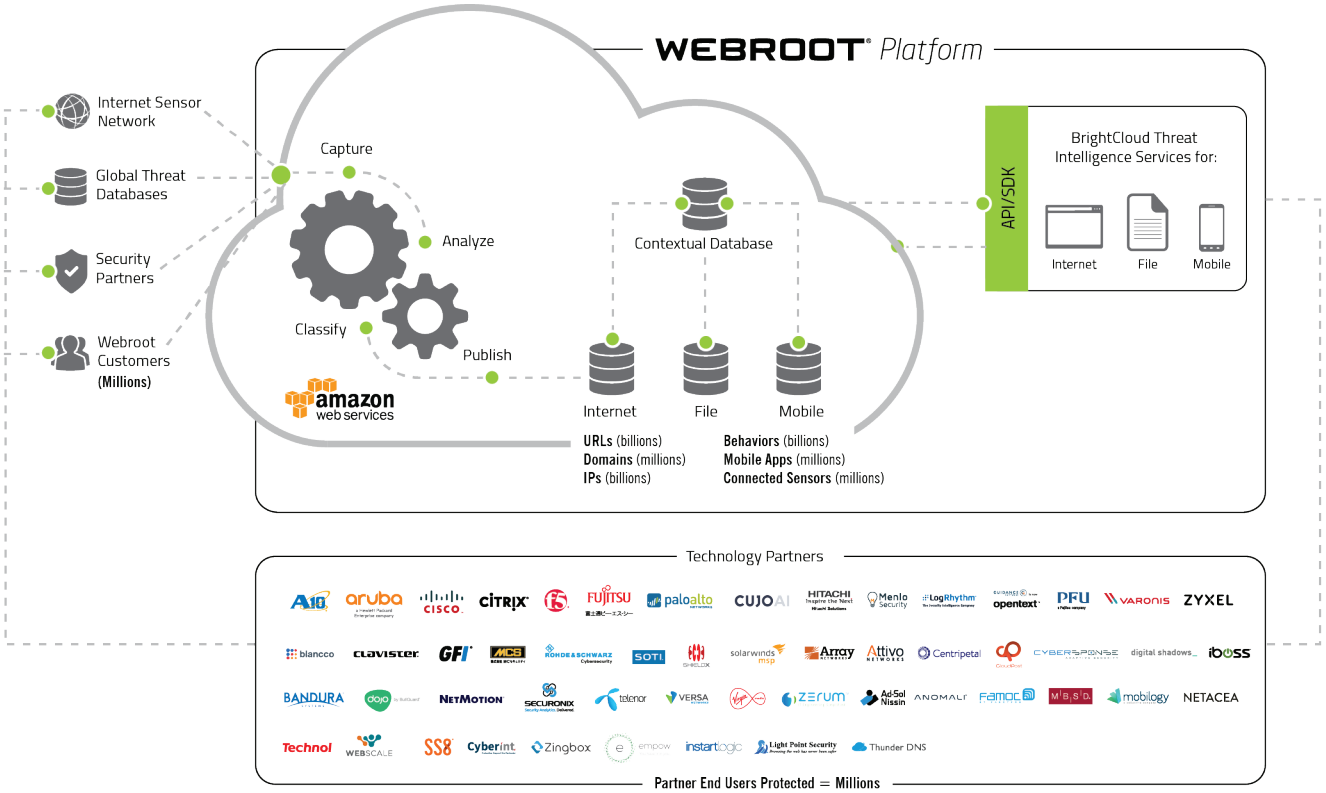
By combining zero-day threat detection, malware behavior analytics, and internet classification, and reputation services—all powered by advanced machine learning hosted on big data cloud platforms—Webroot BrightCloud® Threat Intelligence Services enable partners to enhance and add value to their products and services. In fact, more than 80 leading security and network vendors around the globe integrate Webroot threat intelligence.

With over 6 petabytes of data and growing, including over 32 billion classified URLs and billions of IP addresses and files, the cloud-based Webroot® Platform is designed from the ground up to produce real-time, accurate, and actionable threat intelligence around URLs, IP addresses, files, and applications. Data from globally distributed endpoint security agents, protecting millions of real users across all market segments, is combined with active web crawling techniques, IP address scanners, and a global passive sensor network. All of these data sources feed into the platform, along with multiple other external data sources. All of this data is analyzed and correlated within the platform to enhance accuracy, while also allowing for prediction of previously undetected threat sources.

The unprecedented scale, real-time response, and performance of the Webroot Platform gives anti-fraud providers the edge they need to provide world-leading risk assessment and protection services to their customers.

In the first quarter of 2018, RSA found that 65% of fraud transactions originated from a mobile device.[1]

[1] RSA Quarterly Fraud Report, Q1 2018



The Webroot® Platform

Casting a Wider Net

To uncover the latest threats from URLs, IP addresses, applications, and files, Webroot benefits from being the leading provider of threat intelligence to the cybersecurity industry. Through the relationships with over 80 cybersecurity vendors forged over a decade of collaboration, Webroot has visibility into new URLs seen by tens-of-millions of partner-protected users as the devices that protect them make lookups to our API services, allowing us to crawl, classify, and identify threats as they arise.

Additionally, the techniques we use to protect our own endpoint security customers from phishing attacks allow us to detect and block phishing URLs as soon as any user attempts to access them, anywhere in the world. Webroot leads the industry in real-time phishing detection and prevention, utilizing advanced machine learning techniques to implement highly accurate detection and target identification on a global scale. Webroot is proud to bring the benefits of this technology to the fraud protection marketplace.

Protecting Online User Interactions

Reliable session-level risk assessment for fraud protection is very challenging. Webroot is uniquely positioned to provide a range of actionable threat intelligence services that add significant value in this ongoing battle against fraudulent use of online services.

To understand the risk during online user interactions with any financial service, it is essential to analyze as many data points as possible. The Webroot approach to user session analytics for risk analysis and fraud prevention comprises three key pillars:

1. User Source IP Analysis
2. Referring URL Analysis
3. User Environment Analysis

These three components are delivered in the form of SDKs and/or cloud-hosted web APIs, whereby queries and scans can be performed and the data can be interpreted and acted upon however the Webroot integration partner or their end customer chooses. These service components are as follows:

User Source IP Analysis

The IP address being used by an end user for their activity can be a good risk indicator for many reasons. For example, if a user is transacting from a public WiFi hotspot that is often used to compromise the privacy of its users, there is a high likelihood that Webroot will have detected malicious activity from the IP address of this location and blacklisted it in an appropriate threat category, and/or will have reduced its reputation score to reflect its high-risk nature.

Protect your network and customers through:

① User Source IP Analysis

② Referring URL Analysis

③ User Environment Analysis

Webroot can supply its partners with a real-time IP blacklist which is continuously updated with new threats throughout the day. This blacklist contains millions of malicious IPs along with their classifications and reputation scores, allowing for granular, risk-based assessment of allowing a user to transact from a blacklisted IP. The blacklist has granular categories and can be used to screen users who are hiding their identity or location via TOR or proxy services, as well as to identify users coming from IP addresses that are actively being used for web attacks or other malicious activities.

Webroot also provides IP reputation scores for all 4+ billion IPv4 addresses via our cloud API—whether blacklisted or not—which can be another important indicator when determining the risk of allowing a user access to a financial platform, and when assessing transaction risk. Finally, Webroot provides geolocation and ASN/ISP-related data for all IP addresses, which can also be used for geo-analysis, geo-fencing, or assessment of whether the session is originating from within a virtual hosting environment.

By combining these data points, anti-fraud partners can create innovative services, such as one that detects account takeover attacks and other threat types, delivering proactive security to their customers. IP threat data is backed up by detailed threat history information, also accessible via our API.

Referring URL Analysis

When a user first lands on a website, their browser provides data detailing the URL the user was on before being forwarded to the protected site. This data, provided with a "REFERER" header, can be retrieved at the web server or application delivery controller, and can provide a valuable risk/threat indicator for the session. Because Webroot is the leading provider of granular web classification and reputation services, we are ideally placed to provide insight into any risks associated with the referring URL.

Webroot offers SDK, local database, and cloud-based API solutions to enable partners to implement high-performance URL risk assessments, based on a platform that has classified over 750 million domains covering 32 billion URLs globally to date.

User Environment Analysis

If a user's device is compromised, there is a high likelihood that their financial transactions are being monitored, as well as a significant chance that they or their sessions are being manipulated to divulge sensitive information or even transfer money to fraudsters without the user's knowledge.

When a user downloads an app for interacting with a financial service, the anti-fraud service provider has a unique opportunity in terms of being able to make an assessment of the suitability of the user's mobile device when requesting service access or making a transaction. Webroot focuses on the high-risk Android™ mobile operating system and provides an Android Mobile Security SDK, which allows anti-fraud partners to screen the user's mobile device to determine the device's security.

Device-borne threats that can be detected through the Mobile Security SDK include malware apps (banking Trojans, "wrapped" fraudulent applications, etc.), potentially unwanted applications, and rooted devices. The Webroot® SDK collects this threat data on the device itself and provides it and a risk score to the anti-fraud partner via their own SDK or app, which is built to contain the SDK.

Protecting User Transaction Environments

Webroot® endpoint security solutions provide multi-vector protection for end users against online fraud attempts. From integrated keylogger and man-in-the-browser protection, to real-time phishing detection and behavior-based malware detection, as well as a variety of other advanced capabilities, there is no better fraud prevention solution for end users who access sensitive services.

Webroot has partnered with the anti-fraud industry to deliver leading endpoint protection solutions to protect the Windows® and MacOS® computers used by the end customers of leading financial institutions around the world. Banks typically offer their customers Webroot security as a value-added service, and strongly recommend their users deploy the security software to protect themselves.

Impact analysis has shown that even a modest adoption rate amongst a user community can result in a significant reduction in fraudulent account activity. The explanation for this is that the highest risk user population is also the population of users who are most likely to install free software that is provided to them by an institution they trust.

Webroot believes that endpoint security is paramount in the battle against online fraud, and we have engineered our groundbreaking protection with this in mind.

Proactive and On-Demand Detection of Targeted Phishing Attacks

Phishing sites are notoriously difficult to locate and detect, both for users and cybersecurity service providers. This is especially true when relying on lists of known phishing sites, which are often three to five days old by the time they are published. According to Webroot threat research, the majority of phishing sites are live for only 8 to 12 hours, sometimes for less than 1 hour. Webroot has brought advanced machine learning to this battle, and has built specialized models to differentiate phishing content from legitimate content on the web. Using the power of this Real-Time Anti-Phishing service, Webroot fights back against phishing in three distinct ways:

1. Webroot protects endpoint security users from phishing attacks in real time, whenever they visit a malicious site, even if the site itself has never been seen before.
2. The Webroot Platform proactively crawls all URLs visited by users of our partners' security platforms, allowing us to find phishing sites on an even larger scale. Our crawlers even capture screenshots of the phishing site in question to allow visual confirmation by human analysts of the machine learning platform's determinations.
3. If partners suspect a URL may pose a phishing risk, they can make a Webroot API call to get a real-time crawl and classification of the site in milliseconds, so they can determine if it is indeed a phishing site.

When a site is classified as phishing, the Webroot platform will perform a target assessment of its content to understand which brand or entity is being targeted. Webroot tracks many hundreds of targeted entities, and can add more as required by our partners.

Anti-fraud partners can also query the Webroot Platform to get an up-to-the-minute report on all phishing activity detected that is targeting their clients' brands, allowing them to provide a unique and proactive notification or takedown service for their customers.

Conclusion

Webroot is fighting fraud across many fronts, using the latest technical platforms and solutions to help our partners stay at the leading edge of the battle. We are proud to partner with many leading names in the cybersecurity industry who have integrated our threat intelligence into their products and are excited to work with innovative partners in the evolving anti-fraud market. Learn more at webroot.com/financialservices.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900