WEBROOT
Smarter Cybersecurity™

Webroot® Threat Intelligence

Fight Cyber Threats with the Power of Webroot® Threat Intelligence

Cyberattacks are now so frequent that cyber defenses without access to broad, instant, and actionable security intelligence simply aren't good enough. Without intelligent defenses in place, organizations will get infected more and more regularly, and may not become aware of breaches until it's too late. In this threat landscape, effective malware prevention requires continuous monitoring of every individual endpoint, an immediate response to anything new or unexpected occurring on any device, and visibility into the broader threat landscape to mitigate the opportunity for threats to penetrate defenses. Infection dwell times of days, weeks, or months are unacceptable, as are forensics and audits that can detail the kill chain but are unable to break it.

The goal of all cybersecurity is to mitigate attacks. However, understanding one set of attack vectors will no longer let you stop the next attack; threats and attacks are too variable, polymorphic, and unpredictable. Proactive mitigation, real-time visibility, and an immediate response are the only real defenses.

Webroot® Smarter Cybersecurity™ solutions and BrightCloud® Threat Intelligence Services are all powered by the Webroot Threat Intelligence Platform, which was purpose-built to deliver robust, machine-learning driven threat prevention.

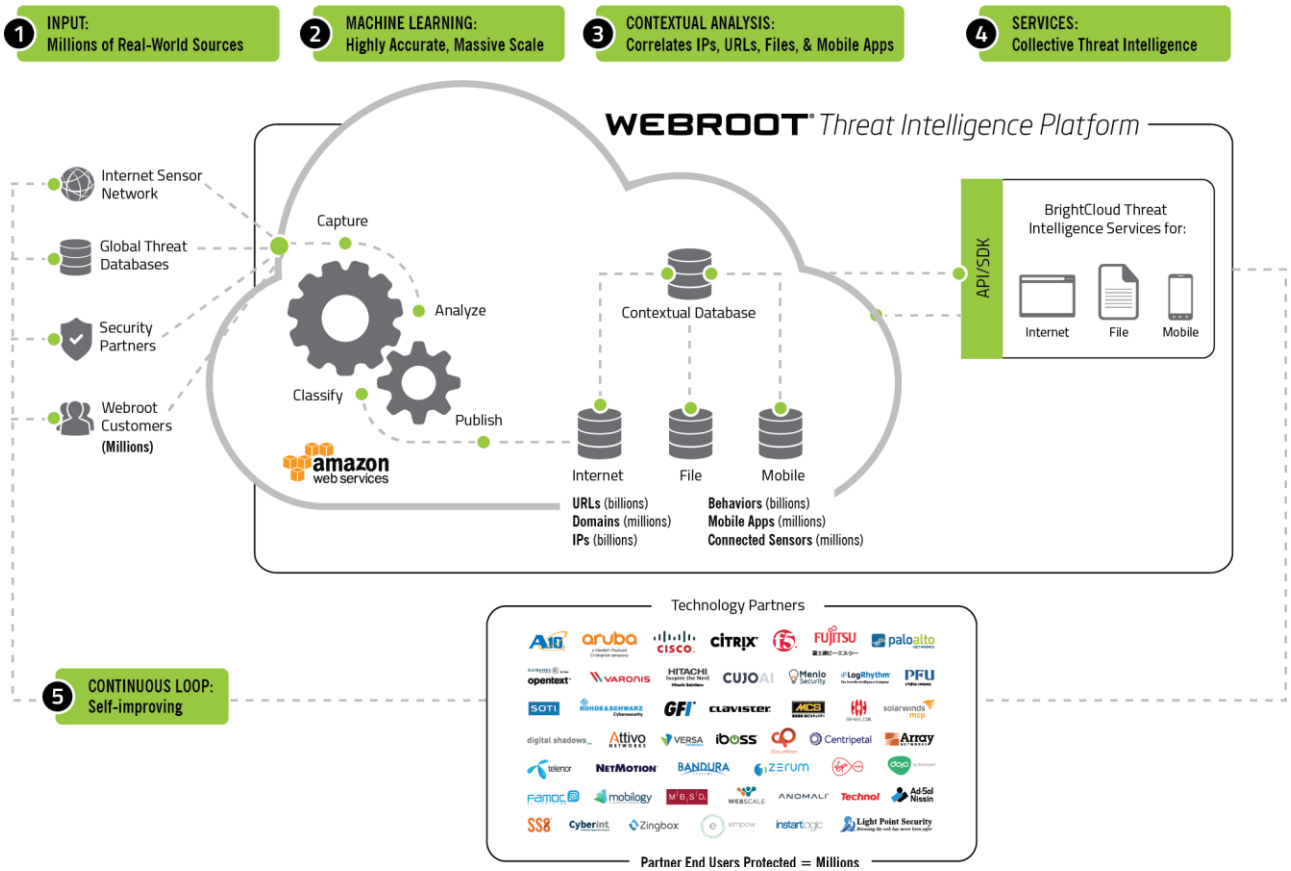
Collective and Predictive

The Webroot Threat Intelligence Platform encounters tens of millions of instances of malware and potentially unwanted applications and monitors billions of IP addresses and URLs. It analyzes millions of new and updated mobile apps for malicious behavior and studies major malware trends based on data from millions of endpoints. All of this and more continuously enriches the Webroot Threat Intelligence Platform and allows Webroot to accurately and effectively protect organizations from sophisticated attacks.

Continuous Analysis and Correlation

1. **Monitor**
   Accurately monitor the entire IPv4 space and in-use IPv6 addresses and continuously update a dynamic list of approximately 8-12 million malicious IP addresses
2. **Classify**
   Classify and score over 95% of the internet on a continuous basis and detect phishing sites in real time
3. **Categorize**
   Categorize millions of files that are seen across millions of Webroot customer endpoints
4. **Assess**
   Assess the risk of tens of millions of mobile apps

The Webroot Threat Intelligence Platform integrates billions of pieces of information from millions of sensors to create the world's largest threat detection net, providing proactive protection against both known and never-before-seen attacks.



Webroot® Threat Intelligence Platform

IT departments, users, and others need access to up-to-date intelligence on threats to their systems and endpoints of all types. Threats are constantly changing, so security controls must adapt accordingly. These security controls include being aware of the latest malicious IPs, the types of websites that are most often impersonated in phishing attacks, and the categories of apps that are most likely to be malicious.

Real-time, contextual, and predictive threat intelligence that spans the spectrum of attack vectors is the critical component in implementing a defense-in-depth strategy. It's the only way to fight back against today's cybercriminals and give companies an edge. It's what makes the Webroot Threat Intelligence Platform not simply a cloud-based data repository, but the most powerful, real-time threat analysis engine of its kind.

Massive data processing capacity, coupled with our proprietary implementation of the most advanced machine learning technology available, and a powerful contextual analysis engine, has enabled Webroot to accurately classify and score unsurpassed numbers of URLs, IPs, files, and mobile apps to help keep our customers and technology partners ahead of the exponential proliferation of threats they face.

Machine Learning

A key differentiator is our unique approach to machine learning. In web threat analysis, most security vendors use Bayesian networks or support vector machine (SVM) models to populate their work queues for human analysis. This approach isn't scalable, or even particularly accurate. Webroot, on the other hand, uses maximum entropy discrimination (MED) and other techniques, such as Active Learning, Active Feedback, and Deep Learning, to generate highly accurate and scalable web threat analysis. Here is a brief outline of the differences between the three machine learning technologies used, as well as the levels of accuracy associated with each. track device location, and drain the battery

1. Bayesian networks analyze site features to make predictive determinations and provide a simplistic, two-dimensional model to split known good from bad sites across a flat feature space.
2. SVM analyzes data, feature, and content patterns to make predictions on sites at a higher degree of accuracy than Bayesian networks, but still requires human analysis to achieve an acceptable confidence level.
3. MED is an extension of SVM that is better at classifying noisy and confusing data, but also requires a lot of computing power. While MED can use all given features for more accurate classification, the challenge is to create an efficient system that optimizes performance and minimizes computing power consumption.

Webroot supplements MED with Active Learning, Active Feedback, and Deep Learning. Active learning refers to the process in which human experts provide feedback to the machine learning algorithm when it has difficulty classifying certain objects during training. Active feedback is the process of incorporating human feedback into the machine learning algorithm while it is actively classifying in the real world, not just in training. Deep learning uses a layered approach to improve the efficacy of classification. Machine learning is involved at every step of the classification cycle, from an object's origins to its numerous relationships and beyond.

As an example, through enhanced MED, the Webroot Threat Intelligence Platform currently classifies well over 5,000+ URLs per second at an error rate of less than 2% (versus an average human error rate of 5-15%). Webroot

27+
Billion URLs

15+
Billion File Behavior Records

600+
Million Domains

62+
Million Mobile Apps

4+
Billion IP Addresses

57+
Million Connected Sensors

utilizes global teams of multilingual web analysts to analyze the relatively small number of websites where machine learning technology doesn't achieve a sufficient degree of determination confidence. Human analysts evaluate these cases and then feed each of them back into the machine learning model, continuously improving our accuracy.

Data Correlation

Webroot Threat Intelligence also leverages a powerful contextual analysis engine that takes previously disparate data and correlates it to create a deeper insight of the interconnected landscape of URLs, IPs, files, and mobile apps. Mapping the relationships between these different data points enables Webroot to provide highly accurate and dynamic intelligence that is always up to date, with virtually no false positives. For example, a seemingly benign IP may not show up as a risk on other IP reputation lists. Because that IP has been tied to other known malicious URLs, IPs, files, or mobile apps by the contextual analysis engine, its reputation score is reduced via this correlated intelligence, keeping customers safe from what could be a never-before-seen attack.

Real-time Visibility

The Webroot Threat Intelligence Platform doesn't rely on stagnant signature files. Our smarter approach to cybersecurity:

- Identifies the point and time of infection and alerts admins accordingly
- Minimizes the dwell time and vulnerability window between the launch and detection of an attack
- Protects endpoints around the globe against never-before-seen threats in real time
- Enables technology partners to offer enhanced protection to their end users by integrating Webroot BrightCloud Threat Intelligence Services

GETTING STARTED

To learn more or try the Webroot Unity API for yourself, please contact us directly on 02087337103, or use the button below to drop us a line.

CONTACT US

Smarter Endpoint Protection

Webroot SecureAnywhere® Business Endpoint Protection provides a multi-vector advantage over other solutions, covering threats from email, web browsing, file attachments, hyperlinks, display ads, social media apps, and connected devices like USB drives. It also identifies sophisticated, never-before-seen threats that use blended strategies to deliver malicious payloads.

Our unique approach to endpoint protection is powered by the Webroot Threat Intelligence Platform, providing global visibility of all attacks underway, leading to enhanced and timely protection for users and their devices through all stages of an attack including delivery, infiltration, and infection. This allows Webroot to closely monitor the activities of unknown processes until it can definitively categorize file behaviors as good or bad, with a high level of accuracy. If a previously unknown file's activities are later identified as malicious, Webroot SecureAnywhere Business Endpoint Protection can quickly and easily roll back the changes made by the malicious process.

Smarter Web Filtering

Webroot SecureAnywhere® DNS Protection provides a simple yet highly effective way to prevent everyday web usage from becoming a major security.

By leveraging the industry-leading Webroot Threat Intelligence Platform to automatically block malicious websites and filter undesirable website types, MSPs can reduce the number of malware threats entering their customers' networks.

- **Cleaner Network:** Reduce malware entering your network by up to 90%.
- **Improved Network Speed:** Lessen network traffic by managing internet use at the domain layer.
- **Higher Overall Malware Efficacy:** Increase overall security and reduce infection rates by enforcing policies at the domain layer.
- **Lower TCO, Higher Margins:** Reduce the costs associated with operation and delivery, man time spent remediating infections, and productivity hours lost due to malware.
- **Improved Productivity:** Fewer online distractions and lower infection rates lead to increased productivity for clients.