Webroot® Threat Intelligence Platform

Improve Cyber Resilience with Webroot® Threat Intelligence

Cyberattacks are now so frequent that 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 regularly, and may not become aware of breaches until it's too late. In this threat landscape, being cyber resilient 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's cyber resilience solutions and BrightCloud® Threat Intelligence Services are all powered by Webroot's threat intelligence platform, in order to deliver robust, machine-learning driven threat prevention.

Collective and Predictive

The Webroot Threat Intelligence Platform analyzes more than 500 billion data objects daily, including domains, URLs, IP addresses, file behaviors, and mobile applications. Our intelligence, powered by 6th generation machine learning, is fed by active and passive sensors including more than 95 million consumer and business endpoints. All of this continuously enriches the Webroot Threat Intelligence Platform and allows Webroot to accurately and effectively protect organizations from sophisticated attacks.

The Webroot® 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.

Continuous Analysis and Correlation

1 Monitor
Accurately monitor the entire IPv4 space and in-use IPv6 addresses and continuously update a dynamic list of 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
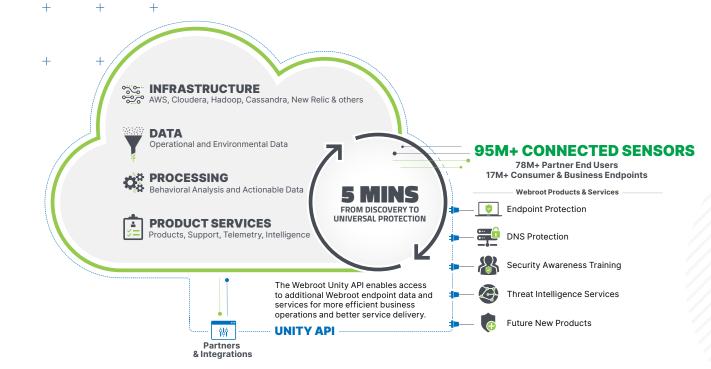Assess the risk of tens of millions of mobile apps

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.

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

Webroot Products & Services

Endpoint Protection

DNS Protection

Security Awareness Training

Threat Intelligence Services

Future New Products

The Webroot Unity API enables access to additional Webroot endpoint data and services for more efficient business operations and better service delivery.

UNITY API

Partners & Integrations

The Webroot® Platform

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 new and historical 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 6th generation Deep Learning allowing us, to generate highly accurate and scalable web threat analysis. Here is a brief outline of the differences between the four machine learning technologies used, as well as the levels of accuracy associated with each.

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. Maximum Entropy Discrimination (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.

4. Deep Learning uses complex neural networks that allow the machine to more accurately and autonomously identify relevant patterns and concepts within continually growing amounts of telemetry from Webroot customers and technology partners.

Webroot 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. 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.

37+
Billion URLs

842+
Million Domains

4.3+
Billion IP Addresses

36+
Billion File Behaviors

31+
Million Mobile Apps

95+
Million Real-World Sensors

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

Better Endpoint Protection

Webroot® Business Endpoint Protection provides advanced multi-vector protection 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's endpoint protection will quickly and easily roll-back the changes made by the malicious processes.

Secure & Private Internet Access Control

Webroot® DNS Protection provides a simple yet highly effective way to minimize everyday internet connectivity being a data privacy or security risk.

By leveraging the industry-leading Webroot threat intelligence data from the Webroot Platform you automatically block suspicious and malicious websites and filter out nearly all undesirable Internet network requests, administrators also gain the visibility to mitigate threats better.

- **Cleaner Network**: Reduce malware entering your network by up to 88%. »» 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.

Information

For more information, including white papers, case studies, and customer testimonials visit www.webroot.com, contact your Webroot account manager, or reach out to a Webroot Channel Partner.

Contact us to learn more – Webroot US

Email: wr-enterprise@opentext.com

Phone: +1 800 772 9383