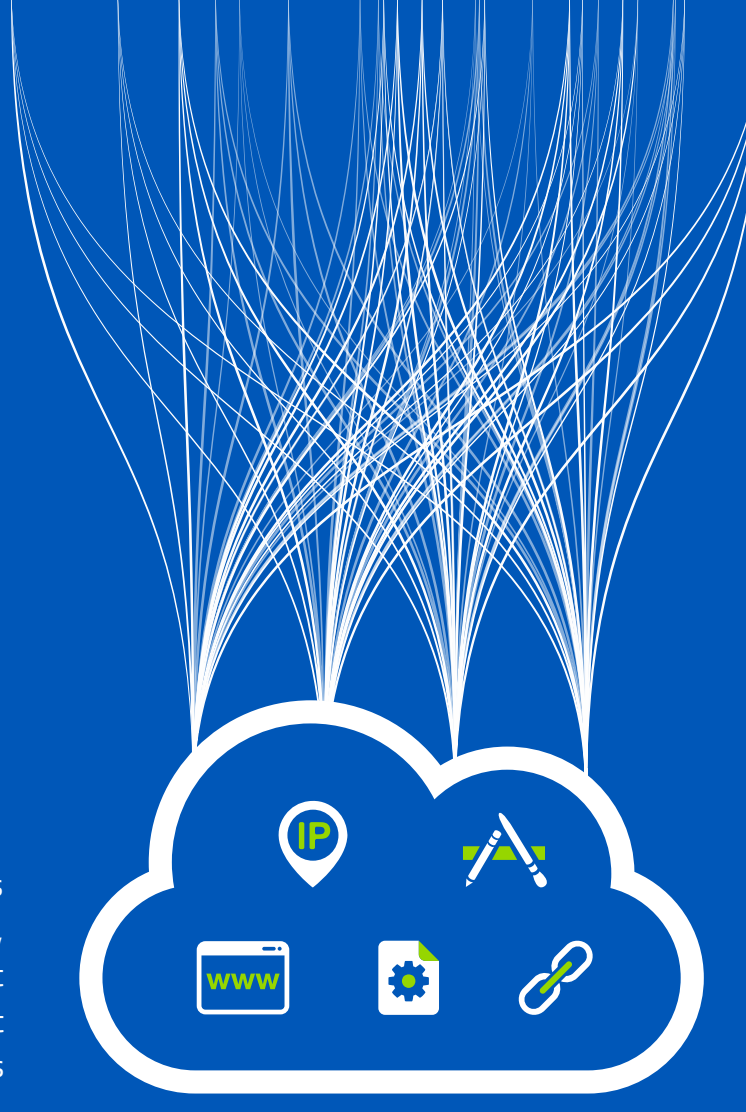
HOST IN THE MACHINE



Machine learning is a complex process, and the Webroot approach is no exception. To accurately classify URLs, IPs, files, and applications as benign, malicious, or requiring more research—in real time—it takes a lot of intelligence and processing power.

The Webroot® Platform, which powers all Webroot solutions and services, maps the relationships between URLs, IPs, files, and apps to provide unique insight into the internet landscape. Along with additional context, such as threat history, hosted files, common IPs, etc., the platform provides a predictive reputation score for each URL and IP address, enabling proactive protection for inbound/outbound traffic.

WHAT FOLLOWS IS A BREAKDOWN OF HOW THE WEBROOT® PLATFORM USES MACHINE LEARNING TO ANALYZE A NEWLY ENCOUNTERED URL.

Time from initial detection to global protection: about 5 minutes

GLOBAL INPUTS

- Millions of real-world consumer and business devices
- 50M users protected through technology partners
- Global sensor network: active/passive sensors, crawlers, scanners, honeypots, etc.
- Vetted, accurate 3rd party feeds for further context

NEW URL
www.benigndomain.com/pages/hiddenmalwarehost

Known classification database
32B URLs 750M Domains 42 Languages

URLs are re-crawled at regular intervals.

Known? YES: URLs scored 1-100 and grouped into 5 bands, trustworthy > malicious. **Malicious URL blocked.**

Known? NO: **Crawling processes**
- Hundreds of classifiers operating in parallel
- Each processes up to 20K classifications/sec
- URLs are classified into 82 categories

Data scientists with decades of experience keep models finely tuned to stay ahead of threats.

1,000 models trained and published per day

Up to 10M input characteristics for each object to determine 40-50M model parameters

Machine learning models use 10+ years of historical and current threat data to make a determination. They also assign a confidence score which can trigger further evaluation by human analysts to feed back into the machine learning models.

Meets confidence threshold? YES

Meets confidence threshold? NO: **WEB ANALYSTS** Human-based analysis used to further train the models

Determination

Cloud-based machine learning models

Webroot is one of the world's largest users of AWS, and we also leverage the San Diego Supercomputer.

These massive processors power our highly advanced machine learning systems, which use 6th gen techniques like deep learning and neural nets.

Malicious? NO

Malicious? YES

Feedback loops train models for continuous improvement

Billions of relationships between URLs, IP addresses, files, and mobile apps are mapped, and are used as part of an algorithm to determine predictive risk scores.

Contextual Analysis Billions of connections
- Predictive risk scores
- Threat Insight shows why a URL or IP is marked malicious
- 6 petabytes of historical data

Deep Crawling
- Proactive detection of previously unknown malicious URLs

If we detect a malicious URL, a patented deep crawling process is used to uncover additional threats. 91% of the malicious URLs found with this method have never been seen by our users before, so users are protected if they're ever encountered.

Real-time database updates

- WEBROOT PRODUCTS FOR CONSUMERS AND BUSINESSES
- THREAT INTELLIGENCE PARTNERS

Leading network and security companies, such as Cisco, F5 Networks, Citrix, and others, trust our threat intelligence to keep their customers safe from the latest threats.

www.benigndomain.com/pages/hiddenmalwarehost
- Category: Malware (out of 82 categories, including 6 emphasized types of malicious URLs)
- Reputation score: 17 (based on 1-100 scale for granular decision-making based on risk tolerance)
- Threat Insights (to help understand why an object was deemed malicious, including its threat history, hosted files, common IPs, and more!)

REMEMBER:

In the time it has taken you to read this infographic, **Webroot has uncovered hundreds of new malicious URLs**.

Learn more about the Webroot approach to machine learning at webroot.com

WEBROOT® Smarter Cybersecurity™