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
- 150+ sources of intelligence
- Global sensor network: crawlers, scanners, honeypots, etc.
- Cloud-based machine learning models

NEW URL

- www.benigndomain.com/pages/hiddenmalwarehost

- Known? YES
- Meets confidence threshold? YES
- Malicious? NO

Contextual Analysis

- Positive risk score
- Threat is known by a URL
- Threat is known by a file
- In partnership of historical data

Real-time database updates

Cloud-based machine learning models

- 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.

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.

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

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.

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