THE SCALE OF WEBROOT MACHINE LEARNING

BrightCloud Threat Intelligence can catch the most elusive, never-before-seen threats.

How? It's simple: The scale, speed and volume of Webroot's machine learning is unmatched, enabling our technology partners to integrate real-time, highly accurate, predictive intelligence to stay ahead of internet threats.

You want to talk about scale? **Let's talk about scale.**

10 MILLION

Webroot has the potential to capture up to 10 million input characteristics for each internet object that we classify

40 MILLION

We then train the machine by assigning up to 40 million weights to our models

MILLIONS

Webroot classifies millions of internet objects every day to determine if they are benign or malicious

1,000

Webroot trains and publishes 1,000 models a day

The Webroot cloud-based platform has the potential to capture millions of characteristics for each object being classified. These characteristics create a "feature space" for internet objects. The location of an object in this"feature space" defines the object.

This massive feature space is what enables BrightCloud to effectively categorize brand new, zero-day internet objects.

Neural Nets

Neural Nets Webroot applies extremely large and complex neural nets on the order of **40 million nodes**, for its machine learning models

They are used to digest and analyze the massive number of characteristics we capture for each object.

Processing Power

At present, the training of a Webroot model utilizes approximately **10 million data points to determine 40 to 50 million model parameters**

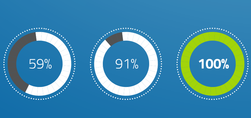
To accomplish this, we leverage Amazon Web Services and the San Diego Supercomputer Center at the University of California, San Diego in La Jolla, CA, typically leveraging up to one terabyte of RAM and 40-50 nodes.

Real World Results

Webroot witnessed **293 million** new unique files in 2016 alone

In 2016, Webroot classified an average of **736,000** new files as malicious per month.

94% of malicious files first seen in 2016 were only seen on one PC in Webroot's user base, demonstrating the continuing growth of polymorphic malware.



Webroot was able to classify **59%** of new malicious files within the first hour

This increases to **91%** after 12 hours

MRG research indicates that Webroot correctly identified **100%** of malicious files within 24 hours

Read more about how Webroot is identifying zero-day threats using machine learning in our complimentary white paper, "**Automating Threat Detection with Advanced Machine Learning at Scale: The Webroot Approach**"

WEBROOT
Smarter Cybersecurity