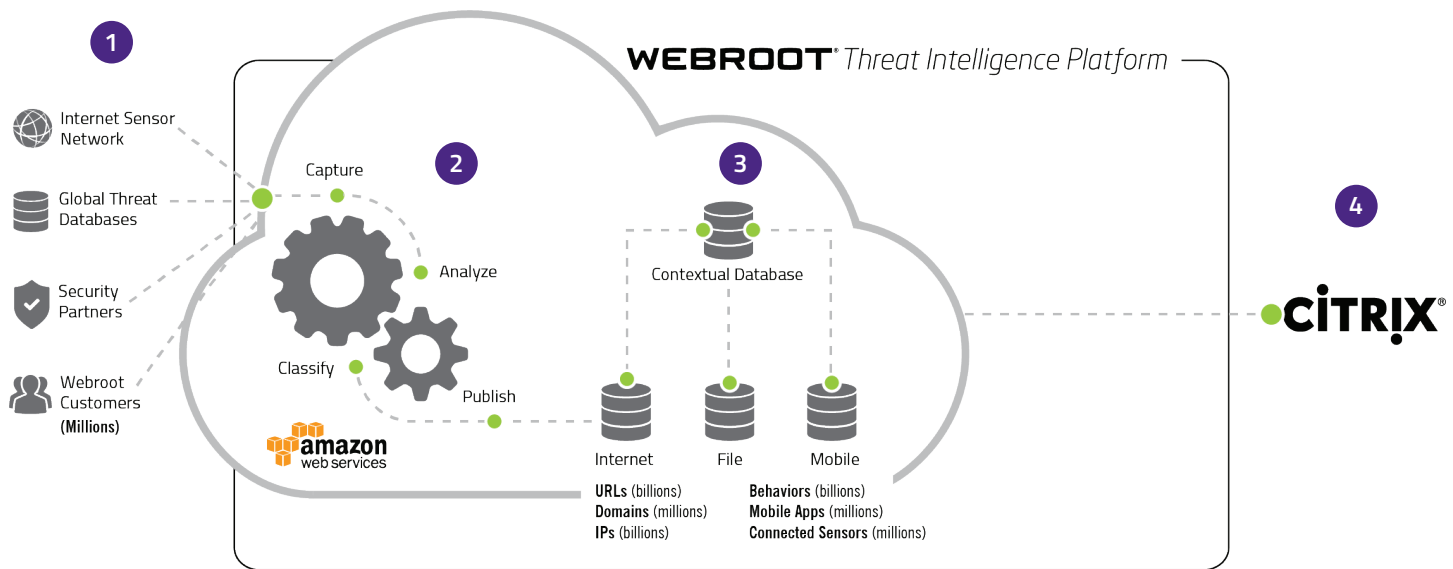


IP Reputation Service for Citrix® ADC and Citrix Web Application Firewall

» Citrix® NetScaler leverages the most up-to-date dynamic IP reputation intelligence available today to block unwanted and malicious traffic coming into your network.

» This highly accurate IP intelligence is made possible by an advanced security intelligence engine that automatically analyzes and correlates feeds from millions of global sensors in real time.

» You can't rely on static, rapidly out-of-date blacklists to guard against zero-hour threats. Get real-time protection through an automatically updated feed of over 8 million dangerous IP addresses.



How It Works

- 1 Real-time threat data is input from millions of sensors and other sources connected to the Webroot Threat Intelligence Platform.
- 2 IPs, URLs, files, and mobile apps are automatically and continually captured, scanned, analyzed, classified, and scored using advanced machine learning and behavioral analysis.
- 3 A contextual analysis engine correlates disparate data for increased granularity and accuracy.
- 4 IP intelligence is updated in near real time (every five minutes) and leveraged by Citrix ADC and Citrix Web Application Firewall.

Key Differentiators

- » **Highly Accurate:** Automated analysis leverages advanced machine learning to provide speed and accuracy to keep up with the dynamic nature of IPs.
- » **Breadth of Coverage:** Correlated data between different internet object types (e.g., linking an otherwise trustworthy IP with a known malicious IP, URL, file, or application) provides better threat intelligence and coverage.
- » **Real-time Data:** Continuously updated feeds (every 5 minutes) of malicious IP addresses can be used to effectively detect recently identified IP threats, stopping malicious traffic at the network edge.

Enterprise Benefits



Safe network
Security against data breaches



No performance impact
Fast and easy deployments



Lower TCO
Consolidate data feeds

IP Reputation Helps Protect Against



Windows Exploits

Active IPs offering/distributing malware, shell code, rootkits, worms, or viruses



Web Attacks

Cross site scripting, iFrame/SQL/cross domain injection, domain password brute force



Phishing

IPs hosting phishing sites, and other fraud such as ad click fraud or gaming fraud



Botnets

Botnet C&C channels and infected zombie machines



Denial of Service

DoS, DDoS, anomalous syn flood, and anomalous traffic detection



Scanners

All reconnaissance, such as probes, host scan, and domain scan



Proxies

IPs providing proxy and anonymization services



Reputation

Infected IPs and those with a reputation score below threshold



Spam Sources

IPs that have been observed to be sources of spam email



Mobile Threats

Denial of service, packet sniffing, address impersonation, and session hijacking

For more information
Contact your Citrix representative.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Citrix. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

World Headquarters

385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA

6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC

Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900