TitanHQ WebTitan CLOUD

Malicious Threat Detection powered by WebTitan

Real Time Threat Detection & Monitoring

WebTitan employs a crowd-sourced approach for obtaining a constant stream of URLs for analysis. This continuous stream of ActiveWeb (URLs actively visited by end users) comes from a global network of customers across a number of high traffic markets: Network Security, Subscriber Analytics, and Ad Tech.

This includes over 550 million end users and growing—and is the primary in-house source for threat corpora used to train human-supervised Machine Learning systems. This combined and integrative approach empowers us to continuously enhance, optimize, and fine-tune our malicious detection capabilities in an ever-changing threat landscape.

- Supporting 550–600 Million End Users.
- Covering numerous industries including:
  - Network Security
  - Subscriber Analytics
  - IoT & Connected Devices
  - Ad Tech
- ActiveWeb Input and queries on:
  - Web Content
  - Web Traffic from browsers
  - Web-connected Device activity

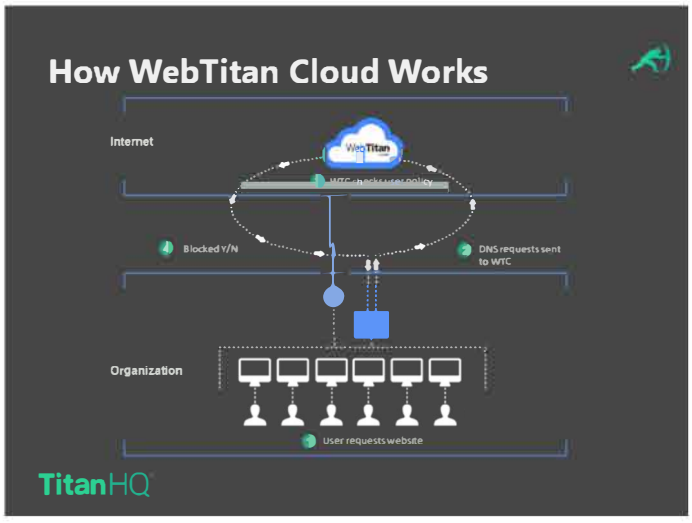
Multi-Vector Threat Detection

WebTitan leverages an integrative, multi-vector approach and in-house analysis to detect, monitor, and accurately categorize new threats. Our approach combines the following methods:

- URLs/Website Detection
  - Link Analysis
  - Content Analysis
  - Static, Heuristic, and Behavioral Anomaly Analysis
  - In-house and 3rd Party Tools
- ActiveWeb Input and queries on:
  - Web Content
  - Web Traffic from browsers
  - Web-connected Device activity

How WebTitan Cloud Works:

- Sign up for a free trial.
- We will create an account for you and send you your log on credentials.
- Log on and create your usage policy or use the default policy to start with.
- Redirect your DNS to our IP's. If you need help, our knowledgeable, responsive and friendly technical support team will guide you step by step.
- Done! You're now completely set up on WebTitan Cloud.



General queries: info@titanhq.com www.titanhq.com

Malicious Threat Detection powered by WebTitan

TitanHQ WebTitan CLOUD

Malicious Detection

Human-Supervised Machine Learning	The WebTitan team continuously samples malicious detections to profile, test, and validate threats. The results of the continuous sampling are then used to feed/train the supervised Machine Learning systems and adjust or tune the efficiency, accuracy, and overall effectiveness of the malicious detection systems.
URL, Domain, and Path Coverage	One of the critical features that WebTitan provides is an ability for deep analysis due to full path detection. In a nutshell, page and path-level reporting provides analytical credibility to what is being marked as malicious. The majority of malicious URLs in the WebTitan databases are detailed down to the path level. In the case of non-IP based URLs, 88.35% are marked as malicious down to the path level. In the case of IP-based URLs, the numberis significantly higher with 99.70% of URLs being identified as having a path. This is extremely important because DNS-based systems typically work at the domain level only.
Malicious URL Revisit Process	Due to the variable life cycle of malicious URLs, it is imperative be able to inspect and detect URLs quickly to ensure they are still malicious. The WebTitan Malicious Detection Service includes an automated revisit process where malicious URLs are revisited on a set schedule. Each day, WebTitan revisits up to 300,000 malicious URLs to determine if they are still infected or are now clean. Since WebTitan's malicious detection service is able to obtain the full path, it is able to revisit that exact URL and obtain crucial results on a granular and highly accurate level.

10 Malicious Categories

WebTitan's threat detection systems utilize the following ten (10) types of Malicious Categories:

1. Ad Fraud:

Sites that are being used to commit fraudulent online display advertising transactions using ad impression boosting techniques including (but not limited to) ad stacking, iframe stuffing, and hidden ads. Sites that have high non-human web traffic and with rapid, large and unexplained changes in traffic.

2. Botnet:

Bots are compromised machines running software that is used by hackers to send spam, phishing attacks, and denial of service attacks.

3. Malware Distribution Point:

Web pages that host viruses, exploits, and other malware are considered Malware Distribution Points.

4. Spyware & Questionable Software:

Software that reports information back to a central server such as spyware or keystroke loggers. Also includes software that may have legitimate purposes, but some users mayobject to having on their system.

5. Phishing/Fraud:

Web pages that impersonate other web pages usually with the intent of stealing passwords, credit card numbers, etc. Also includes web pages that are part of scams such as a "419" scam - where a person is convinced to hand over money with the expectation of a big payback that never comes.

6. Command + Control Centers:

Internet servers used to send commands to infected machines called bots.

7. Malware Call-Home:

When viruses and spyware report information back to a particular URL or check a URL for updates, this is considered a malware call-home address.

8. Compromised & Links To Malware:

Compromised web pages are pages that appear to be legitimate, but house malicious code or link to malicious websites hosting malware. These sites have been compromised by someone other than the site owner.

9. Spam URLs:

URLs that frequently occur in spam messages.

10. Cryptocurrency Mining:

Websites that use cryptocurrency mining technology without user permission.

General queries: info@titanhq.com www.titanhq.com