

Threat Intelligence Feeds

Block domains known to distribute malware, launch phishing attacks and host command-and-control servers using a blend of the most reputable threat intelligence feeds — all updated in real-time.

☒ Use Threat Intelligence Feeds

AI-Driven Threat Detection BETA

Block millions of threats detected by our AI technology — a proprietary AI engine designed from the ground up for DNS with hundreds of signals, terabytes of training data and real-time decision making.

☒ Enable AI-Driven Threat Detection

Google Safe Browsing

Block malware and phishing domains using Google Safe Browsing — a technology that examines billions of URLs per day looking for unsafe websites. Unlike the version embedded in some browsers, this does not associate your public IP address to threats and does not allow bypassing the block.

☒ Enable Google Safe Browsing

Cryptojacking Protection

Prevent the unauthorized use of your devices to mine cryptocurrency.

☒ Enable Cryptojacking Protection

DNS Rebinding Protection

Prevent attackers from taking control of your local devices through the Internet by automatically blocking DNS responses containing private IP addresses.

☒ Enable DNS Rebinding Protection

IDN Homograph Attacks Protection

Block domains that impersonate other domains by abusing the large character set made available with the arrival of Internationalized Domain Names (IDNs) — e.g. replacing the Latin letter "e" with the Cyrillic letter "е".

☒ Enable Homograph Attacks Protection

Typosquatting Protection

Block domains registered by malicious actors that target users who incorrectly type a website address into their browser — e.g. gooogole.com instead of google.com.

☒ Enable Typosquatting Protection

Domain Generation Algorithms (DGAs) Protection

Block domains generated by Domain Generation Algorithms (DGAs) seen in various families of malware that can be used as rendezvous points with their command and control servers.

☒ Enable DGA Protection

Block Newly Registered Domains (NRDs)

Block domains registered less than 30 days ago. Those domains are known to be favored by threat actors to launch malicious campaigns.

☐ Block Newly Registered Domains (NRDs)

Block Dynamic DNS Hostnames BETA

Block Dynamic DNS Hostnames

Dynamic DNS (or DDNS) services let malicious actors quickly set up hostnames for free and without any validation or identity verification. While legit DDNS hostnames are rarely accessed in every-day use, their malicious counterparts are heavily used in phishing campaigns — e.g. paypal-login.duckdns.org.

If you are using DDNS, note that this setting will not block the DDNS services' own website or their update API.

☒ Block Dynamic DNS Hostnames

Block Parked Domains

Parked domains are single-page websites often laden with ads and devoid of any value. Parked domain monetization can sometimes get mixed up with suspicious practices and malicious content.

☐ Block Parked Domains

Block Top-Level Domains (TLDs)


Block all domains and subdomains belonging to specific TLDs.

ADD A TLD

Block Child Sexual Abuse Material

Block domains hosting child sexual abuse material with the help of Project Arachnid, operated by the Canadian Centre for Child Protection. No information is transmitted back to Project Arachnid when a domain is blocked.

☒ Block Child Sexual Abuse Material

 Help us translate or improve NextDNS in your language. [Learn more](#)