Protective Domain Name Service (PDNS)

Protective DNS is a recursive DNS resolver which prevents access to domains known to be malicious.

About PDNS

PDNS was built to hamper the use of DNS for malware distribution and operation. It has been created by the National Cyber Security Centre (NCSC), and is implemented by Cloudflare and Accenture.

PDNS is a recursive resolver, which means it finds answers to DNS queries. Management of your own domains (authoritative DNS) is done separately to this NCSC service and will not be affected by the adoption of PDNS.

It is a free and reliable internet accessible DNS service and is one of the NCSC's widely deployed Active Cyber Defence capabilities. It has been mandated for use by central government departments by the Cabinet Office but is also available to other organisations that wish to use it (see FAQs for eligibility) .

PDNS prevents access to domains known to be malicious, by simply not resolving them. Preventing access to malware, ransomware, phishing attacks, viruses, malicious sites and spyware at source makes the network more secure.

In addition, PDNS provides organisations that use it with metrics about the health of their networks and gives them access to NCSC outreach support to resolve any issues. The data from PDNS is also used to inform and support UK government cyber incident response functions in the event of a cyber attack.

Unable to display video due to your cookie settings. Please change your cookie settings or watch the video on YouTube instead.

Benefits of PDNS

Benefits of PDNS include:

- Blocking malware and malicious sites - PDNS prevents access to sites hosting malware, ransomware and spyware. It also blocks malware communication, which serves to contain active threats
- Dashboard and data logs are available to help customers monitor the status of their networks and resolve any issues
- Subject matter expertise from the NCSC and Cloudflare, including world leading analysis and incident management capabilities
- It is free - the service is centrally funded by the NCSC

PDNS block data can be ingested into Security Information and Event Management (SIEM) tools as a source of threat intelligence to help identify and remediate threats. By consuming the data into a SIEM, organisations can consolidate various security logs into a single view, providing further context for blocks by PDNS.

/

Connectors are available for Microsoft Sentinel and Splunk to simplify and enhance ingesting data.

How PDNS works

- We curate a set of rules for how the DNS response should be modified if the user queries a malicious domain. This is codified in a database called a Response Policy Zone (RPZ) which our DNS resolver operates on
- The rules are created based on knowledge of malicious domains we obtain from commercial, internal and open sources
- We review our rules to ensure we do not accidentally block sites that are used for legitimate purposes
- When a domain is blocked, users will see a block page that states:

> You tried to visit: [http:address of site]. This site may be involved in malicious activity or associated with malware and so access has been blocked.

PDNS Roaming

If your users work remotely or from home without a VPN or enterprise DNS resolver, you might not know the IP addresses of their devices but still want to protect them with PDNS. With PDNS Roaming, end users can benefit from the protection of PDNS wherever they connect to the internet.

PDNS Roaming is available for Windows, macOS and iOS operating systems and directs DNS traffic to PDNS. It allows devices to connect to PDNS when they are outside the office network using the encrypted DNS over HTTPS (DoH) protocol.

For more information about PDNS Roaming, visit the PDNS Knowledge Base (ncsc.gov.uk) under **Roaming.**

/

How to register for protective PDNS

Sign in to your MyNCSC account and complete the following form: https://info.pdns.service.ncsc.gov.uk/sign-up-to-pdns/

Please refer to the eligibility criteria below before completing the form. Eligibility for Protective DNS is reviewed on an ongoing basis with any changes reflected on this page. For guidance on PDNS for the private sector, please see protective-dns-for-private-sector.

For queries on the registration process, please contact pdns.support@accenture.com.

Frequently asked questions (FAQs)

+ Show all

What is DNS? Show

Who is eligible for PDNS? Show

How do you prevent the incorrect blocking of legitimate domains? Show

Does PDNS filter content? Hide

No. PDNS does not provide content filtering. PDNS solely limits its blocking to sites known to contain malicious content like malware or viruses.

PUBLISHED

17 August 2017

REVIEWED

17 September 2024

/

WRITTEN FOR

Public sector

Cyber security professionals