PROTECTIVE DNS

PDNS
Protective DNS

Nominet proudly delivers Protective DNS (PDNS) on behalf of the UK National Cyber Security Centre (NCSC) to protect the UK public sector.

It has been mandated for use by central government services and is available to all public sector organisations in the UK.

The delivery of Protective DNS forms a vital part of the UK's Active Cyber Defence (ACD), designed to tackle cyber attacks to improve national resilience.

PROTECTS AN ESTIMATED 7.2 MILLION USERS

SUCCESSFULLY RESOLVED 0.55 TRILLION DNS QUERIES IN 1 YEAR

SECURES 1,100+ ORGANISATIONS DELIVERING GOVERNMENT SERVICES

ADDITIONAL PROTECTION OF NHS, HSCN & VACCINE SUPPLY CHAIN 12,000+ SITES | 1,000+ ORGANISATIONS

COUNTERS MANY ADVANCED PERSISTENT THREAT (APT) ATTACKS AT SCALE

CYBER DEFENCE ANYWHERE PDNS ROAMING

NHS: National Health Service
HSCN: Health and Social Care Network

Protective DNS in action

NHS protection in the face of COVID-19

Onboarding of the Health and Social Care Network to PDNS was accelerated (within 24 hours) following CISA alert that malicious actors were targeting US healthcare.

Many COVID-19 related malicious domains were blocked, including a webpage hosting malware and a fake web shop being used for phishing.

Ransomware defence

In 2022, PDNS blocked over 5 million requests for domains associated with ransomware, a significant contribution to protecting UK organisations from this threat.

SolarWinds

Disclosure of a sophisticated software supply chain attack of the SolarWinds Orion product saw the PDNS dataset become a primary data source for analysis of risk and response. It revealed:

- How many public bodies were affected
- The extent of compromise
- Where was affected, giving assurance to many core parts of the Government

National Cyber Security Centre | NOMINET CYBER