NOMINET CYBER | PROTECTIVE DNS

Cyber security is the frontier of national defence

Governments, public sector organisations and critical services are under threat from sophisticated attacks orchestrated by criminal groups and enemy nation states, for example, the attack on SolarWinds. In this complex attack environment, defence is needed that is built into the very infrastructure of a country, effective on a local and central basis.

On a local level, councils, schools and other public sector organisations need visibility and protection against cyber threats. Intelligence that is specific to them and access to wider industry expertise and incident management support.

At a central level, governments need international threat intelligence and trend analysis, reliable, scalable defence technology, and service delivery that will allow them to defend their nation and citizens against cyber attack.

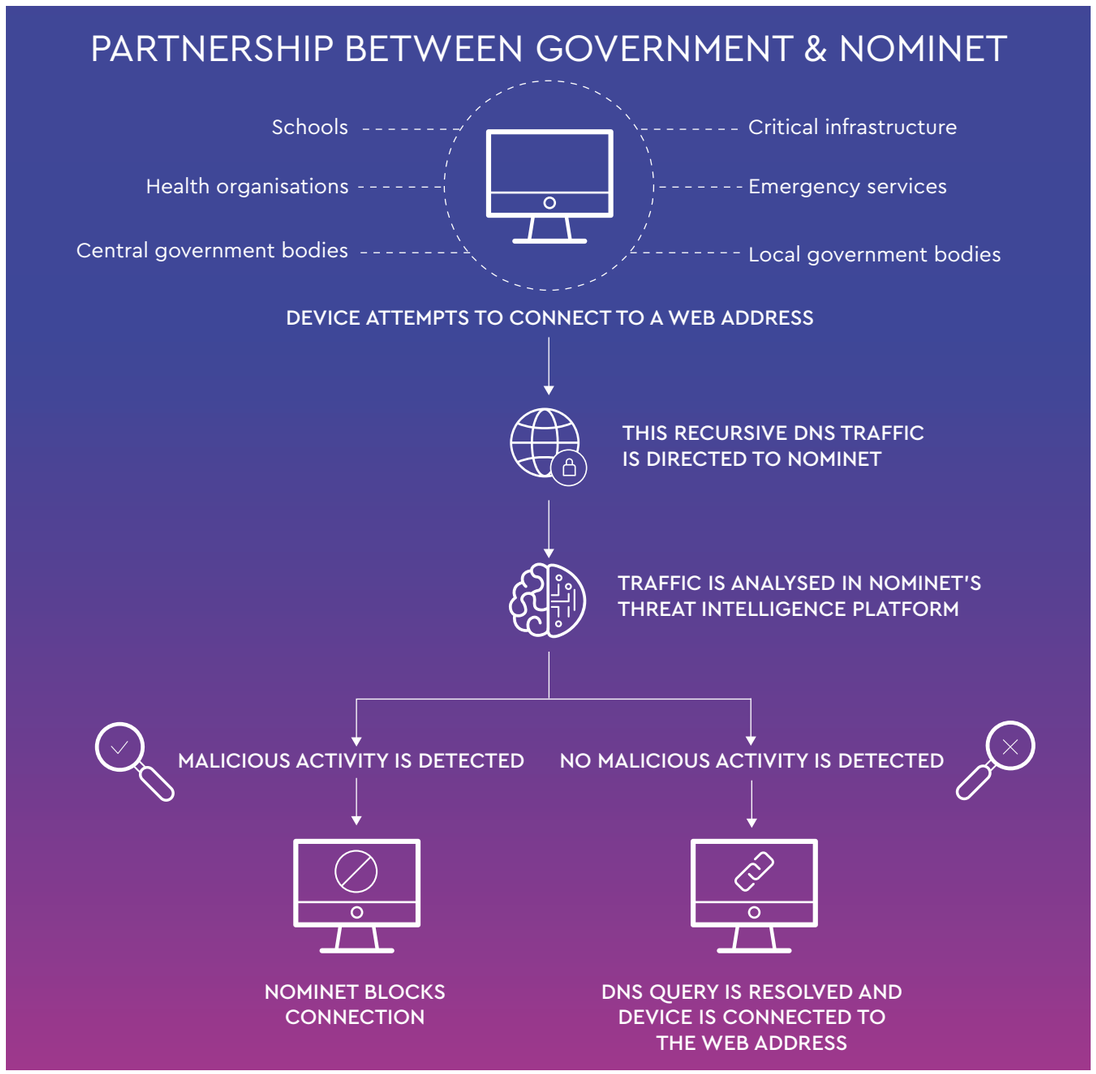
What is Protective DNS?

Every connection between an organisation's network and the world wide web is present in the DNS (Domain Name System) traffic. This includes visiting a web address in your browser as well as machine-initiated actions, such as a software update. In other instances, it could be a malicious connection.

Nominet's Protective DNS is designed to analyse and block DNS requests deemed malicious.

It is based around a recursive resolver. Built to answer DNS queries, including those over DoH and DoT, the recursive resolver does not resolve a query if the domain is known to be malicious. Protection is provided against malware, ransomware, phishing attacks, viruses, spyware at source, and malicious sites. It also stops malware already on end devices from 'calling home' mitigating the damage of an attack.

Despite the additional analysis, domains are resolved significantly faster than many free DNS resolver services.



Nominet Protective DNS

Nominet Protective DNS is specifically designed for governments and critical infrastructure. It offers world class threat intelligence, discovery of malicious activity and blocking of malicious connections. It enables governments to enact early incident response and offer informed guidance to the public sector and beyond of the most imminent threats.

Scalable – Nominet Protective DNS has proven resiliency at a national scale. Storing, aggregating, managing, and securing vast amounts of data. Most recently it has launched a Digital Roaming capability to offer protection away from the office network.

Accurate – Threat intelligence is curated for the government audience from multiple threat feeds, including commercially available, open source and proprietary. This feeds into a set of rules – a codified database or Response Policy Zone (RPZ) – for how DNS response should be modified in the instance that malicious activity is detected with minimal false positives.

Intelligent – A team of DNS specialists, data scientists and security experts sit behind the scenes to evolve the solution and as a support system for end users. From identifying specific threat actors to advising on severity and remediation.

Service-led – A full service-wrap is delivered with Nominet's Protective DNS by local dedicated teams. This will include bespoke support and reporting depending on whether the end customer has one IT administrator or an entire security operations team. Service stretches across onboarding, deployment, training and troubleshooting through the user hub, to marketing support spreading awareness of the service.

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 6 MILLION USERS

SUCCESSFULLY RESOLVED 237 BILLION PDNS QUERIES IN 1 YEAR

SECURES 900+ 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 DIGITAL 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

Emotet domains, originally used as a banking trojan, were seen to be evolving as a 'dropper' to deliver ransomware e.g. Ryuk and Conti and were blocked more than any other 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

Who is Nominet?

The .UK Registry

Part of UK's critical infrastructure with **25 years** DNS expertise managing **>11m** domains & handling **150bn** queries per month

Focus on cyber security

Years of R&D efforts resulted in launch of a Protective DNS solution in 2017

A public benefit organisation

Donating over **£49m** to tech-for-good initiatives that have helped and supported more than 1 million young people

Designed for government

Nominet Protective DNS is built for large scale, national protective interventions that move the needle