
NOMINET CYBER
PROTECTIVE DNS

Government and industry must join forces to elevate cyber defence at a national level, protecting a nations most critical assets

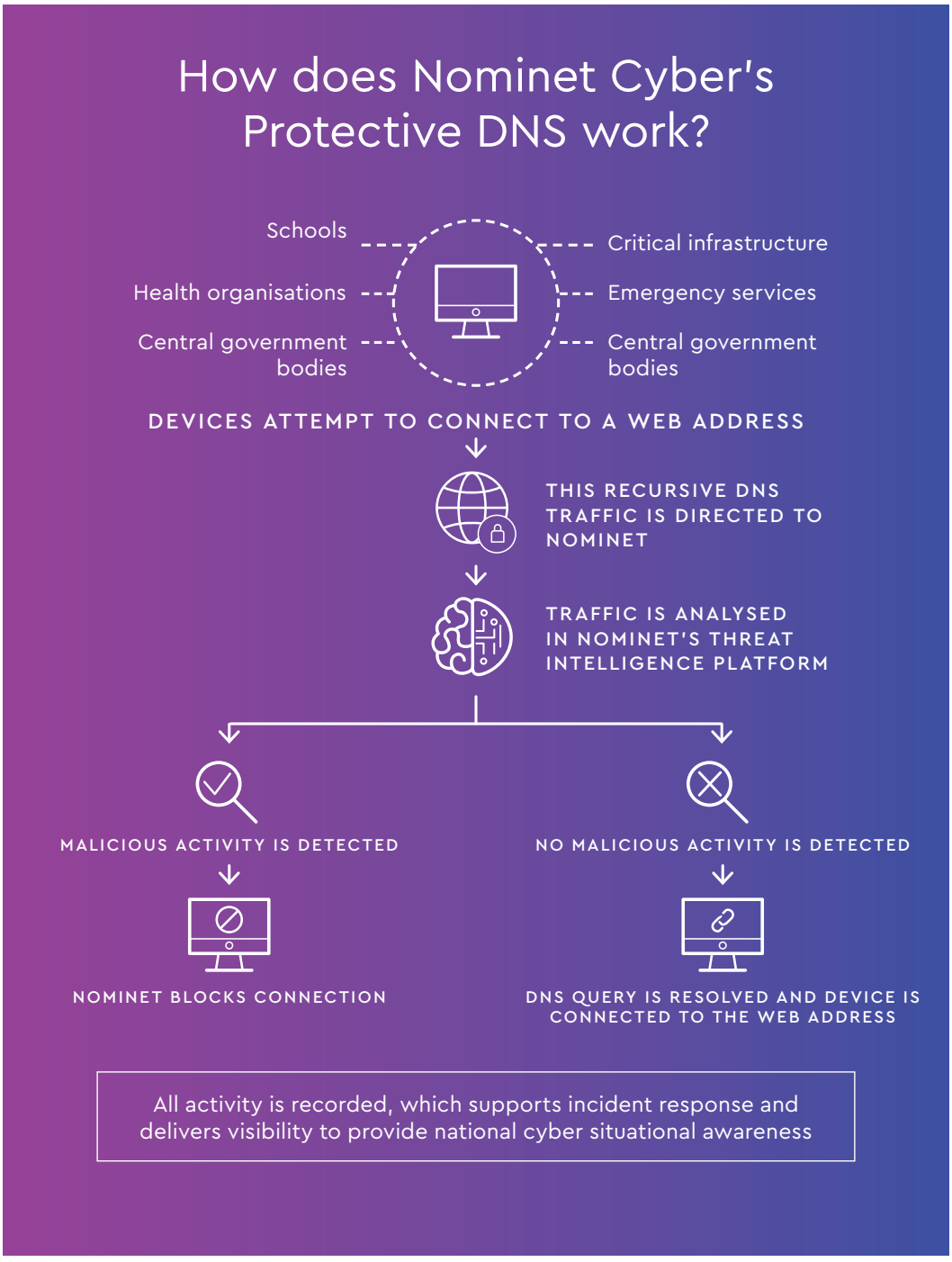
Cyber security is a global challenge requiring international cooperation to protect critical infrastructure. Government and industry must join forces in this complex environment to build defence into the infrastructure of a country, effective on a local and central basis.

Nominet Cyber work closely with international cyber security agencies to collaborate on this challenge and share intelligence within these communities. Our goal is to protect at scale against attacks from criminal and nation state actors and improve cyber security resilience at a national level, for the protection of essential public services.

What is Nominet Cyber's 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 Cyber's Protective DNS is designed to analyse all DNS requests and block those deemed to be malicious. It is based around a recursive resolver. Built to answer DNS queries, including those over DoH (DNS-over-HTTPS) and DoT (DNS-over-TLS), the recursive resolver does not resolve a query if the domain is known to be malicious. The solution is a secure service built and managed to rigorous performance and security requirements.



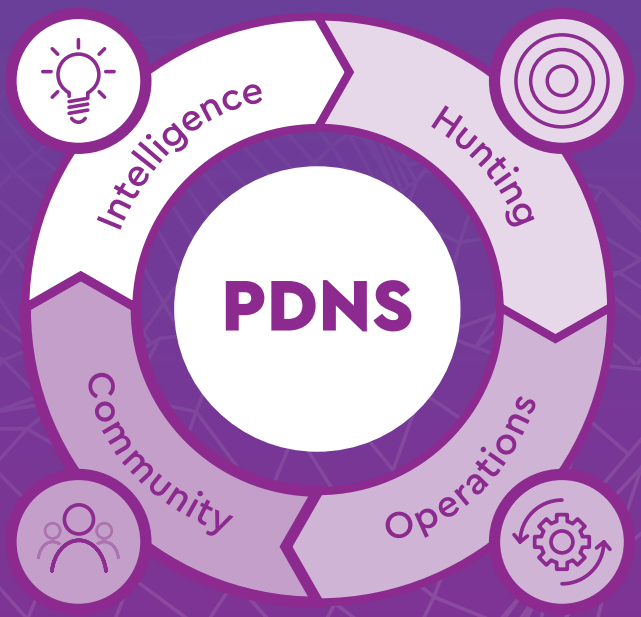
A joined up approach to protection at scale

Protect against cyber attacks at scale, including: malware, ransomware and phishing attacks

Detect new threats through a combination of automated and manual analysis

Respond to emergency situations by utilising PDNS data to support remediation

Capture actionable intelligence based on your own requirements. We work with you to understand the pipeline of activities we need to undertake to deliver a solution tailored to your needs.



Sharpen your understanding of the threat landscape and gain greater visibility of your networks. Our multi-faceted approach to threat hunting is driven by Intelligence data and our own sources.

Share best practices and information with other Protective DNS customers to drive future Intelligence data. Benefit from the insight of international peers to elevate your own cyber defence.

Deliver triage, analysis and communication to your end users based on Hunting information. Our service wrap frees up time for your own analysis and complements your incident response.

Nominet Cyber is the only Protective DNS provider that:

Delivers a 'top-down' solution to give national intelligence and law enforcement benefit to a central authority

Provides a sovereign capability tailored to a customers' needs, including a bespoke service wrap

Has unrivalled expertise in national level DNS as part of Nominet, the .UK registry for over 25 years

Works exclusively with governments worldwide to support their specific challenges

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

NOMINET

A PUBLIC BENEFIT COMPANY

A force for good in the UK digital economy, global internet and government cyber security communities, delivering services that make our world more connected, inclusive and secure

THE .UK REGISTRY

Part of the UK's critical national infrastructure, with 27 years of DNS expertise managing 11m domains that millions of businesses and individuals rely on daily

PROTECTING PUBLIC SERVICES

Helping to secure public services to protect digital economies and minimise cyber disruption through the delivery of Protective DNS solutions to governments globally