whalebone

Experts Say

# DNS Security Should Not Be Ignored.

Critical insights from industry leaders demystify the role of DNS in cybersecurity.

# DNS Security: A Must–Have Solution

Both renowned experts and institutions are outspoken about DNS security being a must–have, and the industry perspective is finally changing.

This brochure compiles selected expert insights from reports and key articles that reinforce the criticality of DNS security being an essential part of even a basic–level cybersecurity posture.

# Selected Quotes

(By Year)

2025

## National Security Agency (NSA) [1]

“NSA and the partnering agencies [CISA, FBI, ASD, CCCS, NCSC-NZ] recommend[...] a multi-layered approach to detection, and organizations leverage Protective DNS (PDNS) services that offer protection from fast flux enabled threats. Organizations[...] should use cybersecurity and PDNS services that aid in blocking malicious activity.”

2024

## GigaOm Analyst Paul Stringfellow [2]

“Almost all cyberattacks will start by interacting with DNS[...]”

“DNS security tools add value by identifying risks and potential threats at these very early stages, which we can proactively isolate and mitigate[...]”

“DNS security solutions are easy to deploy, with a low-risk integration[...] and little if any impact on users.”

“If you want a low-risk, high-value cybersecurity investment that will improve your security posture, then I would recommend you look into the DNS security space and understand how it can improve security, reliability, and performance.”

[1] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4143636/nsa-and-partners-issue-guidance-on-fast-flux-as-a-national-security-threat
[2] https://gigaom.com/2024/03/18/dns-security-the-forgotten-hero-of-your-cybersecurity-strategy

2022

## Australian Signals Directorate (ASD) [3]

“In a gateway context, a DNS can be an effective and scalable mitigation capability against a variety of cyber risks, such as by using DNS filtering to stop undesirable content, or using a Protective DNS (PDNS) service to block malicious domains.”

2022

## NIS2 Directive (EU) 2022 [4]

“Upholding and preserving a reliable, resilient and secure DNS are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation[...]”

“Member States should encourage the development and use of a public and secure European DNS resolver service.”

2022

## US Executive Office of the President [5]

“Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported.”

“Agencies should adjust their DNS architecture and associated monitoring to move closer to a zero trust architecture.”

[3] https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&qid=1719994587907

[5] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

2021

## UK National Cyber Security Centre [6]

“Protective DNS (PDNS) systems prevent malicious domains from being visited by devices in your network[...] Preventing access to these domains should protect your organisation against malicious actors, making it harder for them to compromise your networks, and harder to exploit any compromises.”

2021

## Gartner Analysts Craig Lawson and John Watts [7]

“Organizations should implement DNS security to protect users, devices, and other critical infrastructure.”

2021

## Cybersecurity and Infrastructure Security Agency (CISA) [8]

“Due to the centrality of DNS for cybersecurity, the DoD included DNS filtering as a requirement in its Cybersecurity Maturity Model Certification (CMMC) standard (SC.3.192).”

[6] https://www.ncsc.gov.uk/guidance/protective-dns-for-private-sector

[7] https://www.gartner.com/en/documents/4002327

[8] https://web.archive.org/web/20240828180627/https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting-Protective-DNS_UOO11765221.PDF

2020

## Former NSA Director of Cybersecurity Anne Neuberger [9]

"Protective DNS (PDNS) systems prevent malicious domains from being visited by devices in your network[...] Preventing access to these domains should protect your organisation against malicious actors, making it harder for them to compromise your networks, and harder to exploit any compromises."

2019

## Health Law Advisor [10]

"The importance of the Domain Name System (DNS) to your organization's cybersecurity cannot be understated."

"Protect DNS functionality as a fundamental component of your organization's overall cybersecurity and compliance strategy."

"An organization cannot comply with [legal] regulatory frameworks requiring reasonable network security safeguards without considering threats to DNS."

2019

## CISA [11]

"Select and use a PDNS system as part of a layered defense-in-depth strategy[...]"

[9] https://executivegov.com/2020/06/anne-neuberger-on-nsas-secure-dns-pilot-program

[10] https://www.healthlawadvisor.com/harden-your-organizations-domain-name-system-dns-security-to-protect-against-damaging-data-loss-and-insider-threat

[11] https://www.cisa.gov/news-events/directives/ed-19-01-mitigate-dns-infrastructure-tampering

2006

## Center for Internet Security (CIS) [12]

“Awareness of protecting DNS servers and services seems to be particularly lagging behind, which is astounding given that DNS serves as the foundation on which these other Internet services depend.”

“So often, the security of DNS services is entirely overlooked or it’s importance is significantly underestimated.”

“Given the importance of DNS to most Internet traffic, it is frustrating that many administrators, managers and even service providers do not recognize the importance of securing their DNS environment.”

“Since your organization’s DNS security is critical to the network services your organization depends on, it needs a dedicated security hardened system with minimal services running.”

“Historically DNS continues to be a problematic service with regard to security in that it is unauthenticated and fairly easily spoofed.”

[12] https://www.cisecurity.org/~/jssmedia/Project/cisecurity/cisecurity/data/media/files/uploads/2017/04/CIS_BIND_Benchmark_v10.pdf

## Why DNS Security is Essential

1 Most cyber threats leverage the DNS layer as a part of their modus operandi.

2 Implementing Protective DNS (PDNS) helps block malicious domains before they have an opportunity to cause harm.

3 Governments and cybersecurity experts globally advocate for strongest possible DNS security measures.

## Recommended Reading

Find out more about how following organizations use PDNS to protect their networks.

CASE STUDY – **TRANSPORTATION & LOGISTICS**

whalebone

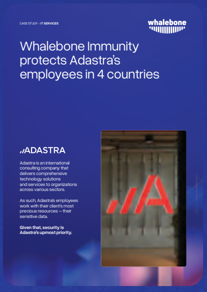
Railway Company Slovakia Protecting employees all over the country and in the field

ŽELEZNIČNÁ SPOLOČNOSŤ SLOVENSKO

"Whalebone Immunity smoothly integrates with all of our security measures, adding an important security layer to stop threats other solutions might miss."

PATRIK MALY
IT SPECIALIST, RAILWAY COMPANY SLOVAKIA

**Railway Company Slovakia:** Protecting Employees Across the Country and in the Field


CASE STUDY – **IT SERVICES**

whalebone

Whalebone Immunity protects Adastra's employees in 4 countries

//ADASTRA

Adastra is an international consulting company that delivers comprehensive technology solutions and services to organizations across various sectors.

As such, Adastra's employees work with their client's most precious resources – their sensitive data.

**Given that, security is Adastra's upmost priority.**

How **Adastra** Protects its Employees in 4 Countries

CASE STUDY – **MANUFACTURING**

whalebone

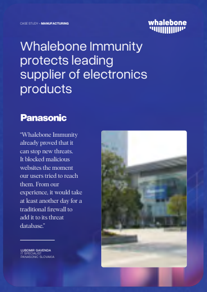
Security DNS Filtering for AERO Vodochody AEROSPACE

Aero | VODOCHODY

Security of the internal network is one of the main priorities of the company AERO Vodochody AEROSPACE, which is why they continuously seek technologies that can improve it.

**This is the reason why the company decided to implement Whalebone Immunity.**

Security DNS Filtering for the **World's Largest Manufacturer** of Training Jet Airplanes


CASE STUDY – **MANUFACTURING**

whalebone

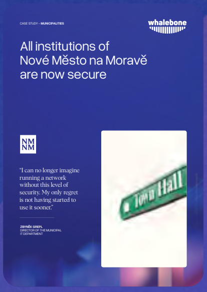
Whalebone Immunity protects leading supplier of electronics products

Panasonic

"Whalebone Immunity already proved that it can stop new threats. It blocked malicious websites the moment our users tried to reach them. From our experience, it would take at least another day for a traditional firewall to add it to its threat database."

LUBOMIR GAVENDA
IT SPECIALIST
PANASONIC SLOVAKIA

How PDNS Provides a Key Security Layer to **Panasonic Slovakia**


CASE STUDY – **MUNICIPALITIES**

whalebone

All institutions of Nové Město na Moravě are now secure

NM
NM

"I can no longer imagine running a network without this level of security. My only regret is not having started to use it sooner."

ZBYNĚK GREPL
DIRECTOR OF THE MUNICIPAL IT DEPARTMENT

All Institutions of **Nove Mesto na Morave** (Municipality) Are Now Secure

### Take Action Now

Integrate DNS security into your cybersecurity strategy today.

For more information, visit:
whalebone.io

whalebone