

Leveraging PDNS for a ZTDNS Strategy.



This white paper explores how Protective DNS (PDNS) supports a Zero Trust DNS (ZTDNS) approach by filtering and securing DNS traffic against cyber threats. It details Whalebone Immunity's capabilities, including encrypted DNS protocols, identity-based policies, and real-time threat intelligence, to enforce continuous verification of DNS requests. Readers will learn practical recommendations for integrating PDNS within Zero Trust, improving network security through proactive DNS monitoring and control. Ideal for organizations seeking to reinforce DNS security within a Zero Trust framework.

Table of contents

- 4** INTRODUCTION: THE ROLE OF ZERO TRUST AND PROTECTIVE DNS IN MODERN CYBERSECURITY
- 5** BEYOND BUZZWORDS: DNS SECURITY IN A ZERO-TRUST CONTEXT
- 7** UNDERSTANDING PROTECTIVE DNS IN A ZERO TRUST MODEL
- 9** REGULATORY COMPLIANCE BENEFITS OF PDNS
- 10** WHALEBONE IMMUNITY: TECHNICAL ADVANTAGES TOWARD A ZTDNS FRAMEWORK
- 15** CONCLUSION: RECOMMENDATIONS FOR ORGANIZATIONS ADOPTING ZTDNS WITH PDNS
- 16** HAVE A CONVERSATION WITH US

Introduction: The Role of Zero Trust and Protective DNS in Modern Cybersecurity

Modern cybersecurity requires a proactive, defense-in-depth approach to mitigate evolving threats. Zero Trust is a model that operates on the assumption that no network traffic—internal or external—can be inherently trusted. Zero Trust DNS (ZTDNS) applies these principles to DNS security,

demanding constant verification of all DNS requests. Protective DNS (PDNS), as implemented through solutions like Whalebone Immunity, contributes toward a ZTDNS strategy by actively filtering, blocking, and monitoring DNS traffic based on up-to-date threat intelligence.

This white paper explores the technical mechanisms and security benefits of integrating Whalebone Immunity into a ZTDNS philosophy.

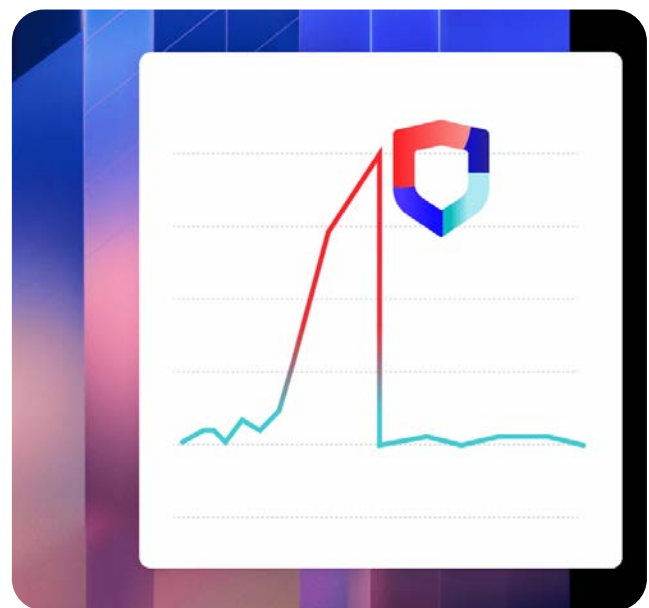
“Our analysis highlighted that using secure DNS would reduce the ability for 92% of malware attacks both from command and control perspective, deploying malware on a given network.”

UNITED STATES DEPUTY NATIONAL SECURITY ADVISOR AND FORMER
NATIONAL SECURITY AGENCY DIRECTOR ANNE NEUBERGER

Beyond Buzzwords: DNS Security in a Zero-Trust Context

IDC's 2023 Global DNS Threat Report highlighted the increasing importance of DNS security. The report revealed that, while 80% of organizations recognized DNS security as critical, only 21% were actively using DNS data for threat intelligence.

This gap underscores the need for more organizations to leverage DNS as a critical part of their security strategy, not just as a trendy add-on.



Microsoft's introduction of ZTDNS is generating significant interest in the cybersecurity community. While the term 'ZTDNS' may seem like just another buzzword, it's important to acknowledge the underlying principles behind it that substantially strengthen DNS security – and thus security overall.

At the heart of the ZTDNS principle is the idea of restricting IP connections to only those that have been properly resolved via DNS queries. This approach adds a powerful layer of security, effectively enhancing overall system resilience.

By ensuring that only legitimate and safe DNS-resolved connections are allowed, this method tightly controls network activity, making it harder for attackers to exploit any vulnerabilities. In practice, this means that before any device or service can connect to an IP, the system checks if the IP has been resolved through a verified DNS query. This limits the possibility of unauthorized or malicious connections since they bypass DNS entirely.

Although strict enforcement may introduce challenges – which can be easily resolved with the right configuration (see Microsoft's Deployment Considerations for

Windows ZTDNS Client) – the security benefits far outweigh these issues.

Essentially, it narrows the scope of potential threats by drastically reducing the attack surface that attackers can target. Traditional DNS was not designed with security as a primary concern. However, as threats are pervasive and attackers increasingly sophisticated, adding layers of security to DNS is not just advisable – according to CISA, Gartner, GigaOm, and other authorities, it's now essential. Microsoft's ZTDNS is an effort to integrate DNS into a Zero Trust framework, emphasizing the importance of verifying every network connection, whether internal or external.

Applying strong identity-based authentication at the DNS level is not only feasible but also an advisable measure that can make life significantly more challenging for attackers. Whalebone has been ahead of this curve, having already implemented strong authentication, for example, within our Home Office Security application. Each device is assigned a unique certificate and private key, ensuring that only authenticated devices can establish connections with our resolvers.

This approach aligns with the Zero Trust principle of 'never trust, always verify,' ensuring that every DNS request is securely authenticated.

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

GARTNER RESEARCH

QUICK ANSWER: HOW CAN ORGANIZATIONS USE DNS TO IMPROVE THEIR SECURITY POSTURE?

Understanding Protective DNS in a Zero Trust Model

Protective DNS is a DNS security layer designed to prevent the resolution of malicious domains. Within a ZTDNS approach, PDNS continuously monitors and validates DNS queries,

filtering out suspicious traffic and enhancing visibility into DNS usage. Whalebone Immunity's PDNS capabilities allow organizations to enforce ZTDNS principles

by controlling DNS traffic with precise, dynamic threat intelligence and ensuring encryption and authentication of DNS communications.

Technical Components of ZTDNS Principles Enhanced by PDNS

1. Local DNS Resolvers for Isolated Traffic

Local DNS resolvers are essential for isolating and controlling DNS requests within an organization's perimeter.

By using Whalebone Immunity's PDNS solution, organizations can configure local DNS resolvers that reduce reliance on external

servers, limiting the exposure of DNS queries to potential threats.

Local resolvers enable faster DNS responses, as traffic does not need to travel outside the network for resolution, and allow for detailed internal monitoring. Additionally, local

resolvers allow granular enforcement of access policies, enabling security teams to specify which devices or users can make DNS requests based on established trust parameters.

2. DNS Encryption and DNSSEC

DNS encryption protocols, such as DNS over HTTPS (DoH) and DNS over TLS (DoT), secure DNS traffic by preventing third parties from intercepting, spoofing, or manipulating DNS requests. Whalebone Immunity supports both protocols to provide encrypted

DNS resolution, to align with Zero Trust principles by concealing DNS queries from unauthorized parties and preventing DNS data leakage. In addition, Whalebone supports DNSSEC (Domain Name System Security Extensions), which complements DoH/DoT by ensuring

the authenticity and integrity of DNS data along the resolver-to-resolver path. Together, these technologies provide comprehensive protection against DNS-based attacks, such as spoofing and cache poisoning, and guarantee that only legitimate and secure requests are processed.

3. Identity-based Access and Authentication Policies

Zero Trust prioritizes identity-based verification at each network interaction. Whalebone Immunity reinforces this by tying DNS requests to verified device and user identities, allowing administrators to enforce strict access policies at the DNS

level. By linking DNS requests to specific users or devices, security teams can limit DNS resolutions to trusted sources and easily track and analyze DNS traffic at a user level by using Active Directory or another standard solution connected

via Whalebone API. Additionally, Whalebone Immunity can integrate with Active Directory and is able to implement role-based DNS filtering based on network segmentation, ensuring that DNS queries align with each user's privileges and needs.

4. Real-time Threat Intelligence Integration for Dynamic Blocking

Real-time Threat Intelligence Integration for Dynamic Blocking
Real-time threat intelligence is essential for a responsive ZTDNS approach, as it provides data on newly identified malicious domains and emerging threats. Whalebone

Immunity integrates continuously updated threat intelligence, proactively blocking DNS requests associated with known malicious domains, ransomware distribution sites, and phishing sites. This integration of real-time intelligence

not only prevents potentially harmful DNS resolutions but also provides organizations with the ability to monitor trends in attempted access to malicious sites, offering insights into possible internal security threats and vulnerabilities.

5. Automated Monitoring and Anomaly Detection for DNS Traffic

Monitoring and analyzing DNS traffic is critical in identifying potential security incidents early. Whalebone Immunity's PDNS solution includes automated anomaly detection, which continuously analyzes DNS traffic patterns to identify unusual

activity, such as frequent access attempts to restricted domains or high rates of DNS resolution failures. Anomaly detection enhances Zero Trust by identifying and isolating potentially compromised devices or suspicious traffic patterns for further

investigation. These monitoring capabilities also enable organizations to detect subtle indicators of potential attacks, such as DNS tunneling, where attackers attempt to exfiltrate data by encoding it within DNS queries.

“Due to DNS being foundational to most online activity, ensure that PDNS is provided as a high availability service.”

CISA,
SELECTING A PROTECTIVE DNS SERVICE

Regulatory Compliance Benefits of PDNS

Integrating PDNS as part of a ZTDNS strategy supports compliance with data privacy protection and cybersecurity regulations such as the EU's NIS2 Directive and other national cybersecurity frameworks. By enforcing encrypted DNS requests,

identity-based access controls, and continuous monitoring, a PDNS solution like Whalebone Immunity restricts unauthorized data access and prevents the exfiltration of sensitive information. These controls help organizations demonstrate

accountability and data protection by design, aligning with regulatory requirements for data confidentiality, breach mitigation, and robust access management in DNS services.

“Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend.”

—NIS2 DIRECTIVE (EU) 2022/2555
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (PARAGRAPH 32)

Whalebone Immunity: Technical Advantages toward a ZTDNS Framework

At Whalebone, we fully embrace the principles of Zero Trust, not just in name but in practical, actionable approaches that enhance DNS

security. While we have talked about the potentially misleading aspects of the 'Zero Trust DNS' label, we also recognize the value in the underlying

principles of Zero Trust, particularly when applied thoughtfully to DNS.

Local Resolvers for Immediate Verification

One of the key aspects of our approach is the deployment of local resolvers as close to the client as possible. By ensuring that DNS resolution and verification occur directly within the network, we enhance direct visibility, improve security, and reduce latency, embodying the Zero Trust principle of verifying every request as close to the source as possible.

Encrypted DNS Communication

Whalebone also offers DNS over HTTPS (DoH) and DNS over TLS (DoT) for internal networks. These encryption protocols ensure that all DNS communications are secure, protecting against interception or tampering. This aligns with the core Zero Trust tenet of securing every layer of communication.

Comprehensive DNS Traffic Visibility

Visibility is crucial in a Zero Trust framework, and Whalebone provides complete oversight of both internal and external DNS traffic. This allows us to detect anomalies and potential threats in real time, ensuring that any suspicious activity is quickly identified and addressed.

Whalebone Immunity provides an all-encompassing PDNS solution designed to reinforce ZTDNS principles through robust DNS security measures:

Encryption and Privacy Controls

Immunity supports DoH and DoT, maintaining DNS confidentiality and integrity to prevent eavesdropping or tampering.

Comprehensive Threat Intelligence

With a dynamic feed of malicious domains, Immunity ensures that users cannot inadvertently access high-risk domains, reducing the chances of attacks leveraging any domain translation. According to US Deputy National Security Advisor and former NSA Director Anne Neuberger, 92% of attacks include the domain translation at some point.

Actionable Data for the SOC Team

Immunity provides full integration with SIEM via API or syslog for easy correlation with other security systems.

Detailed Reporting and Analytics

Immunity's logging and analytics capabilities allow for continuous visibility into DNS usage and incidents, supporting Zero Trust monitoring and anomaly detection.

Identity Verification and Role-based Filtering

Immunity's integration with identity-management system Active Directory enforces strict DNS policies based on user role and device type, which aligns with the Zero Trust objective of limiting access to only necessary permissions.

Protective DNS (PDNS) is a critical component in reinforcing a Zero Trust DNS strategy by providing an added layer of security that ensures all DNS requests are verified, filtered, and encrypted. Whalebone Immunity's features – including encrypted DNS protocols, real-time threat intelligence, and identity-based policies – serve

to continuously protect DNS traffic and reinforce Zero Trust principles. By adopting Whalebone Immunity, organizations can achieve greater security resilience, preventing DNS-based attacks and maintaining stringent oversight of DNS activity within the Zero Trust model.

“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.”

AUSTRALIAN SIGNALS DIRECTORATE (ASD)

GATEWAY SECURITY GUIDANCE PACKAGE: GATEWAY TECHNOLOGY GUIDES

Gaining the Upper Hand with Whalebone's Local & Regional Threat Intelligence Exchange Networks

With cyber threats evolving at an unprecedented pace, real-time protection is no longer optional but essential. Whalebone's Threat Intelligence Network serves as a critical defense layer, blocking 15

million unique threats daily to protect millions of people across the globe. Whalebone recognizes the importance of regional threat intelligence, as many cyberattacks are geographically specific or

tailored to regional vulnerabilities. The Whalebone Threat Intelligence team conducts regional OSINT research to ensure localized threats are quickly detected and neutralized.

Localized Cybersecurity: Tailored Regional Protection

As no two regions face the same cyber threats, we take a country-specific approach to identifying cyber threats in every country where we operate. Recognizing that each country's unique regulatory landscapes and specific cyber challenges require a tailored approach, our Threat Intelligence team tailors cyber threat intelligence (CTI)

by utilizing open-source intelligence together with historical and language analysis to fit the needs of individual countries. This, along with our focus on Local Threat Intelligence Exchange, helps to ensure that local regulations are met and that region-specific threats, such as phishing campaigns or malware attacks, are addressed as quickly as possible. This targeted

approach allows us to integrate precise local threat intelligence that directly responds to the most critical risks in each country into our existing global Threat Intelligence solution – so you can trust that you're protected against the threats that matter most to wherever you are.

Collaboration at the Core: Working with Governments and Local Experts via DNS4EU Project

We believe that effective cybersecurity comes from close cooperation with a diverse network of cybersecurity experts. As the appointed Consortium Leader for the European Union's DNS4EU project, our Threat Intelligence Network actively works with government agencies, Computer Emergency Response Teams (CERTs), CSIRTs (Computer

Security Incident Response Teams), academic research institutes, and other cybersecurity vendors. This networked approach ensures that our intelligence is informed by local experts and reinforced by national cybersecurity centers (NCSCs). By working together, we strengthen national and regional defenses, creating a cybersecurity ecosystem

that ensures public institutions and critical-infrastructure verticals like communication service providers (CSPs, such as telecoms and ISPs), transportation, utilities, manufacturing, and others – to stay ahead of emerging threats and help ensure uptime of essential services.



“Protective DNS (PDNS) systems prevent malicious domains 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.”

UK NATIONAL CYBER SECURITY CENTRE:
PROTECTIVE DNS FOR THE PRIVATE SECTOR

Whalebone's leadership in the DNS4EU project has enabled real-time threat detection and mitigation across Europe with Consortium Members from 10 European countries and 100s of 'Stakeholders'. By collaborating with regional CERTs and CSIRTs, Whalebone ensures that intelligence

on phishing campaigns, ransomware attacks, and malicious domains gets shared and acted upon in real time. DNS4EU Stakeholders include technical experts, industry leaders, government officials, and representatives from various sectors, all working together to influence the

direction of DNS4EU. The role allows participants to engage with European authorities and other stakeholders to ensure that the system meets technical, legal, and regulatory requirements while maintaining data privacy and security standards.

Conclusion: Recommendations for Organizations Adopting ZTDNS with PDNS

Deploy Local DNS Resolvers

Establish local resolvers to ensure DNS queries are processed within the organization's network, reducing external exposure and enhancing control.

Enforce Encrypted DNS Protocols (DoH/DoT)

Secure DNS traffic with DoH and DoT to prevent unauthorized access to DNS queries.
Implement Role-based Access Policies – Leverage identity-based verification to limit DNS access, limited according to users' roles and responsibilities.

Integrate Real-time Threat Intelligence

Utilize out-of-the-box dynamic intelligence feeds to proactively block access to known malicious domains and prevent DNS-based threats from reaching end-users. Additionally, users can enhance their local threat intelligence by blocking particular domains they observe and consider as dangerous.

Continuously Monitor DNS Traffic

Employ anomaly detection features to track DNS traffic patterns and respond to irregular activity, ensuring swift detection and mitigation of potential threats. By leveraging Whalebone Immunity, organizations can integrate PDNS to reinforce their ZTDNS approach, achieving a comprehensive DNS security solution aligned with Zero Trust principles to protect against modern cyber threats.

Have a Conversation with Us

If you're ready to enhance your organization's DNS security — or if you have questions about how ZTDNS principles fit into broader cybersecurity strategies — Whalebone is here to help. Reach out to our team to learn how our proven PDNS solutions can safeguard your network and data with a proactive and comprehensive approach.



www.whalebone.io



Follow us

©2025 Whalebone, s.r.o.
All rights reserved 2025