whalebone

Whalebone Immunity Setup Guide

Over 90% of attacks use DNS. Block them with Immunity.

Domains play a crucial role in communication between attackers and malware. Without DNS protection, your network remains vulnerable to modern attack methods.

Firewalls are not enough:

"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.."

ANNE NEUBERGER
US NATIONAL SECURITY AGENCY
DIRECTOR OF CYBERSECURITY

"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

"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

"Member states should encourage the development and use of a public and secure European DNS resolver service."

EUROPEAN COMMISSION
NIS2, SECTION 100

Protect your entire network in under 2 hours

DNS resolver is a crucial part of infrastructure you should have under your control

Protective DNS disrupts the whole cyberattack life-cycle

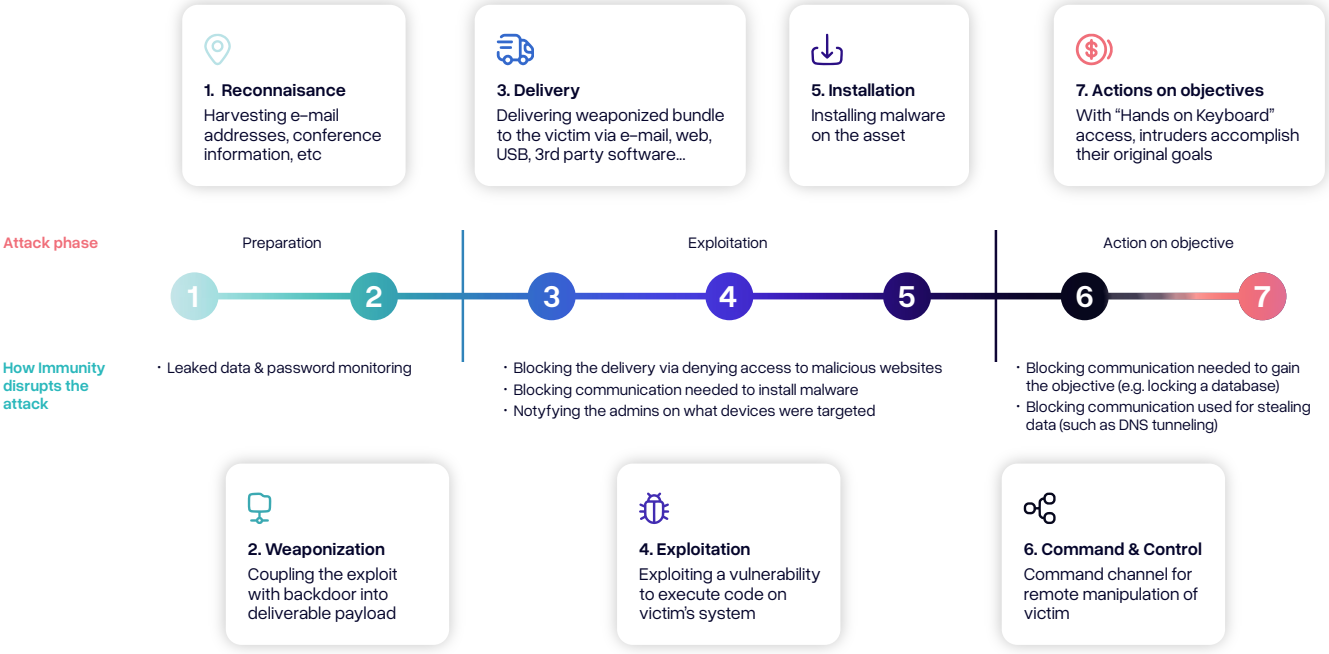
With ZTDNS, 80% more threats are detected compared to using only next-gen firewall*

** Based on research of data provided by independent German security authority AV-TEST*

Make sure to take advantage of the free trial version to instantly make work of you and your team more effective:

- **Instant Security** – Requires no installation or special skill set, start using in 30 minutes
- **Immediate Results** – During a free trial, over 50% of our customers discover malicious traffic, and around 50% also uncover leaked sensitive information tied to their domain
- **Proven ROI** – Our customers, from Panasonic to Slovak Railways, consistently report significant threat reduction and improved operational resilience with Whalebone Immunity
- **Market Leadership and unique threat intelligence** – Appointed Consortium Leader for DNS4EU and threat intelligence partnerships with more telcos than any other DNS security provider (plus over 300 ISP customers)
- **ISO Certified** – 9001, 27001, 22301, 27018

No matter the attack phase, Whalebone Immunity closes your security gaps:



What to do next

> “Even though I was not used to working with Linux, I was able to deploy Whalebone Immunity in half a day thanks to comprehensive product documentation.”
>
> PATRIK MALÝ
> IT SPECIALIST AT RAILWAY COMPANY SLOVAKIA

Choose how do you want to deploy Whalebone Immunity into your network:

- **System Requirements** — Whalebone Immunity for on-premises deployment requires a linux VM with 2 cores, 4GB of RAM, and 80GB drive to be able to host a resolver for up to 25k users.
- **Supported DNS Protocols and Encryption** — Whalebone Immunity supports all standard DNS protocols, including DNS over HTTPS (DoH) and DNS over TLS (DoT), applying industry-standard encryption to protect DNS queries against interception or manipulation. This ensures baseline privacy and security, particularly for enterprises focused on data integrity. DNSSEC validation is ensured for every query.
- **Network Requirements** — Whalebone Immunity offers flexible deployment options with minimal hardware requirements. It can function as a local DNS forwarder, making it compatible with complex network setups, or as a full DNS resolver on-premises for comprehensive coverage ensuring full control over infrastructure, deep visibility and fast resolution speed. For organizations seeking a lighter setup or second form of backup, Whalebone’s cloud deployment is available, reducing on-premises infrastructure needs while ensuring robust DNS security across network configurations.
- **Widen Your Security Perimeter** — Designed for enterprise scalability, Whalebone Immunity handles networks of varying sizes and complexity, with performance adjustments for larger networks. It covers remote workers thanks to Home Office app deployable via MDM solutions.

We’ve simplified the process to get you up and running with Whalebone Immunity in no time:

1. **Discover & Plan**	**Schedule a Demo Call** — Learn about Whalebone Immunity’s powerful DNS protection capabilities, and collaborate with our team to model the best use case for your network.	**1–2 days**
2. **Free Trial**	**Experience Immunity Firsthand** — Start a free trial to see Whalebone Immunity in action on your network — and how easy it is to run. Discover malicious traffic and assess its impact on your network’s security.	**1 week**
3. **Deploy & Integrate**	**Fast & Easy Deployment** — With minimal configuration, protect your entire network in less than 2 hours. Choose from on-premises, cloud, or hybrid options for seamless integration.	**1 hour (cloud)** **Up to 5 hours (on-prem/hybrid)**
4. **Lifetime Support**	**Expert Support** — We provide ongoing support so that you get maximum value with minimal maintenance.	**Continuous**

Your Trusted Solution

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

ZBYNEK GREPL
DIRECTOR OF MUNICIPAL IT
NOVE MESTO NA MORAVE
(CZECH MUNICIPALITY)

> “It blocked malicious websites the moment our users tried to reach them. It would take at least a day for a firewall to add them to its threat database.”

LUBOMIR GAVENDA
IT SPECIALIST
PANASONIC SLOVAKIA

DNS4EU
JOIN
THE EUROPEAN
SAFE DIGITAL SPACE

Trusted by the European Union
The European Commission appointed Whalebone as Consortium Leader for DNS4EU, an initiative to secure Europeans’ critical infrastructure and services via innovative and reliable cybersecurity solutions.

Whalebone is committed to the highest standards of data security and operational excellence. We hold internationally recognized certifications, including ISO 9001, 27001, 22301, and 27018, attesting to our rigorous quality management, data protection, business continuity, and privacy standards.

Additionally, Whalebone collaborates closely with AV-TEST, a respected German security testing authority, to ensure that our solutions meet stringent performance and security benchmarks — with the lowest possible false positives.

By leveraging Whalebone Immunity to close security gaps, organizations benefit from robust support in maintaining compliance with key regulatory frameworks such as GDPR and NIS2, safeguarding sensitive data and reinforcing network security to meet European and global standards.

Get Started Now with a Free 30-Day Trial

With a quick setup in less than 2 hours, you can explore Whalebone Immunity with:

- **Flexible Deployment Options** — Choose from on-premises, cloud, or hybrid models
- **Seamless API Integration** — Integrate smoothly with existing infrastructure
- **Immediate, Quantifiable Results** — Identify threats and see measurable security improvements

Easily redirect part of your network traffic to Whalebone resolvers to start the free trial.

immunity@whalebone.io

We will happily answer your questions.
Mutual satisfaction is our main goal
— we will do our best to fulfill your requests.

www.whalebone.io

Learn more about our products at:
whalebone.io/immunity

Follow us on LinkedIn for more information on DNS security.